Consent Through the Lens of Semantics: State of the Art Survey and Best Practices

Anelia Kurteva [a,*], Tek Raj Chhetri [a], Harshvardhan J. Pandit [b], and Anna Fensel [a]
[a] *Semantic Technology Institute (STI) Innsbruck, Department of Computer Science, University of Innsbruck, Innsbruck, Austria*
[b] *ADAPT Centre, School of Computer Science and Statistics Trinity College Dublin, Dublin, Ireland*
E-mails: anelia.kurteva@sti2.at, tekraj.chhetri@sti2.at, pandith@tcd.ie, anna.fensel@sti2.at

Editors: Michel Dumontier, Maastricht University, Netherlands; Sabrina Kirrane, Vienna University of Economics and Business, Austria; Oshani Seneviratne, Rensseler Polytechnic Institute, USA
Solicited reviews: R V Guha, Google, USA; Patricia Serrano-Alvarado, Université de Nantes, France; Allan Third, Open University, UK; James P McCusker, Rensselaer Polytechnic Institute, US

Abstract. The acceptance of the GDPR legislation in 2018 started a new technological shift towards achieving transparency. GDPR put focus on the concept of informed consent applicable for data processing, which led to an increase of the responsibilities regarding data sharing for both end users and companies. This paper presents a literature survey of existing solutions that use semantic technology for implementing consent. The main focus is on ontologies, how they are used for consent representation and for consent management in combination with other technologies such as blockchain. We also focus on visualisation solutions aimed at improving individuals' consent comprehension. Finally, based on the overviewed state of the art we propose best practices for consent implementation.

Keywords: Consent, GDPR, Semantic Web Technology, Ontology

1. Introduction

In the era of Big Data and the Internet of Things an unprecedented amount of data is being generated. According to the World Economic Forum[1], the data generated by connected devices, social networking sites, including personal information, is a new asset in modern time [1]. However, when the data consists of sensitive and personally identifiable information, depending on the way it is used, the impact on the individual and the society at large could be both positive and negative [2]. The use of the data and the potential of harm (to fundamental rights such as privacy) is the principle behind laws such as the European General Data Protection Regulation (GDPR)[2][3], which came into effect on 25th May 2018, superseding its predecessor - the Data Protection Directive (95/46/EC)[3] and the national laws transposing it.

GDPR is designed to establish lawfulness, fairness and transparency regarding personal data processing. It is also designed for purpose and storage limitation, data minimisation, maintaining integrity, confidentiality and accountability. It applies to all individuals and organisations that collect and process information related to EU citizens, regardless of their location and data storage platform [4, 5]. The fines for non-compliance with GDPR vary based on the severity of the law violations. According to GDPR the maximum fine is *"up to 20 million euro, or 4% of the firm's worldwide annual revenue from the preceding financial year, whichever amount is higher"* (Article 83).

*Corresponding author. E-mail: anelia.kurteva@sti2.at.
[1] https://www.weforum.org
[2] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[3] https://eur-lex.europa.eu/eli/dir/1995/46

In 2019 the National Commission on Informatics and Liberty (CNIL)[4] fined Google with 50 million Euro for not complying with GDPR [6]. This action has set a warning and a strong message to all the technology companies about the consequences of not complying with GDPR. In order to avoid those fines, organisations must follow the six legal basis of GDPR, amongst which is consent implementation.

GDPR 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"* (Art. 4 (11)) and has introduced additional requirements for how consent should be collected. To be specific, consent must be:

- **Freely given.** Users have the right to consent or not based on the provided information. One should not be pressured to consent (Rec. 43).
- **Specific.** Consent should be requested about specific data (Art. 7).
- **Informed.** Users are presented with information about the data controller's identity (Art. 7, Rec. 32