Horizon 2020 Programme
DG CNECT
Next-generation Internet

NGI TRUST

Project acronym: **PAE:CG**

Project title: **Privacy as Expected: Consent Gateway**

Partners: **Trinity College Dublin (TCD), OpenConsent Ltd., Birmingham City University (BCU)**

Trinity College Dublin
Coláiste na Tríonóide, Baile Átha Cliath
The University of Dublin

OPEN CONSENT

BIRMINGHAM CITY University

Deliverable 2.4

Consent Receipts

Deliverables leader:	**Trinity College Dublin**
Authors:	Harshvardhan J. Pandit (TCD)
Due date:	2021-06-12
Actual submission date:	2021-07-12
Dissemination level:	Public
DOI:	https://doi.org/10.5281/zenodo.5076603

Abstract: Consent is an instrument which enables an individual to express and exercise control over actions and consequences related to their self. When enshrined under law, 'consent' forms the basis of legal justification as a permission for specified activity or implication. Within data protection and privacy laws, consent has long been a crucial instrument for providing the individual with agency, authority, and control over how their personal data is collected, stored, used, and shared with other external entities.

With laws increasingly realising the necessity to define additional requirements for what constitutes valid consent, and the prevalence of malpractices regarding consent processes - especially on the web, the issue of providing individuals and organisations with an effective and practical tool for recording their stance in a consent interaction is a powerful tool for accountability, transparency, and technological innovation.

Based on this guiding principle, this document provides the work produced within the Privacy as Expected: Consent Gateway (PaE:CG) project regarding information related to consent, and relevant for producing a receipt outlining the record made for capturing this information in an authoritative manner. The deliverable outlines the motivation, existing work in this area, the information fields identified by the project, its specification and extraction from web pages, and opportunities it has availed of regarding dissemination and standardisation.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Disclaimer

Copyright

Table of contents

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

1. Introduction

Consent is a mechanism that enables individuals to express their choices and thus exercise control regarding use of their personal data. Laws within the privacy and data protection domain, such as the General Data Protection Regulation (GDPR) and ePrivacy Directive (ePD) for the European Union, regulate where consent can be used and applied as the legal basis, and on this basis be used to justify how an organisation can obtain, use, store, and share personal data.

Consent, as regulated within domain-specific laws, must meet several requirements in order to be considered 'valid' i.e. meeting the legal requirements and obligations in order to be used as a justification for the processing of personal data. These requirements include notions such as 'informed consent' - provision of information to the individual so as to enable and empower them to make a conscious decision, as well as 'rights' such as the ability to withdraw consent without detriment.

An unintended consequence of this is the *mania* of consent and cookie banners being present on most of the websites, which expose the working and reliance of the web advertising ecosystem on the *consenting* of the individual. There have been numerous studies that outline how this has exposed the underlying tracking and surveillance activities, their unprecedented scale, and the sensitivity of the data they operate within.

Simultaneously, there is ample evidence and reporting that discloses the plethora of malpractices utilised in consent activities which not only do not meet the legally set requirements of what is considered 'valid consent', but also actively harms the individual and society at large by providing them little to no control over how their own personal data is being collected, utilised, and shared across any of the thousands of companies operating within the web advertising ecosystem.

One of the challenges and problems with the way consent operates currently is that the individual has no alternate mechanism or means to understand what they've consented to or to introspect their decision after they've made it. The 'Consent Receipt' specification was created with the intent of providing both the individual and the organisation with a record of the consent. In principle, this makes the experience of *consent* more transparent and accountable, similar to the way in which a grocery bill or receipt enables recording a transaction and using that information in cases of discrepancy and complaints.

1.1. Aims and Objectives

As laws, their interpretations, and the ecosystem within which they operate has evolved rapidly over the past few years, the consent receipt has become difficult to utilise within legal systems such as those defined by the GDPR. The primary aim of this work is therefore to provide a **Consent Receipt specification based on GDPR's requirements regarding consent**.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Additionally, the work also provides an exploration of the following objectives:

1. Providing trust, transparency, and accountability by utilising cryptographic signatures - as explored in prior work[1] ;
2. Operating within a global landscape consisting of multiple non-compatible jurisdictions - and the role of standards such as ISO/IEC 29100[2] and 29184[3] in harmonising vocabulary and application ;
3. Specifying information required within the receipt in online notices and the webpages they operate within ;

1.2. Relation with Other Work and Deliverables

Within the PaE:CG project, the D2.4 Consent Receipt work package and its deliverable D2.4 guides the information fields utilised by the other deliverables, which are: D2.1 User Plug-in, D2.2 Consent Gateway, and D2.3 Server Component. While the implementations of these deliverables use only a *subset* of the possible fields, the D2.4 deliverable outlines the greater set of fields possible for inclusion and their role within the consent processes.

[1] Jesus, V. (2020). Towards an Accountable Web of Personal Information: The Web-of-Receipts. IEEE Access, 8, 25383–25394. https://doi.org/10/ggsgh4
[2] https://www.iso.org/standard/45123.html
[3] https://www.iso.org/standard/70331.html

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

2. Legal Requirements

2.1. ePrivacy Directive (ePD)

The ePrivacy Directive (ePD), as amended in 2009, outlined the requirement for consent in connection with any storage and access of data deemed non-essential or not 'strictly necessary' for the service requested by the user. This, when applied to the utilisation of 'cookies' as a persistent data storage technology, has resulted in the prevalence of 'cookie banners' across the web. Where such data, irrespective of its medium or technology as covered under the ePD, is considered or involves personal data, the resulting consent must meet both i.e. it must satisfy the conditions for valid consent under both ePD and GDPR.

As such, the consent receipt, by virtue of its aims and intentions of providing individuals more transparency and control over the *purposes* of their personal data being processed, focuses more on the GDPR rather than being concerned with modelling itself as a 'cookie receipt', despite the deep entanglement of cookies within the consent and personal data sharing ecosystems on the web.

2.2. General Data Protection Regulation (GDPR)

The GDPR has several clauses outlining the requirements for obtaining valid consent, both in direct (e.g. specifying consent) as well as indirect (e.g. specifying information provision to individuals) forms.

Art.4-11 defines consent as "*... any **freely given, specific, informed** and **unambiguous indication** of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her;*" (emphasis added).

Along with this definition, Rec.32 clarifies that the conditions for consent "*... could include **ticking a box** when visiting an internet website, **choosing technical settings** for information society services or another **statement or conduct** which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data.*" (emphasis added). Rec.32 additionally states, "*Silence, pre-ticked boxes or inactivity should not therefore constitute consent.*", which lays out the foundation for requiring some definitive action or statement from the individual for it to be considered their consent. It is clear from these that investigations and demonstrations of valid consent must also include the specific action or statement indicating consent.

In continuation of the above, Art.7-2 says "*If the data subject's consent is given in the context of a written declaration which also concerns other matters, the **request for consent** shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.*", and also, "*If the data subject's consent is to be given following a request by electronic means, the request must be clear,*

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

concise and not unnecessarily disruptive to the use of the service for which it is provided.", and also in Rec.42 as, "*a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms.*" All of these imply that investigations for the validity of consent must not only look at the action, but at all the artefacts and their utilisation in the presentation of a request for consent, and their role in how the individual makes and executes their decision.

GDPR outlines the information relevant to the consent and requires it to be provided to the individual as part of the request for consent. This information is outlined through Rec.32 (purpose, processing activities, and their inter-relations), Rec.42 (identity of controller, purpose, processing activities), Rec.60 (purpose, processing activities, profiling, possible use of icons), and indirectly through Art.13 for when information is collected directly from the individual, and Art.14 for when information is collected indirectly from the individual - where for both Art.13 and Art.14 the timing of this information is clarified in Rec.61 as "**at the time of collection** from the data subject, or, where the personal data are obtained from another source, **within a reasonable period**" (emphasis added).

The information to provided, as outlined in Art.13 and Art.14 includes (quoted verbatim, emphasis added):

1. the **identity and the contact details of the controller** and, where applicable, of the **controller's representative**;
2. the **contact details of the data protection officer**, where applicable;
3. the **purposes of the processing** for which the personal data are intended as well as the legal basis for the processing (*consent in this case)*;
4. the **recipients or categories of recipients** of the personal data, if any;
5. where applicable, the fact that the controller intends to **transfer personal data to a third country** or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Art.7 of the GDPR, along with Rec.32, Rec. 42, and Rec. 43 lay the general conditions for validity of consent. Art.7-1 states, "Where processing is based on consent, the controller shall be able to **demonstrate that the data subject has consented** to processing of his or her personal data" (emphasis added), which makes it clear that the consent thus obtained must be demonstrable by the data controller not only in terms of a final artefact indicating the consent, but also including the validity of the process of requesting and obtaining that consent. Consequently, it is also an important distinction when determining whether the controller is not respecting the individual's choice in matters of consent, such as when controller assumes consent where no such consent is given by the individual or they are coerced into giving their consent (as stated in Art.7-4).

GDPR's Art.9 outlines special categories of personal data, whose processing is generally prohibited, unless exempted via a higher degree of responsibility

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

provided through the outlined legal bases. Of these, one is consent (Art.9-2), whose validity requires a higher degree of action or statement by the individual, which is referred to as 'explicit consent'. This is clarified by Article 29 Working Party's Guidelines on consent under Regulation 2016/679, which refers to 'not explicit consent' as 'regular consent', and that 'explicit' has higher requirements from such regular consent by means of the way it is expressed by the data subject. It says, "*It means that the data subject must give an* ***express statement of consent***. *An obvious way to make sure consent is explicit would be to* ***expressly confirm consent in a written statement***. *Where appropriate, the controller could make sure* ***the written statement is signed by the data subject***, *in order to remove all possible doubt and potential lack of evidence in the future*." (emphasis added). This not only raises the bar on how consent should be considered valid, but also offers additional avenues into how consent can be *authenticated* via the participation of the individual i.e through signing. While this is the norm in universities and academic institutions, which provide participants an informed consent sheet to sign and a copy to keep, the application of this method is enhanced by the GDPR.

From the Art.9 concept of *explicit consent*, there is an added emphasis on recording the manner in which individuals express their consent, as well as the possibility for the individual to *sign a statement indicating* an authoritative declaration of their consent. This is of interest to the general idea of consent receipts (as a record) and the notion of signing it (as a form of authorisation regarding their decision).

Additionally, GDPR expresses requirements and possibilities for consent utilised in certain special areas, such as for scientific research (Rec. 33), requirements for the consent of a parent or guardian in case of children (Rec.38), and the use of consent in legitimising transfers of personal data to third country (Art.49-1a) which also specifies that the individual must be informed about possible risks and the existence (or absence) of adequacy decisions and safeguards.

GDPR considers the ability to withdraw consent a right of the individual. In Art.7-3 it says, "*The data subject shall have the* ***right to withdraw his or her consent*** *at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be* ***as easy to withdraw as to give consent***." (emphasis added). From this description, it is clear that the validity of consent also includes assessing whether the information about withdrawal and the actual process of withdrawing consent.

Similar to the right to withdraw consent, GDPR also requires providing information about the existence and application of other rights, as outlined in Art.12 - Art.23. Though these rights have a relationship with consent, in that they may or may not apply depending on the legal basis used, the provision of their information may be an important factor within the notice and request for consent.

Alongside the text of the GDPR, there have been guidelines provided by the Article 29 Working Party (A29WP), and the European Data Protection Board

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

(EDPB) which are authoritative interpretations for requirements, validity, and compliance associated with consent. These include:

- Guidelines 05/2020 on consent under Regulation 2016/679 by EDPB. Version 1.1 Adopted on 4 May 2020.
- A29WP's Guidelines on consent under Regulation 2016/679. Adopted on 28 November 2017. As last Revised and Adopted on 10 April 2018

2.3. CCPA and the use of automated signalling

The California Consumer Protection Act (CCPA) is a state-level legislation passed by the state of California, USA which revamps the privacy landscape by a large margin compared to its predecessors. Distinct from the GDPR, CCPA allows use of data without prior consent from the individual. Instead, it focuses its application on providing individuals with the ability to object to utilising collected data for other purposes and further sharing - via opt-outs.

Relevant to this work are its use of a different and distinct vocabulary, such as the use of 'sell' as a form of data processing action, which is not present in GDPR, and its utilisation in the 'right' to 'opt-out' of 'selling data' to third parties. The fact that CCPA allows machine or technical signals to express this choice is an important change. The Global Privacy Control (GPC)[4] is a (binary) signal that has been developed to take advantage of the opt-out feature in the CCPA, and has been confirmed to be legally enforceable in the manner intended by the CCPA. It has also been adopted and used by high-profile entities such as - Brave (web browser), DuckDuckGo (search engine), New York Times (data controller), and others.

Therefore, for avenues where CCPA is relevant or is applicable, the existence of such signals and their relevant status is important when recording information about consent. Similar to this, GDPR allows use of signals, though the Art.21-5 statement, "*the data subject may exercise his or her right to object by automated means using technical specifications*". Though it must be considered that the right to object is not applicable for consent, as stated by Art.21-1.

Another relevant initiative, similar to the GPC, but applied to the GDPR, and providing a larger variety of controls, is the Advanced Data Protection Control (ADPC)[5]. Instead of providing a single binary signal like the GPC, ADPC instead enables expressing choice over a list of purposes as determined and described by both the controller and the individual. It also enables expressing the right to object to such purposes or at a broad global level. Both the GPC and ADPC are currently in development, and are yet to be evaluated within the GDPR landscape. However, their existence implies the need to consider such technical specifications or controls or 'settings' as being an important aspect of the individual's choices in respect of their privacy and thus their consent.

[4] https://globalprivacycontrol.github.io/gpc-spec/
[5] https://www.dataprotectioncontrol.org/spec/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

3. Existing Work and the State of the Art

3.1. Consent Receipt specification v1.1

The Consent Receipt specification version 1.1 (CRs)[6] provides the outcomes of the work conducted within Kantara's Consent and Information Sharing Working Group. It provides a list of fields representing the information to be represented in a record of consent and its utilisation as a receipt.

It is important to note that the terminology utilised within the Consent Receipt is based on ISO/IEC terminology for providing a global interoperability and application of the record. At the same time, it presents a challenge for utilisation in legal and regulatory use-cases which require specific concepts to be utilised based on their definitions within the jurisdictional law.

In the following paragraphs, the fields within the Consent Receipt v1.1 specification are described and commented on for their usefulness and compatibility within the framework provided by GDPR.

1. Version - provides a way to refer to the version of specification, thereby providing the means to have alternative fields and information interpretations for different use-cases and jurisdictions. CRs does not provide further guidance on how versions should be declared and used.
2. Jurisdiction - provides a way to specify jurisdictions 'applicable' to the 'transaction' i.e. consent. This provides the means to specify the legal context within which the receipt information must be evaluated. CRs does not provide further guidance on what values or specificity should be used when defining jurisdictions - such as whether 'GDPR' is considered a jurisdiction or 'EU' should be used instead.
3. Consent Timestamp - the timestamp of the 'transaction'. Necessitates use of ISO 8601 date and time format. This information is necessary for maintaining a record of the consent. Additionally, the timestamp of receipt generation and provision may also be relevant to determine its continued applicability, such as when providing a receipt after the individual has withdrawn their consent.
4. Collection Method - refers to the method in which consent was obtained. This is an important field as it assists in determining the validity of consent in meeting the requirements laid out by GDPR. CRs does not provide further guidance on the information or its format to be used to specify such methods. The examples provided further in the document outline use of textual descriptions to specify request and indication regarding consent.
5. Consent Receipt ID - provides a unique identifier for the receipt. This provides the means to refer to the consent record represented by the receipt, and can be utilised as a shared identifier by both the controller and the individual. CRs necessitates it to be a UUID-4 string.
6. Public Key - refers to the controller's public (cryptographic signature) key. Provides the means to verify the authenticity of a receipt by asking the controller to sign it. The PaE:CG application furthers application of this field

[6] Lizar, M., & Turner, D. (2017). *Consent Receipt Specification v1.1.0* (p. 29). Kantara Initiative. https://kantarainitiative.org/download/7902/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

to enable other parties to sign the receipt. CRs does not provide guidance on the specific forms of signing and keys to be used or their verification processes.

7. Language - refers to the language in which consent was 'obtained', which must be a ISO 639-1:2002 language code (e.g. 'en' for English). While this field is important in investigations of validity of consent, it is unclear as to what constitutes 'language' and what it refers to - the notice or the control exercised by the individual. For general purposes, it can be assumed that both notice and controls (e.g. button saying 'I Agree') utilise the same language, and that this field refers to the language used to communicate with the individual. Additionally, it is also important to distinguish this field's application as referring to the technical language or machine-readable metadata through which the consent processes are communicated.
8. PII Principal ID - PII Principal is ISO terminology for 'Data Subject'. Refers to the identifier, such as email address or username, used to identify and refer to the individual. CRs states this is a mandatory field and that consent is not possible without an identifier. PaE:CG differs from this perspective, and considers that the Receipt (and its identifier) can be utilised as an identifier in referring to both the individual and their consent.
9. PII Controller - ISO terminology for 'Data Controller'. CRs requires this field to specify the 'name' of the 'first' controller who 'collects the data'. Further utilisation of the field is elaborated as controllers determining the purposes of processing, and possibility for more than one controller to be associated with the processing of personal data (referred to as PII in ISO terminology). This relates to the GDPR requirements for a controller's identity (e.g. Art.13), data protection officer, and representatives.
10. On behalf - refers to the PII Processor ('Data Processor' under GDPR) acting on behalf of a PII Controller or PII Processor. Notably, CRs defines this as a boolean field (yes/no) which only suffices to denote the existence of a processor being used without further information on their identity or role within the purposes specified regarding consent. GDPR does not mandate specification of a processor's identity, but does refer to 'categories' of processors being specified alongside other information.
11. PII Controller Contact - refers to the name of the controller. Together with other fields related to PII Controller's contact (Contact, Address, Email, Phone, URL), CRs provides a rigid structure for specifying how a controller must offer communication. This provides difficulties when specifying newer forms of modern communication mediums, such as social media handles and instant messaging services.
12. Privacy Policy - refers to the policy and 'applicable terms of use' in effect when consent was obtained and receipt was issued. Mentions the link specified to refer to the specific 'version' of policy for continued reference when it evolves. GDPR by contrast does not mandate specifying privacy policy explicitly, but the requirements of Art.13 and Art.14 offer implicit guidance on the necessity to include references to any notice which exist to provide information on the processing of personal data. By extension, this includes the notice providing information for request of consent.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

However, this field specifically refers to a specific commonly used form of notice, i.e. the privacy policy.

13. Purpose - refers to a 'short, clear explanation of why the PII is required', which is what the GDPR refers to as 'purpose for which the personal data is processed'. It is an important field, with conditions and requirements in how it is communicated to the individual which also affect the validity of their consent.
14. Service - refers to a generic concept 'service' which is commonly used but not defined within the GDPR. It can be understood to provide a greater abstraction to the purposes used and to group them in relation to a specific 'service' or 'product' offered or utilised by the controller. A further field, 'Primary Purpose' is used to refer. as a boolean (yes/no), whether the purpose is part of the 'core service' of the controller. CRs does not provide guidance on what constitutes 'core service'.
15. Purpose Category - refers to 'reason the PII Controller is collecting the PII'. Is another form of abstraction for providing a general or commonly understood description of the 'category' of purposes. While not defined in GDPR, it may be of value to better understand and utilise purposes for both controllers and individuals. A good example of this is the category 'Marketing' with further detailed explanation provided using the 'Purpose' field, while the 'Service' field offers information on the specific service or product under which this purpose is utilised. It is important to note that other than purpose, the other fields (service, category) are not defined and consequently not utilised within GDPR evaluations of consent. Additionally, GDPR requires purpose descriptions to be clear and sufficient on their own.
16. Consent Type - refers to the 'type' of consent used by the controller as justification to process personal data. CRs uses a default value of 'explicit', with other values requiring descriptions of the consent method. For GDPR, there can be 'regular' and 'explicit' as consent types. It is important to note that these 'types' are defined based on legal requirements and are thus confined to jurisdictions they are applicable in. This results in incompatibilities when the same term is used in different contexts, for example 'explicit' consent is not the same within ISO/IEC 29184 and the GDPR[7]. Therefore, any notation of a consent type must be interpreted alongside the information about jurisdiction it is defined in.
17. PII Categories - refers to the categories of PII 'that will be shared as understood by the PII principal'. CRs provides predefined categories that must be used, which limits the applicability of the receipt for other use-cases. It is important to note the language used to describe which categories are to be defined, which may constitute a limited description where only the information 'shared' by the individual needs to be defined. By contrast, GDPR requires providing information about personal data categories with specific obligations when they are collected from the individual (Art.13) or obtained from other sources (Art.14). Both the CRs and GDPR are ambiguous regarding data obtained via further processing of collected data, such as through inferences.

[7] Pandit, H. J., & Krog, G. P. (2021). Comparison of notice requirements for consent between ISO/IEC 29184: 2020 and General Data Protection Regulation. *Journal of Data Protection & Privacy*, *4*(2), 193–204.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

18. Termination - refers to the 'conditions for termination of consent', which includes links to policies defining how consent is terminated. While GDPR necessitates the provision of information about the right to withdraw consent, it is important to distinguish between the two terms - 'terminate' and 'withdraw'. The term 'terminate' refers to the termination of consent as a justification for processing of personal data, whereas 'withdraw' specifically refers to the individual's choice and control to withdraw their consent. The withdrawal of consent can effectively be referred to as its termination, but it is not the only way in which consent can be terminated. For example, consent is terminated after it 'expires' following a temporal duration, or consent is found invalid by an authority or a court and is terminated.
19. Third Party Disclosure - refers to whether the controller is 'disclosing' PII to a third party, indicated using boolean values (yes/no). CRs does not provide guidance on what is considered 'third party'. It provides a further field for indicating the 'Third Party Name' which can be used to which the 'PII Processor may disclose the PII'. Under GDPR, it is important to not only specify when data is being 'disclosed' to a 'recipient', but also the identity of the third party as a recipient. It is also important to consider that this obligation applies regarding who discloses the data since the processor acts on the instructions of a controller, and therefore any sharing of data to a third party by a processor is still considered as a decision of the controller.
20. Sensitive PII - refers to whether 'PII' is designated sensitive or not sensitive (as a boolean yes/no) with a further field for indicating the categories of sensitive PII as defined by CRs. Under GDPR, the notion of 'special categories of personal data' is not similar to 'sensitive personal data', since obligations refer specifically to special categories only. But it can be considered that special categories are a subset to that of sensitive data, and that in most cases, the processing of sensitive data requires a higher degree of responsibility similar to what is intended for special categories.

CRs provides a data structure and a 'schema' indicating how the receipt fields should be structured and used. It demonstrates the use of JSON as a format for specifying this information, and its use in producing both machine-readable and human-readable receipts.

3.2. ISO/IEC 29184: Online Privacy Notices and Consent

ISO/IEC 29184 is a recent standard published in 2020 relating to the use, provision, applicability, and standardisation of notices used for providing information and controls to individuals for requesting their consent. It fits within the larger ISO 29100 framework regarding privacy.

29184 provides guidelines and conformity conditions for notices in terms of how they should be provided in terms of visual appearance, linguistic modalities, timing, locations, forms, accessibility, and persistence. It also provides information on the expression of content within a notice, which consists of the purposes of processing personal data, identity of controllers, details about legal basis, and describing processing of personal data and its collection including its method, location, use, retention, disclosure to third parties, and timing. It specifies four

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

çategories of data collection methods to be specified in a notice - directly from the individual, indirectly through another source, observed, and inferred.

In terms of jurisdiction, 29184 specifies that the geographic location is relevant when specifying the location and jurisdiction for personal data being stored - which is in line with GDPR's requirements for data transfers to third countries and the use of adequacy decisions and safeguards.

29184 uses the concept of 'choice' as referring to the action made by the individual, which can only 'entail' consent when the requirements under which that choice is made are informed and fair. This is similar to the concept of 'validity of consent' under GDPR. The 'control' defined by 29184 requires the controller to preserve evidence of this choice (relevant to GDPR's demonstration of consent), and to provide information to the individual regarding how they can access and revise their choice (in context of consent).

Notably, 29184 specifies organisations should provide information about plausible risks to the individuals where there is an impact to privacy and their likelihood are deemed high or the risks are not evident from the other information provided to the individual. While GDPR also has risks assessments and their use in consent (such as for data transfers), the phrasing and requirements set out by 29184 are broader than those described within the GDPR. 29184 further elaborates how risks can be specified, their placement, and specificity within the notice alongside other information for relevance.

There are some user-centric guidelines specified within 29184, such as the indication of specific accounts or identifiers being used within which consent is expressed, the frequency and timeliness of consent, renewing notices on information change and further on renewing consent.

An interesting description of the forms in which notices may be provided consists of design features such as layering, just-in-time presentation, use of icons, and the provision of notices in machine readable formats. 29184 does not provide guidance on how such machine-readable formats can be utilised or guide their development, though in its appendices it provides the consent receipt specification (v1.1) as an example of a record of consent that can be retained by controllers and individuals.

An interesting interpretation of these requirements taken together, especially regarding the existence of consent receipts and machine-readable notices is that they obviously share an overlap in the information contained within. PaE:CG posits that for consent receipts to be an effective tool, the information contained within can be provided through such machine-readable notices. Therefore, the development of PaE:CG consent receipt also guides the creation of machine-readable notices.

3.3. ISO/IEC 27560: Consent Record Information Structure

ISO/IEC 27560 is an ongoing effort at standardising consent records in terms of information fields and their interpretation. It started in 2020 and is currently in the working draft stage where the contents are iterated upon and are considered unstable for use. The Consent Receipt v1.1 forms the starting pivotal point for the development of 27560, and furthermore the existing ISO 29100 privacy framework

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

and the 29184 standard provide contextuality for guiding the development and application of 27560.

3.4. IAB and the Transparency & Consent Framework

The Interactive Advertising Bureau (IAB) develops industry standards for the online advertising industry, and is the creator of the Transparency & Consent Framework (TCF)[8] used widely in publisher-consumer negotiations via Real-Time Bidding (RTB) for publishing ads on web pages. The TCF specification describes the format (called DaisyBit) which contains the list of user's consent to a specific predefined list of purposes and controllers/recipients. The IAB maintains a list of participating organisations (called vendors) within the advertising ecosystems which are then permitted to collect and utilise data and consent for purposes such as analytics, marketing, running ad campaigns, and utilising profiling and serving personalised ads based on it.

It is tempting to accommodate such a large infrastructure of consent (both in terms of scale of operations and the number of individuals involved) within the specifications and standards for recording consent. However, it is essential to understand that there have been serious doubts about the legality of these operations[9][10][11][12], and their influence in collecting consent through Consent Management Providers (CMP) that utilise malpractices such as dark patterns[13][14]. Simultaneously, the TCF works on a predefined list of purposes and controllers, which significantly affects the representation of consent in technical form, for example by reducing the amount of information required to represent consent given for purposes as binary bits (yes/no).

Therefore, while a consent receipt can be generated based on the TCF specification and its use for a specific use-case such as a website, the specification of the receipt itself is required to support a broader and more comprehensive set of information for compliance, transparency, and accountability for all stakeholders involved.

---

[8] https://iabeurope.eu/tcf-2-0/

[9] Fouad, I., Santos, C., Kassar, F. A., Bielova, N., & Calzavara, S. (2020). On Compliance of Cookie Purposes with the Purpose Specification Principle. *IWPE*, 9.

[10] Matte, C., Bielova, N., & Santos, C. (2020). Do Cookie Banners Respect my Choice? *41st IEEE Symposium on Security and Privacy*, 19. http://www-sop.inria.fr/members/Nataliia.Bielova/papers/Matt-etal-20-SP.pdf

[11] Matte, C., Santos, C., & Bielova, N. (2020, October 1). *Purposes in IAB Europe's TCF: Which legal basis and how are they used by advertisers?* Annual Privacy Forum (APF 2020). https://hal.inria.fr/hal-02566891

[12] Santos, C., Bielova, N., & Matte, C. (2020). Are cookie banners indeed compliant with the law? Deciphering EU legal requirements on consent and technical means to verify compliance of cookie banners. *Technology and Regulation*, 91–135. https://doi.org/10/ghtr3n

[13] Gray, C. M., Santos, C., Bielova, N., Toth, M., & Clifford, D. (2021). *Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective*. 18.

[14] Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed Consent: Studying GDPR Consent Notices in the Field. *ACM SIGSAC Conference on Computer and Communications Security (CCS'19)*, 18. https://arxiv.org/abs/1909.02638

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

3.5. Representations of Consent

The representation of information associated with consent in both human-readable and machine-readable forms has seen explorations within both academia and industry. While efforts such as IAB and its TCF are focused on the industry use-cases, academia generally focuses more on research and compliance as its focus. Within these, some approaches offer helpful designs and considerations that have influenced the work conducted within the PaE:CG project, and are listed in this section. For a more general perspective on the role of semantics (and semantic web) and the different perspectives on 'implementing consent', refer to our survey paper[15].

GConsent

GConsent[16] is a semantic web (OWL2) ontology for representing consent based on requirements of complying with the GDPR. It models concepts based on the notion of 'consent lifecycle' which considers consent as an artefact that has a state and attributes, and which can be stored and managed in an information system. This perspective is based on the utilisation of 'consent management' technologies by controllers, as well as its implications for individuals in terms of managing their own consent.

Along with modelling information associated with consent, GConsent also provides an exploration of recording the 'provenance' of consent in terms of how it was obtained through activities and expressing the relationship between activities and artefacts used in the process. It provides a list of 'competency questions' which form the basis of investigation for determining which information is needed and how it should be expressed as fields.

In terms of information, GConsent provides modelling of location, time, context, expiry, medium, controllers, data subjects, minors (child), third parties, delegations (e.g. parent for a child), and status. The notion of 'status' in particular is of interest as it outlines the difference between various concepts associated with the lifecycle and state of consent. Of these, GConsent defines 'explicitly given', 'given by delegation' and 'implicitly given' as states where consent is considered valid for processing. Other states where consent is not considered valid for processing are expired, invalidated, not given, refused, requested, unknown, and withdrawn.

SPECIAL

SPECIAL (Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance)[17] was an European H2020 project that utilised semantic web technologies to define a specification for consent representation in the form of policies, and a compliance checker that verified compatibility

[15] Kurteva, A., Chhetri, T., Pandit, H. J., & Fensel, A. (2021). Consent through the lens of semantics: State of the art survey and best practices. *Semantic Web Journal*. (in-press) https://hdl.handle.net/2262/96593

[16] Pandit, H. J., Debruyne, C., O'Sullivan, D., & Lewis, D. (2019). GConsent—A Consent Ontology Based on the GDPR. In P. Hitzler, M. Fernández, K. Janowicz, A. Zaveri, A. J. G. Gray, V. Lopez, A. Haller, & K. Hammar (Eds.), *The Semantic Web* (pp. 270–282). Springer International Publishing. https://w3id.org/GConsent

[17] https://specialprivacy.ercim.eu/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

between an individual's and controller's policies for utilising valid consent. Its applications also explored visual interfaces for specifying information and choices in relation to consent, and consent for IoT within smart cities.

The 'base' policy in SPECIAL consists of specifying personal data categories, processing operations, their purposes, recipients, and storage limitations such as temporal (duration or interval) or geographical. Information about policies and their provenance is recorded in a distributed ledger for compliance demonstration and validation purposes. The concepts utilised within the policy were defined as a controlled vocabulary within the SPECIAL project based on the use-cases developed along with their industrial partners.

SPECIAL's semantic reasoner offers a performant and fast mechanism for comparing two policies (user and controller) and determining whether they are compatible (controller's policy is permitted under the user's), which it then uses to enforce, validate, and demonstrate that consent is being utilised in the correct form and manner. Its logs incorporate consent revocation or withdrawal to prevent further use of consent in processing.

DUO

The Data Use Ontology (DUO)[18] offers a way to annotate genomic and medical/health datasets with conditions for reusing the data. The annotations are defined using semantic web and consist of both permissions as well as prohibitions. While DUO itself does not specify application towards GDPR compliance, it provides a way for indicating control of data (re-)use based on the consent of the individual(s). For this, it uses 'consent codes' which specify restrictions based on types of research studies, recipients (e.g non-profits only), publication requirements, ethical approval needed, time limits, and many others.

It is interesting to note that while legal frameworks do not provide any such ability to restrict the kind of data sharing, there are use-cases and a clear demand to specify them with the usefulness of consent in letting the individual determine how they wish their data to be (re-)used.

P3P

Platform for Privacy Preferences (P3P)[19] is an obsolete specification for enabling websites to declare policies regarding their intended use of personal data that they would obtain from users. P3P permits users and websites to declare their respective policies and compare them for compatibility when a user visits a website. If they do not match, the user is asked if they wish to still continue to visit and use the website. This can include purposes and preferences for what kinds of cookies must be stored.

The information possible to be expressed through preferences includes the categories of personal data and whether they are identifying or not (PII), how this data would be used (e.g. tracking, personalisation), recipients, storage duration and whether the user can access the stored information. The P3P policy is expressed using XML or can be compacted and utilised in HTTP headers.

[18] https://github.com/EBISPOT/DUO
[19] https://www.w3.org/P3P/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

While P3P seems much needed today, when it was developed and brought to fruition as a standard under the W3C umbrella, it failed to gain traction and adoption, and consequently was rendered obsolete. The development and failure of P3P[20] offers an insight into future development of privacy preference specifications and processes, including consent.

DPV

The Data Privacy Vocabulary (DPV)[21][22] is an ongoing effort by the Data Privacy Vocabularies and Controls Community Group (DPVCG)[23] for representing information about personal data handling based on legal requirements such as those for GDPR compliance but with the intention of providing a generic vocabulary. DPV reflects a community consensus in its representation of information regarding data protection and personal data processing.

The 'base' or 'core' vocabulary within the DPV consists of personal data categories, purposes and processing activities, data controllers, data subjects, recipients, legal bases, technical and organisational measures, risks and their mitigations, and rights. DPV expands on each of these concepts in a modular top-down fashion by providing top-level abstractions in the form of taxonomies. For example, it provides distinction between different categories of purposes in the form of where their intended usage is, such as for research and development, fulfilling legal obligation, personalisation, and so on.

The development of DPV provides an important artefact in exploring the different categories of information possible to be expressed across use-cases, and the necessity of providing an upper-level framework for consolidating concepts as a taxonomy. It enables interoperability and commonality in the expression of purposes and other legal concepts, which is important when there are different stakeholders involved in the functioning of both data processing and consent. At the same time, it also provides a way to extend and specialise a concept for a particular use-case, such as specifying the 'type' of personalisation being offered.

As consent records and receipts are developed into a full fledged tool for both individuals and organisations, the role of such interoperable vocabularies will be crucial in providing use of the declared information without friction.

[20] Schwartz, A. (2009). Looking back at P3P: Lessons for the future. *Center for Democracy & Technology, Https://Www. Cdt. Org/Files/Pdfs/P3P_Retro_Final_0. Pdf*.
[21] https://w3.org/ns/dpv
[22] Pandit, H. J., Polleres, A., Bos, B., Brennan, R., Bruegger, B., Ekaputra, F. J., Fernández, J. D., Hamed, R. G., Lizar, M., Schlehahn, E., Steyskal, S., & Wenning, R. (2019). Creating A Vocabulary for Data Privacy. *The 18th International Conference on Ontologies, DataBases, and Applications of Semantics (ODBASE2019)*, 17. https://doi.org/10/ggwx7x
[23] https://www.w3.org/community/dpvcg/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

4. Information and Fields for Consent Records

4.1. Consent Record / Receipt

These fields provide information about the record or receipt rather than about the consent itself. Though each field can be used for either the record (information that is maintained) or a receipt (a record that is issued), for brevity only the 'receipt' fields are mentioned here.

1. **Receipt ID** – provides an identifier for the receipt. The format and specific requirements for identifiers may change with the use-case and domain.
2. **Receipt Schema** – provides a way to specify and refer to the 'schema' of the receipt. In this case, a 'receipt schema' refers to the collection of fields, guidelines on their specification, and constraints on the information that can be used. Schemas provide a way to update the receipt in the future while offering backwards compatibility and allows the use of 'extensions' that can incorporate changes or additional information required in jurisdictions or for use-cases. In this manner, a 'global consent receipt schema' can provide the basis for common interoperable receipt data to be exchanged, while its extensions can provide additional fields required in use-cases and jurisdictions.
3. **Receipt Timestamp** – provides a way to specify when the receipt was generated. It is necessary to distinguish the receipt timestamp from the 'consent timestamp' as receipts can be generated interpedently from consent records and instances.
4. **Receipt Generated By** – refers to the entity that generated the receipt. The use of 'entity' in this case refers to a legal entity rather than an agent or a tool that was used. It is necessary to encode information about the entity for accountability and trustworthiness.
5. **Receipt Generation Method** – refers to the method that generated the receipt. This information may be of interest to record how the receipt was generated in the context of its provision. For example, receipts may be generated by a specific algorithm, tool/software, or registry.
6. **Receipt Generation Reason** – refers to the 'reason' the receipt was generated. This information may be of interest to record the context behind receipt generation, such as user request, or compliance audit.
7. **Receipt Provision Location** – refers to the 'location' the receipt was provided at. Here, location can refer to the specific URL, website, page, email, or device such as the user's smartphone. Recording information about receipt provision may be of interest regarding fulfilling obligations for providing information to the individual.
8. **Receipt Provision Format** – refers to the 'format' of the receipt, which can be machine-readable or human-readable, such as JSON, PDF, text.
9. **Receipt Language** – refers to the 'language' the information within the receipt is provided in. This refers to language, such as 'English', intended for human readability rather than machine languages.
10. **Receipt Encoding** – refers to the 'encoding' of text within the receipt. This information is required in order to correctly interpret the information within the receipt.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

11. **Receipt Signature** – refers to the 'cryptographic signature' denoting an entity has 'signed' the receipt. This information is of interest for accountability and trustworthiness as it allows a controller to authoritatively denote a receipt as a copy of its own consent record, as well as the data subject to specify their acceptance of the receipt. In addition, signatures also enable other entities, such as witnesses and notaries, to participate in the process.
12. **Receipt Signing Entity Identity** – refers to the identity of the entity that has signed the receipt.
13. **Receipt Signing Entity Role** – refers to the 'role' of the entity. For example, as data controller, data subject, auditor, witness or notary.
14. **Receipt Signing Algorithm** – refers to the specific algorithm of the signature, such as RSA. This information is required in order to utilise and verify the signature.
15. **Receipt Checksum** – refers to the data representing 'integrity' of information within the receipt. This field can be used to ensure that the information within the receipt is correct and has not been corrupted.
16. **Receipt Checksum Format** – refers to the 'format' of the checksum, which is required to utilise and verify the checksum.
17. **Receipt Replaced** – refers to whether this receipt is intended to 'replace' another previously provided receipt. References to other receipts can be made by quoting their identifiers. This can be useful when information in a receipt is changed or updated, or the previous receipt is no longer usable for any reason. Whether the replacement is intended to invalidate the previous receipt depends on the specific implementation and interpretations of a receipt management process.
18. **Related Receipts** – refers to other 'related' or 'companion' receipts. References to other receipts can be made by quoting their identifiers. This enables linking receipts that share a connection or context together, such as when multiple receipts are generated within the same 'transaction' but are provided separately, or when information within the receipts is intended to be usable independently from others. An example of where this can prove useful is when receipts are generated to represent single instances of consent from a process where the individual sets some preferences, and each preference is assumed to be an independently usable and revocable instance of consent.

4.2. Entities

An 'entity' refers to the concept as defined within law to refer to data controllers, data processors, data subjects, recipients, and so on. Information about entities is essential to the context and understanding in a receipt. Given that entities largely share the same set of information (e.g., name, address, identifier), the consent receipt benefits from abstracting these information fields to be applicable to any entity defined within the receipt.

1. **Entity Name** – refers to the 'legal name' of the entity.
2. **Entity Role** – refers to the 'type' of entity, such as data controller, data processor, data subject, and so on.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

3. **Entity Identifier** – an identifier by which the entity can be uniquely referenced. This can be the company registration number or account identifier for individuals.
4. **Entity URL** – an URL or website for the entity. For companies, this can be used to refer to where additional information about the entity can be found. For individuals, this can be used to refer to the URL of their account or identity within the controller's systems.
5. **Entity Address** – refers to the physical geographical location or 'address' for the entity. For companies, this is their location of registration as a legal entity. This information is necessary for understanding and evaluating legal jurisdiction and its associated obligations and compliance such as in case of rights.
6. **Entity Contact** – refers to the contact or communication point for the entity. It is important to note that in the current times, conventional communication mediums such as telephones or even emails are not the norm. An entity may offer communication via other means depending on the context and usefulness of a service, such as providing an option to contact them via social media accounts or through a service provided on their own website or product. Therefore, the contact information for an entity should be open-ended in that it can specify the 'type' of contact in addition to its value, for example as "telephone – 000-xyz", or as "Twitter - @twitter".
7. **Entity Policies** – refers to the 'policy' documents provided or declared by the entity. For companies (but perhaps also for individuals) this can be used to denote their privacy policy. It is of interest to note that a 'privacy policy' is not the only kind of policy document that may be of relevance and thus need to be recorded. Depending on the context, the receipt may benefit from recording other documents such as terms and conditions (as a form of contract), ethical policies, responsible use policies, guidelines, and even an AI policy given the topicality of its perceived impact and potential for harm. For these reasons, such policies must be specified in terms of their 'type' (e.g. privacy policy) and their location (e.g. a URL). Given that policies can change and evolve with time, it is necessary to specify its location as referring to the specific version at that point in time. For similar reasons, a policy document may also be accompanied along with its checksum to ensure its contents have not changed since the receipt has been issued.
8. **Entity Public Key** – refers to the 'cryptographic key' whose information is publicly available and can be used to verify the entity's identity and that entity's signatures. The 'public key' information must be accompanied along with the type or method of key for correctly interpreting and using it.

4.3. Notice and Consent Request

1. **Notice Provision by Entity** – refers to the entity that provided the notice. Given that there can be multiple entities involved in the processing of personal data (i.e. as data controller as well as data

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

processors), it is important to declare the entity that fulfilled the obligation of notice provision to the individual.

2. **Notice Identifier** – refers to an identifier for uniquely referring to the notice. This provides a way to refer to the notice in isolation without including the individual's choices and consent. Where notices are provided to categories of individuals, such as all users or a service or visitors to a website, such common identifiers aid in assessing the notice for adherence to valid consent requirements. The identifier for a notice can be an URL if the notice is intended to be preserved and provided at that URL.
3. **Notice Version** – refers to the specific 'version' of a notice. This information is of relevance when it is necessary to refer to different 'versions' of a notice, such as when a notice changes its terminology, design, or is versioned based on date. This information can be part of the notice identifier where the identifier for each version of the notice is distinct and can be used to refer to that specific version.
4. **Notice Timestamp** – refers to the timestamp for when the notice was provided to the individual. Recording this timestamp is essential since the notice, which may also contain the consent request, must be provided contextually to the timing and location for an individual to make an informed decision regarding their consent.
5. **Notice Provision Method** – refers to the specific design or method used to provide the notice. For example, a popup dialogue or text.
6. **Notice Provision Location** – refers to the specific location where the notice was provided to the individual. If provided on a website, this information may refer to the URL of the page where the notice was provided rather than the domain of the website.
7. **Notice Provision Medium** – refers to the underlying 'medium' the notice is provided within. For example, the notice can be provided as HTML rendered in a web browser, as JSON data, or as an image.
8. **Notice Provision Form** – refers to the form of the information in a notice in terms of how the individual perceives and interacts with it. For example, the notice may use interactive elements to enable the individual to explore information or use graphical representations and icons to indicate information visually.
9. **Notice Language** - refers to the language the notice was provided in.
10. **Notice Checksum** – refers to a checksum provided for the notice to verify the notice has not changed since the receipt was issued. Combined with information about the notice identifier, version, and location, this can provide a high degree of accounting for notices.
11. **Notice Scope** – refers to the scope of the notice in terms of whether it refers to a consent request, provision of information to the individual, or other related matters. It is essential to specify this information since such notices serve to fulfil obligations regarding providing information as well as choice and control to the individual. It is also essential to ensure the request for consent as part of the notice was not combined with other unrelated matters which may affect the validity of consent.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

12. **Notice Content** – refers to the information provided in a notice. This information is categorised in the further sections regarding choices and decisions offered regarding consent, information about processing of personal data, risk assessments, and legal information such as jurisdictional rights and obligations. It is important to connect information presented in a notice and to distinguish it from information additionally added to the receipt from other sources. This is useful to determine the comprehension of the information by an individual before making a decision about their consent.

4.4. Choice and Decision regarding Consent

The 'choices' are possibilities offered to the individual for making decisions regarding their consent. Requirements for choices affect the validity of given consent, such as when there is no option to refuse the consent is not considered freely given and is thus invalid. While the information described in this section utilizes the concept of 'choice' and that of 'consent' as the permissive decision made by the individual, the commonly used terminology differs from this in that it considers 'consent' as the possible set of all decisions made - including that of granting consent as well as refusing it. For this reason, the section's first list describes the abstract view of how choices translate into a decision regarding consent, and then a second list considers consent as an artefact as a more relevant approach for practitioners.

1. **Type of Choices Provided** – refers to the choices provided regarding consent, conventionally in the notice. The 'choice' in this case is representative of the control exercised by the individual regarding their consent for processing of personal data. A choice therefore may have 'types' such as being permissive, prohibitive, or a combination of both (e.g. for different purposes). It is important to record information about all types provided, irrespective of whether they were chosen or not, since the validity of consent is also dependent on the choices provided. For example, where the only type of choice provided is to accept the given request, the consent is not considered valid. The 'type' of choice may also be used to indicate its 'quality', such as 'explicit action' for consent. Alternatively, the 'type' of choice can also be interpreted in the context of its use in obtaining consent, such as 'giving consent', 'refusing consent', or 'no decision'. This provides the receipt the ability to specify any decision made regarding consent, such as granting or refusing it.
2. **Label of Choices Provided** – refers to the 'label' or 'text' used to convey the choice to the individual. Along with the 'type' of choice, the 'label' used to indicate the choice is also important to record since it reflects the understanding of the individual. Labels also are essential in cases where explicit consent is needed as they are required. Labels can include phrasing such as "Agree", "Reject". Additionally, choices can be presented also a series of preferences (e.g. using checkboxes or toggles) and a combined decision can be exercised through a

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

dedicated button. Labels in such cases may have the phrasing “Accept All” and “Reject All”.

3. **Method of Exercising Choice** - refers to the action or method used to indicate or exercise the choice. For example, the ‘method’ for a choice that is described using text can be said to be a ‘button’ where the action of clicking that button is used to indicate selection of choice. The terms used to indicate such methods can refer to commonly used design terminology such as radio buttons, checkboxes, or dropdowns. Recording this information is essential to determine the ‘action’ used to signal a decision made regarding consent.
4. **Selected Choice(s)** - refers to the choices selected by the individual which then imply the decision they made. For example, when the choice indicated by the button ‘I agree’ is selected, it implies that the individual has granted their consent through this action. It is essential to specify which of the offered choices was selected since it forms the basis for interpreting decisions made regarding consent. There may be more than one selected choice based on the design of the notice and consent requesting interface, such as multiple checkboxes for selection of conditions.
5. **Choice selection timestamp** - refers to the timestamp when that choice was selected. Is representative of the timestamp of decisions made. When the decision is granting consent, it is the timestamp for that consent instance.
6. **Who made the choice** - refers to the entity that made the choice. The entity making the choice may be different from the individual or data subject the consent is representative of. For example, a parent or guardian may make the decision on behalf of a child. When the decision is made by the data subject themselves, this information is generally omitted since it refers to the self.
7. **Relationship of individual that made the choice with the data subject** - refers to the role of relationship between the individual that made the choice and that of the data subject. In above, the role of being a ‘parent’ is the justification for why they can make a decision on behalf of the data subject is a child. This information is essential when decisions are made by an individual that is not the data subject.
8. **Choice duration or expiry** - refers to the temporal duration or condition until which the choice is considered to be enforced. The controller may decide to ‘renew’ or ‘refresh’ the choice or provide an opportunity to change it after this period. For example, when the individual has chosen to grant their consent, the duration or expiry of this ‘choice’ reflects the applicability of that consent. In another example, the individual has refused to grant consent and the same duration can apply to when the controller can request it again.
9. **Choice invalidation conditions** - refers to the specific circumstances or conditions under which this choice can be deemed invalid by the controller. For example, the condition of closing an account can invalidate all prior given consent associated with that account. In this

NGI_Trust project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 825618.

case, the invalidation condition will terminate the usability of that consent regardless of its duration or expiry.

10. **Changing the choice** - refers to the ability and information about changing the choice after it has been made. The ability to 'withdraw' consent is applicable only when consent has been granted. Given that the GDPR considers it a 'right' of the data subject, information about how to change the 'choice' for granting consent can be provided here. Similarly, when the choice made is 'refusing' consent, this information can reflect how or where to grant consent instead.

As described at the start of the section, the list of information above reflects the 'choices' offered for decisions made regarding consent. Given the common use of 'consent' as referring to all these decisions, and the notion of it having a lifecycle and attributes as an artefact, the following list provides a separate interpretation of the earlier information.

1. **Consent status** - refers to state, such as given or refused.
2. **Consent type** - refers to 'quality', such as 'regular' or 'explicit'.
3. **Consent label** - refers to label of choice selected, such as 'Agree'.
4. **Consent method** - refers to method of indicating choice, such as 'clicking a button'
5. **Consent timestamp** - refers to timestamp of decision or of consent.
6. **Consent location** - refers to location of decision or of consent.
7. **Consent medium** - refers to medium of decision or of consent.
8. **Consent indicated by** - refers to the entity that indicated the decision regarding consent.
9. **Consent delegation** - where consent decision is not indicated by the individual the consent is about, it is considered a 'delegation'. Information here concerns the entity that made the decision on behalf of the individual, and their relationship with the individual.
10. **Consent expiry** - refers to the temporal duration or validity for the indicated state of consent, after which the state is no longer considered valid.
11. **Consent invalidation conditions** - refers to the conditions which can invalidate the indicated state of consent.
12. **Changing or Withdrawing consent** - refers to information regarding changing the state of consent or withdrawing given consent. Information includes the location and medium of expressing this intention as well as the information required to do so.

4.5. Jurisdiction and Legality

1. **Applicable Jurisdictions** - refers to the jurisdictions whose laws are relevant to the entities and personal data processing represented

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

within the receipt. It is essential to declare juridictions as the resulting rights, obligations, and requirements for compliance are derived from specific laws within them. Applicable jurisdictions are based on the location of controllers, data subjects, or of the service being provided. A jurisdiction may have granularity, for example: an institution, city council, country, or a supranational union such as the EU.

2. **Relevant Authorities in Jurisdiction** - refers to the information about relevant authorities within specified jurisdictions. This information is essential for dispute resolution and exercising certain rights, such as the availability of complaining to an authority.
3. **Rights provided in Jurisdiction** - refers to the information about rights provided within specified jurisdiction. The information about rights includes the specific 'type' of right - such as ability to withdraw consent, to obtain further information, a portable copy of data; who exercises that right - such as whether the data controller or data subject; and how to exercise that right - such as by contacting the controller or using a dedicated link or service. The information about a right should include the information necessary for exercising that right, such as an identifier or the perhaps even receipt itself in matters connected to specified instances of consent.

4.6. Processing of Personal Data

Information provided regarding the proposed processing of personal data plays a vital role for consent to be considered informed as well as for meeting the other conditions regarding its validity. The following fields represent the information provided to the individual regarding the processing of their personal data by means of the receipt. This information is expected to match or align closely with the information provided through the notice and consent request in order for it to be considered the same set of information. The information within a receipt may consist of additional information not provided through the notice. In such cases, the receipt can serve as a form of information provision or a notice itself.

1. **Purposes for processing of personal data** - refers to the list of purposes for which personal data is needed and is processed. The purposes must be described in an unambiguous manner and be comprehensible to the individual. Purpose descriptions may be accompanied by additional information such as their abstracted category and the specific context or service they are intended to be utilised within.
2. **Entity responsible for Purpose** - refers to the specific entity who will be responsible for carrying out the purpose. In the case of GDPR, this will be the data controller responsible for determining and executing the purpose. It is the responsibility of the controller to oversee the purposes it uses for processing personal data, and therefore this information is necessary to be recorded. Where there is only a single controller or the purposes are shared by all controllers, this information can be omitted.
3. **Personal data categories** - refers to the categories (or specific instances of personal data) required in the specified purposes.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Categories must be specified per purpose to indicate their application within the purpose, unless all purposes require the same categories of personal data.

4. **Sensitive personal data categories** - refers to whether personal data categories are considered 'sensitive'. It is important to express the sensitivity of personal data categories given their application to demand a higher level of consent action as well as for the controller to utilise more responsible approaches when processing. It is not sufficient merely to mention that processing contains sensitive categories of personal data. The specific categories themselves must also be represented. For added contextuality, a 'sensitivity' attribute may be associated with each personal data category to indicate what level of sensitivity it constitutes, such as high or low. For brevity, only (high) sensitive categories can be mentioned as such.
5. **Special categories of personal data** - Under GDPR Art.9, certain categories of personal data are considered 'special' whose processing is prohibited unless one of the specified obligations are met. Therefore, in addition to specifying whether some categories are sensitive, it is also essential to specify when such 'special' categories are involved in the processing of personal data.
6. **Identifying personal data** - refers to whether a personal data or a category of personal data is considered identifying or can be used as an identifier.
7. **Processing activities** - refers to the activities or operations constituting 'processing' of personal data as required to complete the purpose. Processing activities must be specified per purpose to indicate their application within that purpose, unless all purposes require the same activities. The specific terms used to indicate processing activities and their interpretation is dependent on laws in specific jurisdiction. For example, GDPR defines a list of activities as 'processing' in Art.4-2, while the CCPA defines 'sell' as a processing activity which is inconsistent with the list in GDPR. While collection, storage, and sharing / transfer are types of processing activities, they are given additional focus due to their relevance in understanding use of personal data as well as the existence of additional obligations specific to their implementation. Therefore, apart from these, information about other forms of processing activities must also be provided - refer to list of activities under GDPR Art.4-2 for examples.
8. **Processor employed for activity** - refers to an entity performing specified processing of personal data on instructions of the controller. Processors may be declared contextually for specific processing activities, such as for collection or storage of data.
9. **Data Collection** - refers to the collection of personal data. Contains the following information which may be independently applicable for separate categories of personal data.
    a. **Source** - refers to source as an entity or location of data collection. For example, data can be collected from devices, provided directly by the individual.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

   b. **Source Type** - Information about collection also includes whether it was obtained directly from the individual, or indirectly obtained by observation, derivation, or inference, or obtained from a third party. In this, observation refers to data being 'observed' through the actions or activities of the individual - such as for mouse movements or keystrokes; 'derived' refers to the data being transformed or extracted from another - such as deriving first name from full name; and 'inference' refers to data being 'inferred' from some other data (as distinct from merely extracting it) - such as guessing age from text.
   c. **Frequency** - refers to frequency of data collection.
   d. **Duration** - refers to duration of data collection. Is not the same as duration of processing or duration of data storage.
   e. **Data Collecting Entity** - refers to the entity that collects data. For example, a processor may collect data on behalf of the controller, or a controller may collect data before sharing it with other controllers.
10. **Data Storage** - refers to the storage of personal data. Contains the following information which may be independently applicable for separate categories of personal data.
   a. **Storage location** - refers to the geographical location where data is stored. Where data is stored outside a jurisdiction, certain additional obligations may become applicable. For GDPR, this implies transfer of data, and in the case of third countries it needs to be specified alongside additional safeguards and measures for data protection.
   b. **Storage location type** - Location may also refer to contextual locations such as - 'stored locally' referring to web browsers or devices, or 'cloud' referring to 'servers'.
   c. **Storage duration** - refers to the temporal duration of the storage. It is implied that after this duration the data will be removed or erased in a secure manner.
   d. **Storage deletion policy** - refers to the policy under which data is erased. Policy may outline aspects such as anonymisation prior to deletion.
   e. **Storage security** - refers to the specific technical and organisational measures utilised to protect stored data. For example, use of encryption or access control to limit use.
   f. **Data storing entity** - refers to the entity that stores data. For example, a processor may store data on behalf of the controller, or a controller may store data after obtaining it from elsewhere.
11. **Data Sharing** - refers to sharing or 'disclosure' of personal data to entities other than data controller, data processor, and data subject. Contains the following information which may be independently applicable for separate categories of personal data.
   a. **Data Recipient** - refers to the recipient of personal data following a data sharing activity.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

b. **Data Recipient Role** - refers to the 'role' or 'type' of entity in obtaining that personal data. For example, recipients are third parties who are companies, or legal authorities, or recipients may be processors receiving data on instructions from the controller. Generally, processors are not considered (third party) recipients.
c. **Data Recipient location** - refers to the geographical location of the entity receiving data. Recording this information is essential as it can imply data transfers outside the applicable jurisdiction, following which additional obligations may apply.
d. **Data Sharing Entity** - refers to the entity that shared data.
e. **Data Sharing frequency** - refers to frequency of data sharing.
f. **Data Sharing Method** - refers to the method in which data is shared. Methods may include specific forms of activities or operations, such as direct transfers, post, APIs.
g. **Data Sharing Security** - refers to the specific technical and organisational measures used to secure the data while it is being shared or transferred. For example: encryption, access control, integrity checking.

12. **Data Transfer** - refers to 'transfer' of data to another entity, storage location, or other operations where data is transferred. Contains the following information which may be independently applicable for specific instances of purposes, processing activities or categories of personal data.
    a. **Data Transfer Location** - refers to the geographic location to where data is being transferred or is transmitted through. Identifying this information is necessary given the additional obligations when data is transferred outside jurisdictions.
    b. **Data Transfer Frequency** - refers to frequency of transfers.
    c. **Data Transfer Method** - refers to the method or process of transferring data. Methods can include information about underlying technologies, protocols, tools and software used.
    d. **Data Transfer Security** - refers to the specific technical and organisational measures used to protect data while it is being transferred. For example: encryption, secure protocols.
    e. **Data Transferring Entity** - refers to the entity which actually transfers or transmits data.
    f. **Data Transfer Recipient** - refers to the entity which 'receives' data after transfer. This information may be relevant given that a controller or processor may transfer data between themselves, where this information is not covered by listing (third party) recipients of personal data. Information about entities between whom data is being transferred is essential to evaluate obligations regarding its safety and protection.

4.7. Risk Assessment

The notion of 'risk' relates to those outlined in the obligations in GDPR regarding the protection of personal data as well as regarding impact to the individual. The

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

following fields relate to specific situations or conditions where GDPR necessitates additional requirements and obligations to be considered:

1. **Transferring data outside jurisdiction** - Assessing whether such risks apply require information on whether data is being transferred across 'third countries' which need additional analysis to ensure relevant protections are in place. The information from earlier fields regarding data sharing and data transfers is therefore relevant here. Where such data transfers occur, information about adequacy decisions, safeguards, or assessments may need to be provided.
2. **Automated decision making** - Where processing involves use of automated decision making, information about the system as well as its perceived impact to the individual may need to be provided.
3. **Processing at large scales** - Where processing takes place at large scales, where scale can be defined as number of data subjects, scope of personal data being processed, scale in terms of amount of data processed, or geographic spread of data subjects and processing - there may be additional obligations to consider in terms of risks and impact assessments.
4. **Use of Monitoring and Profiling** - These types of processing activities require information about their use and impact to be provided to the data subject. Additionally, their existence may trigger application of obligations and rights.
5. **Novel or uncertain use of technologies** - Where a new technology is utilised, or existing technologies are utilised in novel or uncertain ways, information about their existence and use needs to be provided. Such use-cases have obligations regarding assessment of risks and mitigations which must be met.
6. **Scoring and Measurement** - Where processing is intended to produce 'scores' or 'measurement' of individuals, this carries additional responsibilities similar to profiling. Therefore their existence and use needs to be recorded for impact assessments.

The following fields relate to a general assessment of risks and mitigations, which can be associated with any other field or information.

1. **Risks** - information about applicable risks
2. **Likelihood** - how likely is the risk to happen
3. **Impact** - impact of risk materialising
4. **Severity** - severity of impact
5. **Mitigations** - mitigation measures enforced to stop or reduce the impact of specified risks

4.8. Standards, Signals, Measures

The receipt may specify information about use of standards, signals, or measures to convey information about existence of procedures, frameworks, or interpretation of privacy preferences from specifications. An example of standards being used is: ISO/IEC 29184 for indicating quality of privacy notices and consent processes. An example of signals being used to indicate privacy preferences is: Do Not Track (DNT) for signalling prohibition to tracking individuals. Other signals include: Global Privacy Control (GPC) for signalling prohibition to 'sell' data as under CCPA; and Advanced Data Protection Control

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

(ADPC) to indicate preferences for consenting to specified purposes, exercising right to object, and opting out of direct marketing.

Information about such standards and signals may be specified as an acknowledgement for interpretation of consequences, or may be used to replace or influence some fields. For example, use of GPC can be an additional field with a boolean value indicating its applicability - which is interpreted to indicate prohibition from 'selling data'. Another example, use of ADPC can provide information on use of user's (purpose) preferences or recording objections.

4.9. Summary of Information and Fields

A list of possible fields based on interpreting the above information is presented below in the table. The list consists of questions involved in assessing the validity of consent, and the required 'concept of information' necessary to answer or evaluate the requirements based on that question.

Questions about Receipt	Fields
How to uniquely identify or reference this receipt?	Receipt ID
How to uniquely identify or reference the schema of this receipt?	Receipt Schema
When was this receipt generated?	Receipt Generation
Who generated this receipt?	Receipt Generating Entity
How was this receipt generated?	Receipt Generation Method
Why was this receipt generated?	Receipt Generation Timestamp
What location was this receipt generated and provided at?	Receipt Provision Location
What medium was this receipt generated and provided in?	Receipt Provision Medium
What is the language of information used by this receipt?	Receipt Language
What is the encoding of information used by this receipt?	Receipt Encoding
Is the receipt signed?	Receipt Signatures
Who has signed this receipt?	Receipt Signing Entity
What is the role of each entity that has signed this receipt?	Receipt Signing Entity Role
What is the algorithm used in the signature?	Receipt Signing Algorithm
What is the value of the signature?	Receipt Signature
What is the checksum of receipt for verification of integrity?	Receipt Checksum
What is the format of the checksum?	Receipt Checksum Format
Does this receipt replace or void another receipt?	Receipts Replaced
Is this receipt a companion to another receipt?	Relevant Receipts
Questions about Entity	
What is the (legal) name of this entity?	Entity Legal Name
What is the type of this entity?	Entity Legal Type
What is the legal (identifier) of this entity?	Entity Legal Identifier
What is the URL of this entity?	Entity URL
What is the physical address of this entity?	Entity Physical Address

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

What is the communication point for contacting this entity?	Entity Communication Point
What is the type of contact for this entity?	Communication Type
What is the value of contact for this entity?	Communication Details
What are the relevant policies for this entity?	Entity Policies
What is the URI for the policy for this entity?	Policy URI
What is the type of policy for this entity?	Policy Type
What is the version for the policy for this entity?	Policy Version
What is the checksum for this policy?	Policy Checksum
What is the public key for this entity?	Entity Public Key
What is the algorithm or type for the cryptographic public key for this entity?	Public Key Algorithm
Questions about Notice containing Consent Request	
Who provided the notice?	Notice Providing Entity
What is the identifier or URL for the notice?	Notice ID
What is the version of the notice?	Notice Version
What is the timestamp of the notice?	Notice Timestamp
What is the method used for providing the notice?	Notice Provision Method
What is the location used for providing the notice?	Notice Provision Location
What is the medium used for providing the notice?	Notice Provision Medium
What is the form of the notice?	Notice Form
What is the language used for providing the notice?	Notice Language
What is the checksum of the notice?	Notice Checksum
Was the notice associated with consent or matters other than those presented in the receipt?	Notice Provision Purposes
What information about personal data and its processing was provided?	Notice for Personal Data Processing
Questions about Choice regarding Consent	
What choices were presented in the notice?	Choices
What was the type of impact for the choice presented?	Choice Type
What was the value of label for the choice presented?	Choice Label
What was the method for indicating the choice?	Choice Indication Method
Was this the choice chosen?	Choice Indication
When was the choice chosen?	Choice Indication Timestamp
What is the location used for providing the choice?	Choice Provision Location
What is the medium used for providing the choice?	Choice Provision Medium
What is the language used for providing the choice?	Choice Provision Language
What is the form of the choice?	Choice Form
Who made this choice?	Choice Made By Entity

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

What is the relationship of the Entity that made the choice with the data subject?	Entity Relationship with Data Subject
Is there an expiry or validity duration for this choice?	Choice Validity / Duration
Is there a condition or event that invalidates this choice?	Choice Invalidation Conditions
How can this choice be changed or discarded?	Method for Changing Choice
Questions about Consent	
What is the consent decision recorded in the receipt?	Consent Decision
What is the status of consent?	Consent Status
What is the type of consent?	Consent Type
What is the label used to indicate consent?	Consent Indication Label
What is the method used to indicate consent?	Consent Indication Method
What is the timestamp for decision regarding consent?	Consent Timestamp
What is the location where decision regarding consent was made?	Consent Location
What is the medium where decision regarding consent was indicated?	Consent Medium
Who made the decision regarding consent?	Consent indicated by Entity
What was the relationship of decision making entity to individual?	Entity Relationship to Data Subject
When does this decision regarding consent expire or what is its duration?	Consent Duration
What are the conditions under which this decision regarding consent is no longer valid?	Consent Invalidation Conditions
How to change decision for consent or to withdraw it?	Method for Changing Consent or Consent Withdrawal
Questions about Jurisdiction and Legality	
What are the jurisdictions applicable for this record?	Jurisdiction
What are the types of applicable jurisdictions for this record?	Jurisdiction Type
What are the authorities relevant for this record?	Authority
What are the rights included or provided based on jurisdictions for this record?	Rights
Who exercises the right?	Right exercised by
How to exercise the right?	Method for Exercising Right
What is the form of information required for exercising the right?	Information Required for Rights
Questions about Personal Data Handling	
What are the purposes for which consent is required?	Purpose
What is the type or category of Purpose?	Purpose Category
What is the value or label used for Purpose?	Purpose Label
Who is responsible for the Purpose?	Responsible Entity for Purpose

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

What Personal Data or Personal Data Categories are required for this purpose?	Personal Data (/Categories)
Is the personal data of sensitive or of special categories?	Sensitive or Special Category Personal Data
Is the personal data of identifying nature or is an identifier?	Identifier or Identifying Personal Data
Is the personal data inferred or derived?	Inferred / Derived Personal Data
How is the personal data collected?	Data Collection Method
Where is the personal data collected from?	Data Collection Source
What is the frequency of Personal Data collection?	Data Collection Frequency
What is the duration over which Personal Data will be collected?	Data Collection Duration
Are any processors involved in personal data collection?	Processors
How is personal data stored?	Data Storage Method
Where is the personal data stored?	Data Storage Location
How long is personal data stored for?	Data Storage Duration
What happens after data storage period expires?	Data Deletion Policy
Is data securely stored?	Data Storage, Security
Are any processors involved in personal data collection?	Processors, Data Storage Collection
What (other than collect, store, and delete) processing operations required for purpose?	Processing Activity
Who is responsible for carrying out the processing operation?	Processor
Where will the processing be carried out?	Processing Location
Will the Personal Data be shared with other recipients?	Recipients, Data Sharing
Who will be sharing the Personal Data?	Data Sharing Entity
Who will be receiving the shared Personal Data?	Recipient
What will be the frequency of sharing Personal Data?	Data Sharing Frequency
What will be the method of sharing Personal Data?	Data Sharing Method
What will be security measures involved in sharing of Personal Data?	Data Sharing, Security
Questions about Risks and Risk Management	
At any point, will the personal data move outside the stipulated jurisdictions?	Jurisdiction, Data Transfer
If personal data is moved outside stipulated jurisdiction, what are the justifications?	Jurisdictions
Does the purpose involve any automated decision making?	Automated Decision Making
Does the purpose involve processing at large scales?	Large Scale Processing
Does the purpose involve monitoring or profiling of the individual(s)?	Monitoring, Profiling
Does the purpose involve any novel or uncertain use of technologies?	Novel, Uncertain Technologies

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Does the purpose involve creation of scores or measures of the individual(s)?	Scores, Measurements
What risks are involved in the processing of personal data?	Risks
What is the likelihood of risk to happen?	Risk Likelihood
What is the severity of impact if risk does happen?	Risk Severity
What are the mitigation measures undertaken to prevent and address the risk?	Risk Mitigation Measure
What are the technical measures undertaken to safeguard the data and privacy?	Technical Measures
What are the organisational measures undertaken to safeguard the data and privacy?	Organisational Measures
Questions about Standards, Signals, Measures related to Consent/DataProtection/Privacy	
Are there any specific standards, signals, or measures indicated by the individual or their agent in connection with this record?	Signals, Standards, Measures
What is the method for providing the signal or measure?	Signal Method
What is the value of the signal or measure?	Signal Value

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

5. Vocabularies, Schemas, and Formats

5.1. Specifying information

The previous section outlined the list of information relevant for conducting investigations in the validity of the consent process as well as for producing a receipt for recording that information. Specifying this information in the form of a receipt necessitates some agreement or structuring in the form of a schema through which the information can be interpreted and retrieved back from the receipt. The challenges in this task are regarding selecting which fields to specify, given their differences in use across use-cases, jurisdictions, and perspectives.

Additionally, where this information will be retrieved from in order to generate the receipt is also unclear at the moment. By asking controllers to proactively provide this information in an explicit form is risky as it leaves ground open for potential malice and incompetence. Therefore, practicalities decide that this information must be declared in machine-readable form at the source, such as within web pages or provided upon request such as through attached policies or APIs. For this, the information from Section 4 must be interpreted as a series of fields, whose specification must be standardised for agreement and interoperability between stakeholders.

This section, thus, provides guidance on these two challenges for specification of information. The first, specifying information as a series of structured data, is tackled in Sections 5.2 and 5.3 using JSON and ontological representations respectively. The second, providing this information in readily available and machine-readable formats is tackled in Sections 5.4 and 5.5 for declarations in web pages and use of embedded semantics respectively. Following this, the next Section 6 specifies further work and dissemination of work produced in this project regarding information specification and use in web pages.

5.2. Schema and structured notation using JSON

Creating a schema for a structured notation requires certainty about which information is relevant and applicable within the perceived use-cases. For legal compliance purposes, the complete set of information is considered within scope. Additionally, legal compliance necessitates a great degree of flexibility in information specification which may not be practically feasible or desirable. For example, under strict legal interpretations, different purposes may have different personal data categories associated with each of them. At the same time, one may wish to represent purposes and personal data categories collectively by themselves to provide a simpler understanding of the activities.

A complete and ‘correct’ schema therefore may turn out to be quite complex in terms of specification and implementation. Since the goal of this project is to explore the information and corresponding representation as fields, it leaves the task of agreement on structure to standardisation activities which it disseminates this work to. For a more flexible representation of information, refer to the next section 5.3 regarding ontological notation where concepts may be associated as a network or a graph.

Below is one possible JSON representation, provided as an example of what the receipt may look like in this format.

NGI_Trust project has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No 825618.

```
{ "receipt": {
      "identifier": "XXX-XXX-XXX-XXX",
      "version": "dev-3a",
      "timestamp": "2021-01-01T00:00:00",
      "checksum": "0000FFFF9999",
      "language": "EN-GB",
      "status": "issued",
      "signatures": [
            { "entityid": "PIIC-A",
            "signature": "XXX-XXX-XXX-XXX",
            "role": "PII-Controller" },
            { "entityid": "PIIP-1",
            "signature": "XXX-XXX-XXX-XXX",
            "role": "PII-Principal" },
            { "entity": "OpenConsent",
            "signature": "XXX-XXX-XXX-XXX",
            "role": "Witness" } ],
      "revokesreceipts": [],
      "companionreceipts": [] },
 "piicontrollers": [{
      "name": "Acme Inc.",
      "localid": "PIIC-A",
      "address": "Wonderland",
      "url": "http://example.com/",
      "contact": { "phone": "000",
            "email": "acme@example.com" },
      "policies": { "privacy": "http://example.com/privacy",
            "termsconditions": "http://example.com/tandc" } }],
 "piiprincipal": {
      "localid": "PIIP-1",
      "identifiers": [{ "email": "jane@example.com" }] },
 "jurisdictions": {
      "eu": { "laws": ["gdpr"],
            "rights": { "right to object": "http://example.com/object",
            "data portability": "https://example.com/download" } },
      "california": { "laws": ["ccpa", "cpra"],
            "rights": { "do not sell": "http://example.com/opt-out-selling" } }
},
 "consent": {
```


NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

```
      "status": "given",
      "type": "non-explicit",
      "identifier": "1234-abcd-0000",
      "location": "https://example.com/",
      "timestamp": "2021-01-01T00:00:00",
      "expiry": "2022-01-01T00:00:00",
      "withdrawal": "https://example.com/withdraw",
      "signals": { "dnt": true,
            "gpc": true } },
 "purposes": [
      { "purpose": "send newsletters",
            "category": "marketing",
            "processing": {
            "operations": ["collect", "use", "store", "share"],
            "location": ["servers:EU"],
            "processors": { "Mailchimp": "http://example.com/mailchimp" }, },
            "pii": {
            "nonsensitive": ["email"],
            "source": ["website"],
            "collection": ["submitted"],
            "storage": { "location": ["servers:EU"],
                  "duration": ["2 years"] } } }
      {
            "purpose": "analyse service audience",
            "category": "marketing",
            "processing": {
            "operations": ["collect", "use", "store", "share"],
            "algorithmic": true,
            "location": ["servers:EU"],
            "processors": { "Umbrella Corp.": "http://example.com/umbrella" },
},
            "pii": {
            "nonsensitive": ["email"],
            "sensitive": ["location"],
            "source": ["device", "website"],
            "collection": ["observed", "inferred"],
            "storage": { "location": ["servers:EU"],
                  "duration": ["6 months"] } } },
      {
            "purpose": "create personalised profiling",
```


NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

```
"category": "marketing",
"thirdparties": [
{
        "name": "Umbrella Corp.",
        "address": "Racoon City",
        "url": "http://example.com/",
        "contact": { "phone": "000",
                "email": "umbrella@example.com" },
        "policies": { "privacy": "http://example.com/privacy",
                "termsconditions": "http://example.com/tandc" }, } ],
"processing": {
"operations": ["collect", "use", "store", "share"],
"algorithmic": true,
"profiling": true,
"location": ["servers:EU"], },
"pii": {
"nonsensitive": ["email"],
"sensitive": ["location"],
"source": ["device", "website"],
"collection": ["observed", "inferred"],
"storage": { "location": ["servers:EU"],
        "duration": ["6 months"] } } } ] }
```

5.3. Ontological Representations in RDF using JSON-LD

For a more expressive representation of information, ontological notations, such as those standardised using RDF are beneficial as they allow flexibility in terms of how concepts are defined and utilised with relations. JSON-LD is a JSON format used for specifying information in RDF. It permits use of such ontological notations in JSON, which is universally interpretable within the web and software contexts. Therefore, the following ontological notation can be specified using RDF and used through JSON-LD in a fairly straightforward manner. It will require standardisation of ontological representations, especially regarding the concepts and the possible correctness of its expression (e.g. as a schema).

The following table outlines one possible interpretation of the information described in Section 4 as an ontological representation. Each represents a 'competency question' investigating the conditions and information associated with the consent process, and the corresponding concepts and relationships are provided in columns next to it.

CQ	Concept	Relation	Value
Questions about Receipt			
How to uniquely identify or reference this receipt?	Receipt	id	string

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

How to uniquely identify or reference the schema of this receipt?	Receipt	version	string
When was this receipt generated?	Receipt	timestamp	ISO format
Who generated this receipt?	Receipt	by	Entity
How was this receipt generated?	Receipt	method	string
Why was this receipt generated?	Receipt	reason	string
What location was this receipt generated and provided at?	Receipt	location	string
What medium was this receipt generated and provided in?	Receipt	format	string
What is the language of information used by this receipt?	Receipt	language	ISO code
What is the encoding of information used by this receipt?	Receipt	encoding	string
Is the receipt signed?	Receipt	signature	Signature
Who has signed this receipt?	Signature	by	Entity
What is the role of each entity that has signed this receipt?	Signature	role	string
What is the algorithm used in the signature?	Signature	type	string
What is the value of the signature?	Signature	value	string
What is the checksum of receipt for verification of integrity?	Receipt	checksum	Checksum
What is the format of the checksum?	Checksum	type	string
What is the value of the checksum?	Checksum	value	sting
Does this receipt replace or void another receipt?	Receipt	replaces	Receipt
Is this receipt a companion to another receipt?	Receipt	related	Receipt
Questions about Entity			
What is the (legal) name of this entity?	Entity	name	string
What is the type of this entity?	Entity	role	string
What is the legal (identifier) of this entity?	Entity	id	string
What is the URL of this entity?	Entity	url	URI
What is the physical address of this entity?	Entity	address	string
What is the communication point for contacting this entity?	Entity	contact	Contact
What is the type of contact for this entity?	Contact	type	string
What is the value of contact for this entity?	Contact	value	string
What are the relevant policies for this entity?	Entity	policy	Policy
What is the URI for the policy for this entity?	Policy	url	string
What is the type of policy for this entity?	Policy	type	string
What is the verstion for the policy for this entity?	Policy	version	string
What is the checksum for this policy?	Policy	checksum	Checksum
What is the public key for this entity?	Entity	key	Cryptographic Key
What is the algorithm or type for the cryptographic public key for this entity?	CryptographicKey	type	string
What is the value of the cryptographic public key for this entity?	CryptographicKey	value	string

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Questions about Notice containing Consent Request			
Who provided the notice?	Notice	by	Entity
What is the identifier or URL for the notice?	Notice	id	string
What is the version of the notice?	Notice	version	string
What is the timestamp of the notice?	Notice	timestamp	ISO timestamp
What is the method used for providing the notice?	Notice	method	string
What is the location used for providing the notice?	Notice	location	string
What is the medium used for providing the notice?	Notice	medium	string
What is the form of the notice?	Notice	form	string
What is the language used for providing the notice?	Notice	language	ISO language code
What is the checksum of the notice?	Notice	checksum	Checksum
Was the notice associated with consent or matters other than those presented in the receipt?	Notice	scope	string
What information about personal data and its processing was provided?	Notice	about	PersonalData Handling
Questions about Choice regarding Consent			
What choices were presented in the notice?	Notice	choices	Choice
What was the type of impact for the choice presented?	Choice	type	string
What was the value of label for the choice presented?	Choice	label	string
What was the method for indicating the choice?	Choice	format	string
Was this the choice chosen?	Choice	selected	boolean
When was the choice chosen?	Choice	timestamp	ISO timestamp
What is the location used for providing the choice?	Choice	location	string
What is the medium used for providing the choice?	Choice	medium	string
What is the language used for providing the choice?	Choice	language	ISO language code
What is the form of the choice?	Choice	method	string
Who made this choice?	Choice	by	Entity
What is the relationship of the Entity that made the choice with the data subject?	Entity	role	string
Is there an expiry or validity duration for this choice?	Choice	expiry	string
Is there a condition or event that invalidates this choice?	Choice	invalidation	string
How can this choice be changed or discarded?	Choice	change	string
Questions about Consent			
What is the consent decision recorded in the receipt?	Receipt	consent	Consent
What is the status of consent?	Consent	status	string
What is the type of consent?	Consent	type	string
What is the label used to indicate consent?	Consent	label	string
What is the method used to indicate consent?	Consent	method	string

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

What is the timestamp for decision regarding consent?	Consent	timestamp	ISO timestamp
What is the location where decision regarding consent was made?	Consent	location	string
What is the medium where decision regarding consent was indicated?	Consent	medium	string
Who made the decision regarding consent?	Consent	by	Entity
What was the relationship of decision making entity to individual?	Entity	role	string
When does this decision regarding consent expire or what is its duration?	Consent	duration	string
What are the conditions under which this decision regarding consent is no longer valid?	Consent	invalidation	string
How to change decision for consent or to withdraw it?	Consent	withdrawal	string
Questions about Jurisdiction and Legality			
What are the types of applicable jurisdictions for this record?	Jurisdiction	type	string
What are the jurisdictions applicable for this record?	Jurisdiction	value	string
What are the authorities relevant for this record?	Jurisdiction	authority	Entity
What are the rights included or provided based on jurisdictions for this record?	Jurisdiction	rights	LegalRight
What is the type of right?	LegalRight	type	string
Who exercises the right?	LegalRight	by	Entity
How to exercise the right?	LegalRight	method	string
What is the form of information required for exercising the right?	LegalRight	format	string
Questions about Personal Data Handling			
What are the purposes for which consent is required?	PersonalDataHandling	value	Purpose
What is the type or category of Purpose?	Purpose	type	string
What is the value or label used for Purpose?	Purpose	value	string
Who is responsible for the Purpose?	Purpose	by	Entity
What Personal Data or Personal Data Categories are required for this purpose?	Purpose	personaldata	PersonalData
Is the personal data of sensitive or of special categories?	PersonalData	sensitive	boolean
Is the personal data of identifying nature or is an identifier?	PersonalData	identifying	boolean
Is the personal data inferred or derived?	PersonalData	inferred	boolean
How is the personal data collected?	PersonalData	collection	DataCollection
What is the sources of Personal Data?	DataCollection	source	string or Entity
Where is the personal data collected from?	DataCollection	collection	string
What is the frequency of Personal Data collection?	DataCollection	frequency	string

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

What is the duration over which Personal Data will be collected?	DataCollection	duration	string
Are any processors involved in personal data collection?	DataCollection	processors	Entity
How is personal data stored?	PersonalData	storage	DataStorage
Where is the personal data stored?	DataStorage	location	string
How long is personal data stored for?	DataStorage	duration	string
What happens after data storage period expires?	DataStorage	deletionpolicy	string
Is data securely stored?	DataStorage	security	string
Are any processors involved in personal data collection?	DataCollection	processors	Entity
What (other than collect, store, and delete) processing operations required for purpose?	Purpose	operations	Processing
What is the type of processing operation?	Processing	type	string
Who is responsible for carrying out the processing operation?	Processing	by	Entity
Where will the processing be carried out?	Processing	location	string
Will the Personal Data be shared with other recipients?	PersonalData	sharing	DataSharing
Who will be sharing the Personal Data?	DataSharing	by	Entity
Who will be receiving the shared Personal Data?	DataSharing	with	Entity
What will be the frequency of sharing Personal Data?	DataSharing	frequency	string
What will be the method of sharing Personal Data?	DataSharing	method	string
What will be security measures involved in sharing of Personal Data?	DataSharing	security	string
Questions about Risks and Risk Management			
At any point, will the personal data move outside the stipulated jurisdictions?	Purpose	extrajudicial	Jurisdiction
If personal data is moved outside stipulated jurisdiction, what are the justifications?	Purpose	extrajudicial_justification	string
Does the purpose involve any automated decision making?	Purpose	automateddecisionmaking	string
Does the purpose involve processing at large scales?	Purpose	largescale	string
Does the purpose involve monitoring or profiling of the individual(s)?	Purpose	profiling	string
Does the purpose involve any novel or uncertain use of technologies?	Purpose	uncertaintechnologies	string
Does the purpose involve creation of scores or measures of the individual(s)?	Purpose	scoring	string
What risks are involved in the processing of personal data?	<x> reference to any object	hasRisk	Risk
What is the type of risk?	Risk	type	string
What is the likelihood of risk to happen?	Risk	likelihood	string
What is the severity of impact if risk does happen?	Risk	severity	string
What are the mitigation measures undertaken to prevent and address the risk?	Risk	mitigation	string

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

What are the technical measures undertaken to safeguard the data and privacy?	DataCollection	technicalmeasures	string
What are the organisational measures undertaken to safeguard the data and privacy?	DataProcessing	organisational measures	string
Questions about Standards, Signals, Measures related to Consent/DataProtection/Privacy			
Are there any specific standards, signals, or measures indicated by the individual or their agent in connection with this record?	DataProcessing	signal	Signal
What is the type of the signal or measure?	Signal	type	string
What is the method for providing the signal or measure?	Signal	method	string
What is the value of the signal or measure?	Signal	value	string

5.4. Specifying information in web pages

This section describes approaches for providing the information required for generating a receipt within web pages by using machine-readable metadata based on utilising existing means available. By providing this information, the user-agent (such as the web browser) can interact and provide use of information without relying on controller-controlled functionalities for receipt generation and usage. This enables creation of user-empowering APIs, plugins, and components - as has been demonstrated by the PaE:CG project.

Providing JSON or JSON-LD data explicit via `<script>` declaration: A convenient way to provide data for receipt generation is to declare it using JSON or JSON-LD within the web page using the `<script>` element. This enables the data to be readily available and used for receipt generation without further processing (or arguably lesser parsing and processing). The use of JSON-LD (as opposed to JSON) provides more contextuality to the information, which is essential for using different variations or versions of the schema in an interoperable format. It enables declaring the vocabulary used, and permits use of additional information within the same data structure without affecting its readability. Additionally, given that data specified using JSON-LD is valid JSON, it is easier to incorporate into web-based tools and frameworks.

The specific mechanisms for how the data should be declared need to be agreed upon for consistent implementation and interpretation. The easier approach is to declare a global variable with a fixed label for containing the receipt information, such as `var __receiptData = { … };` Another approach is to utilise annotations in the `<script>` element to declare the contents as being data for use in consent receipts, such as by using `<data-*>` to declare the context or intent of information, e.g. as `<data-for="consent-receipt">` and using `<type>` to declare its format as being JSON or JSON-LD.

Specify information and location via `<meta>` declaration: The `<meta>` element provides a way to express metadata information. PaE:CG provides an example of how this can be used, i.e. using `<meta name="pisp" content="..">` to declare information about information source/location for controller specified information and for receipt generation. The meta element can be used to declare any number of concise information or links to information sources, subject to agreement on what terms to use and their interpretation.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Public repository or registry: Given that companies operating and controlling websites or participating in web interactions are public entities in that their legal identity and relevant information should be available to the public, it is possible to create and utilise a public repository or registry of this information which can be queried and utilised in the process of receipt generation. This registry can operate at different levels, such as providing variations of information for juridictions, or providing a mapping between websites and legal entities. In some countries, such a registry is facilitated by government services, such as the UK's companies house[24], which can be repurposed to provide information for other purposes such as use in receipt generation. Browsers and other user-agents can additionally make use of this information to enable the user to identify and understand the legal entity behind the website, similar to how security certificates offer a degree of reliability in communication through verified identity.

Fallback - directly providing information in an API: In situations where none of the above solutions are feasible or available, the controller can directly produce the required information through a standardised API for information request which can then be used to generate the receipt. This relies on creation, adoption, and standardisation of such an API - which is practically difficult to envision. Additionally, this also leaves the information acquisition process depending on the goodwill of the controller, who may not be in a position to provide such information due to infrastructure limitations (e.g. static hosting) or other reasons.

5.5. Semantic metadata annotations in HTML

The current practice for provision of notice and consent requests via dialogs or popups consists of the underlying HTML used consists of an overuse of elements which lack any semantic interpretation or indication of their context regarding consent. Additionally, the specific elements used to provide information and indicate choice, such as checkboxes, as well as controls used to exercise consent decisions, such as buttons, also do not have any semantic information about their involvement in the process of consent.

This section provides approaches for providing semantic markup and annotations over HTML elements to indicate the information, role, and contextual relevance within the consent process. Given that this information, expressed as valid HTML, is machine-readable, it can provide user agents and tools/software the ability to interact with them and provide users additional information, features, protections, and convenience options - including that of extracting and using this information in receipt generation.

Using <dialog> and <form> elements for notice and consent requests: The `<dialog>` element[25] provides a semantic markup for indicating a component is a dialog box or other interactive component. This can be used to represent notices instead of the more generic `<div>` element. Though it is vital to note that at this stage, the `<dialog>` element is not natively supported by all major browsers, but it can still be utilised using polyfill[26].

[24] https://www.gov.uk/government/organisations/companies-house
[25] https://developer.mozilla.org/en-US/docs/Web/HTML/Element/dialog
[26] https://github.com/GoogleChrome/dialog-polyfill

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

The `<dialog>` element, when declared by itself, only signals the existence of a dialog that must be presented to the user for interaction. In order for this element to be declared as a 'notice' consisting of a 'consent request' or a 'consent decision', additional annotations are necessary. This is possible using the `<data-*>` element which can be used as: `<data-type="consent-dialog">`. Similarly, additional `<data-*>` elements can be used to provide contextual information or its location within the web page. For example, the footer of a page usually contains information regarding privacy policies, identity of controller, and contact information - which can be referenced in the consent dialog as being relevant within its context. This will enable the agent to find relevant information without needing its duplication.

The `<form>` element is designed for containing interactive controls for submitting information from the user to the website (controller). Given that the consent request contains choices and controls that need to be interacted with by the user for indicating their decision regarding consent, the use of a `<form>` element to contain this information provides semantic information about its intended interactivity and information transmission. By placing the `<form>` element within a `<form>` element annotated as being a consent-dialog, the interpretation of which aspects of a dialog are intended to contain the interactive controls can be specified to the user-agent. The specific fields indicating the consent controls can be indicated using `<fieldset data-type="consent-request">` to demarcate the interactive decision-making elements from the rest of the notice or request.

For specifying an interactive element is intended for expressing a 'choice' or 'preference' which is consumed as a decision regarding consent, such as for a checkbox or input, an annotation to the input or element can be added as: `<input data-type="consent-choice">`.

For annotating the information required to be provided to the individual, and is within the notice, such as specific purposes related to the consent, a element with annotations using `<data-type="">` can be used to specify its role or category - such as processing, personal data, purpose, storage duration, and so on. The use of `<span>` here is for purely syntactic reasons as the data annotations need to be present within an element. The data annotations can be used with other elements such as `<p>` or `<label>` as well.

The following listings demonstrate how this approach works practically using an example of providing embedded semantic metadata within HTML elements, its use for generating a consent dialogue for provision of information and requesting consent, and the extraction of information for generation of receipt. This work is available in code format in the PAECG repository[27] with a live demo[28].

[27] https://github.com/PAECG/consent-dialogue-markup
[28] https://privacy-as-expected.org/consent-dialogue-markup/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

The first listing provides an implementation of a <dialog> element for use as a notice and for consent request.

```
Listing 1

<dialog id="consent-dialog" open data-type="consent-dialog"
data-policy="privacy-policy" data-terms="terms" data-controller="controller"
data-contact="contact" data-address="address">
	<form method="dialog" target="_self">
	<h3>Consent Request</h3>
	<fieldset data-type="consent-request">
		<details>
		<summary>
			<input id="marketing-checkbox" name="input-marketing"
type="checkbox" data-type="consent-choice">
			<label for="marketing-checkbox">Marketing</label>
		</summary>
		<p>
			We <span data-type="processing">collect</span>, <span
data-type="processing">store</span>, and <span data-type="processing"
data-context="profiling">use</span> your <span data-type="personal-data"
data-context="PII">email</span> for <span data-type="purpose">Marketing</span>.
We will store your data for <span data-type="data-storage-duration">2
years</span>.
		</p>
		</details>
	</fieldset>
	<fieldset data-type="consent-request">
		<details>
		<summary>
			<input id="analytics-checkbox" name="input-analytics"
type="checkbox" data-type="consent-choice">
			<label for="analytics-checkbox">Analytics</label>
		</summary>
		<p>
			We would like to <span data-type="processing">collect</span>
and <span data-type="processing">use</span> data about your <span
data-type="personal-data">usage of our website</span> for <span
data-type="purpose">Analytics</span> and <span data-type="purpose">Improving our
services</span>. This is carried out through <a
href="https://marketingplatform.google.com/about/analytics/"
data-type="processor">Google Analytics</a>.
		</p>
		</details>
	</fieldset>
	<fieldset>
		<details>
		<summary>Withdrawing your consent</summary>
		<p>You can withdraw your consent at any time by interacting with <a
href="/#consent-dialog" data-type="consent-withdrawal">this dialog</a>.</p>
		</details>
	</fieldset>
	<fieldset>
		<input type="submit" data-type="consent-submit" value="Submit
Choices">
	</fieldset>
	</form>
</dialog>
```

The second listing refers to the information placed commonly in a footer, whose identifiers are referenced in the dialog/notice as links for retrieving information.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

```
Listing 2

<footer>
       <p>
       <a href="/" id="controller">Acme Inc.</a>
       Address: <span id="address">Moon rocks, Luna.</span>
       Contact: <span id="contact">000-000-000</span>
       <a href="/terms" id="terms">Terms and Conditions</a>
       <a href="/privacy" id="privacy-policy">Privacy Policy</a>
       </p>
</footer>
```

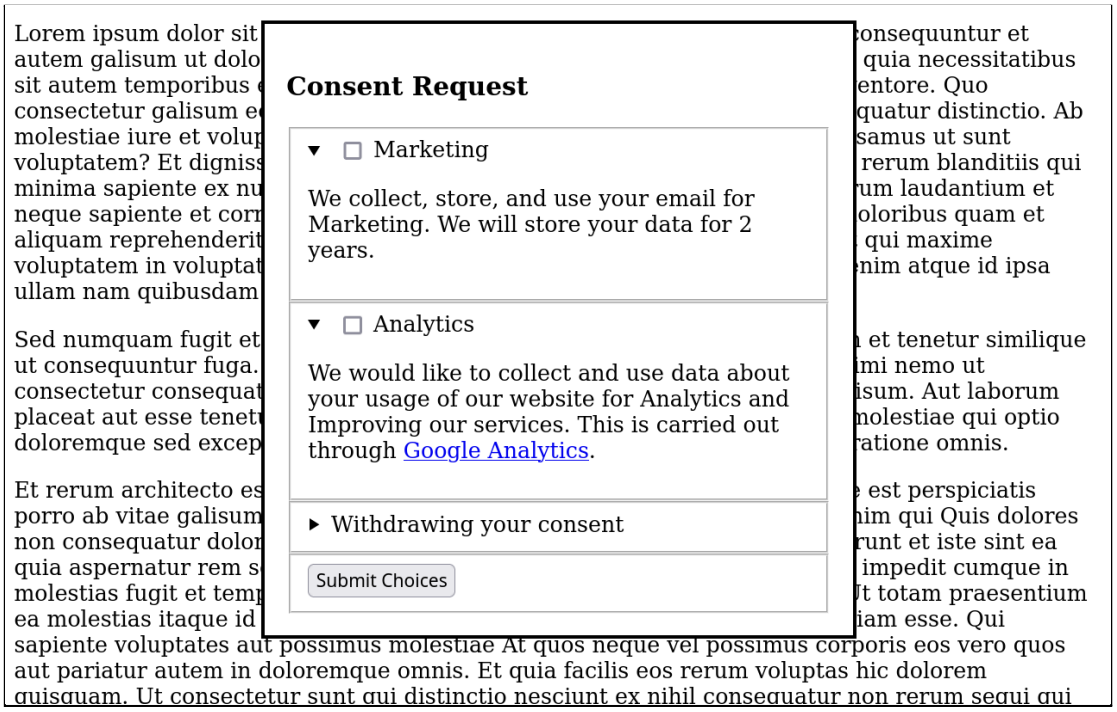
The third listing describes the functionality of extracting information from the dialog using javascript for both the notice contents as well as the user's choices. The execution of this function is triggered by a button for receipt generation, but can also be modified to be triggered for executing when the users makes a decision regarding their consent.

```
Listing 3

<button id="record" onclick="gatherReceiptData();">Generate Receipt</button>

function gatherReceiptData() {
    // retrieve metadata from page for receipt generation
    console.log("Function collects data from elements on page");
    var consent_dialog = document.querySelector("[data-type='consent-dialog']");

    // the consent map is akin to PII in existing browser addon code
    // it represents the data that is captured within a record/receipt
    // it is based on a lot of assumptions, e.g. single controller
    var consent = {
        // data common to all choices on page
        "controller": {
                                                                    "name":
document.getElementById(consent_dialog.getAttribute('data-controller')).textConte
nt,
                                                                  "contact":
document.getElementById(consent_dialog.getAttribute('data-contact')).textContent,
                                                                  "address":
document.getElementById(consent_dialog.getAttribute('data-address')).textContent,
                                                                      "url":
document.getElementById(consent_dialog.getAttribute('data-controller')).href,
                                                              "privacy_policy":
document.getElementById(consent_dialog.getAttribute('data-policy')).href,
                                                                    "terms":
document.getElementById(consent_dialog.getAttribute('data-terms')).href
        },
        "rights": {
                                                                "withdrawal":
consent_dialog.querySelector("[data-type='consent-withdrawal'").href
        },
        // instances represent each independent choice for consent
        "instances": [],
        // status of consent dialog as a whole
        // in relevance to when the record is created
        // could be first request, or given, or subsequent modification
        "status": "requested"
    };
```


NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

```
                                        var          consent_fields          =
document.querySelectorAll("[data-type='consent-request']");
    for (var fields of consent_fields) {
        var instance = {
                                                                "choice_indication":
fields.querySelector("[data-type='consent-choice']").getAttribute('type'),
                                                              "consent_value":
fields.querySelector("[data-type='consent-choice']").checked,
                                                                 "purposes":
Array.from(fields.querySelectorAll("[data-type='purpose']")).map(x              =>
x.textContent),
                                                               "processing":
Array.from(fields.querySelectorAll("[data-type='processing']")).map(x          =>
x.textContent),
                                                          "processing_conditions":
Array.from(fields.querySelectorAll("[data-type='processing'][data-context]")).map
(x => x.getAttribute("data-context")),
                                                               "personal_data":
Array.from(fields.querySelectorAll("[data-type='personal-data']")).map(x       =>
[x.textContent, x.getAttribute("data-context")]),
                                                                 "processors":
Array.from(fields.querySelectorAll("[data-type='processor']")).map(x           =>
[x.textContent, x.href]),
        };
        consent.instances.push(instance)
    }

    // represents gathered information
    console.info(consent);
}
```

The following image shows the resulting dialog and choices presented. The listing shows the data generated following the extraction of information using the above javascript function.



NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

Listing 4

```
{
  "controller": {
       "name": "Acme Inc.",
       "contact": "000-000-000",
       "address": "Moon rocks, Luna.",
       "url": "https://privacy-as-expected.org/",
       "privacy_policy": "https://privacy-as-expected.org/privacy",
       "terms": "https://privacy-as-expected.org/terms" },
  "rights": { "withdrawal": "https://privacy-as-expected.org/#consent-dialog" },
  "instances": [
       {
       "choice_indication": "checkbox",
       "consent_value": true,
       "purposes": [ "Marketing" ],
       "processing": [
       "collect",
       "store",
       "Use" ],
       "processing_conditions": [ "profiling" ],
       "personal_data": [ [  "email", "PII" ] ],
       "processors": [] },
       {
       "choice_indication": "checkbox",
       "consent_value": false,
       "purposes": [ "Analytics", "Improving our services" ],
       "processing": [ "collect", "use" ],
       "processing_conditions": [],
       "personal_data": [ [ "usage of our website", null ] ],
       "processors": [ [
            "Google Analytics",
            "https://marketingplatform.google.com/about/analytics/" ]
  ] } ],
  "status": "requested"
}
```

While the examples here used `<data-*>` elements to embed and reference information within HTML elements, it is possible to use external semantic vocabularies for expressing the information in a more flexible and interoperable manner. A good example of such information being utilised currently is through schema.org[29] which provides schemas for embedded structured data within web pages. Schema.org has been successfully utilised and popularised using its reliance by SEO efforts, and as a result is widely utilised on web pages. Schema.org relies on the use of Microdata, RDFa, or JSON-LD formats for information specification - all of which can also be used to represent information associated with receipt generation. Additionally, these formats can also be used to provide this information using other vocabularies, such as those described within state of the art.

A challenge to the utilisation of such vocabularies is the issue of interoperability and standardisation - which are difficult tasks to achieve given the dual requirements of being agreeable to both the web as well as legal communities. That said, efforts such as DPV showcase the merit and feasibility of such vocabularies being generated and utilised.

[29] https://schema.org/

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

6. Dissemination of work

6.1. This Deliverable

This deliverable represents the work conducted within the PaE:CG project regarding identification and representation of information related with consent. The dissemination level of this document is public, which enables any interested individual or party to view this document freely and without detriment. It has been made available on the project website[30] and has been deposited to Zenodo for long term availability and archival.[31]

6.2. Contributions to ISO/IEC 27560

In terms of PaE:CG, the goals of 27560 align with those of the project in that they both aim to create a specification for consent records and involve the utilisation of CRs as their basis. Given the topicality of PaE:CG's work in addressing the requirements of the GDPR, and the global abstraction intended within development of ISO standards - there is a disparity between utilising the PaE:CG work directly within ISO activities. This difference notwithstanding, several of the concepts have a corresponding overlap between the two. For those that do not, such as the GDPR-specific concept, their inclusion is implicitly of interest as providing motivation for inclusion of additional information within the receipt.

Contributions to 27560 are made by submitting comments on working drafts through national standards bodies and liaisons. As of the end of PaE:CG in July 2021, the current status of 27560 is an invitation of comments on its third working draft. This project has contributed comments to the second working draft at the end of Jan as part of NSAI (IE) and Kantara (Liason). Outputs of this project, including this deliverable, will be submitted through comments as part of NSAI (IE), BSI (UK), and Kantara (Liason) to the third working draft whose deadline for accepting submissions is in August.

6.3. Kantara Advanced Notice and Consent Receipt Working Group

This deliverable will be an input to the Advanced Notice & Consent Receipt Working Group (ANCR-WG)[32] within Kantara. The leadership of ANCR-WG consists of PaE:CG project members who will oversee the transfer of information and its utilisation within the scope of the WG. ANCR has established its aim as - "Publish a Notice and Consent Receipt Specification to address the technical gaps in the current specification and include recent standards and other technical and legal developments." with specific objectives in updating the consent receipt v1.1 and incorporating ISO/IEC 29184 requirements. This deliverable provides valuable work for both objectives.

[30] https://privacy-as-expected.org/deliverables.html
[31] https://doi.org/10.5281/zenodo.5076603
[32] https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=140804260

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

6.4. DPVCG

This deliverable will be an input to DPVCG as suggestions to improve DPV in addressing its fields for representing information about consent. More specifically, the ontological notation and legal references are of interest to the group given its overlap with the concepts in DPV. Members of PaE:CG are also active members of the DPVCG, and will initiate and oversee the contribution.

6.5. Schema.org

Currently, schema.org does not provide any concepts related to consent or even commonly used concepts such as privacy policies, controllers, terms and conditions, notices, and so on. This perhaps reflects its focus on providing concepts only of interest within SEO applications. However, PaE:CG argues that even information such as legal identity, privacy practices of a website, and the availability of this information is a matter of interest and important for search engines. This has applications beyond generation of consent receipts, such as for annotating privacy policies to enable search engines (and authorities, researchers, and machines) to extract information and answer questions for the layperson.

For this reason, PaE:CG proposes this work to form the basis for initiating discussions and suggesting concepts for inclusion in schema.org or the creation of an extension for providing legal concepts for use in web pages. The existing LegiCrowd[33] project has similar goals and provides direction for this application. LegiCrowd specifically addresses consent[34] in three types - explicit, implicit, and for minors and uses the GDPR as its source for the concepts.

6.6. Publication of Research Outputs

This work has produced or been influenced through the following publications funded by the PaE:CG project:

1. "*Comparison of notice requirements for consent between ISO/IEC 29184:2020 and GDPR*" by Harshvardhan J. Pandit and Georg Philip Krog. Published in *Journal of Data Protection & Privacy* vol.4 issue.3 (2021). https://www.henrystewartpublications.com/jdpp/v4
2. "*Crowd-sourcing Multi-Domain Issues in Consent Dialogues for Automated Generation of Legal Complaints*" by Harshvardhan J. Pandit*, Brian Lynch, and Dave Lewis. Presented at *CHI Workshop on Dark Patterns in Design: What Can CHI Do About Dark Patterns? (DarkPatterns)* - co-located with ACM Conference on Human Factors in Computing Systems (CHI 2021). https://doi.org/10.5281/zenodo.4553324
3. "*[How] Do Users Benefit From Giving Consent?*" by Harshvardhan J. Pandit, Soheil Human, and Mandan Kazzazi. Presented at *Workshop on Technology and Consumer Protection (ConPro)* - co-located with IEEE Symposium on Security and Privacy (IEEE S&P 2021) https://doi.org/10.5281/zenodo.4601141
4. "*Role of Identity, Identification, and Receipts for Consent*" by Harshvardhan J. Pandit, Vitor Jesus, Shankar Ammai, Mark Lizar, Salvatore

[33] http://www.legicrowd.org/
[34] http://www.legicrowd.org/schema/schemahierarchy.php

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

D'Agostino at *Open Identity Summit 2021 (OpenIdentity)* https://dl.gi.de/handle/20.500.12116/36495

5. "*Consent Through the Lens of Semantics: State of the Art Survey and Best Practices*" by Anelia Kurteva, Tek Raj Chhetri, Harshvardhan J. Pandit, Anna Fensel. Published in Semantic Web Journal (forthcoming, 2021). http://www.semantic-web-journal.net/content/consent-through-lens-semanticsstate-art-survey-and-best-practices

Additionally, the following publications acknowledge this project and its work as a source for funding:

1. "*Building a Data Processing Activities Catalog: Representing Heterogeneous Compliance-related Information for GDPR using DCAT-AP and DPV*" by Paul Ryan, Harshvardhan J. Pandit, Rob Brennan at International Conference on Semantic Systems (SEMANTiCS). (to be presented) paper archived at: https://hdl.handle.net/2262/96594
2. "*ODRL Profile for Expressing Consent through Granular Access Control Policies in Solid*" by Beatriz Esteves, Harshvardhan J. Pandit, Victor Rodriguez Doncel at Workshop on Consent Management in Online Services, Networks and Things (COnSeNT) - co-located with IEEE European Symposium on Security and Privacy (EuroS&P 2021). (to be presented)

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.

7. Conclusions

This deliverable has provided an exploration of information necessary for investigating whether a consent process has been valid as per legal and social requirements. For guidance, it utilised the GDPR as its source of requirements, though practicality also necessitates its application to any jurisdiction or laws given the universality of privacy and the need for accountability and transparency across borders. This is especially relevant given the prevalence and utilisation of the internet as a pervasive and ubiquitous medium of information exchange and communication.

The work represented in this deliverable is a crucial and timely work for addressing the growing importance of ensuring individuals have genuine choice and control over the 'use' of their 'self' within the changing technological advancements, and by extension their personal data as governed using their 'valid' consent. It is the hope of the author and of the members of this project that this work leads to impactful and meaningful progress within the avenues it will be read, analysed, and disseminated within.

NGI_Trust project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 825618.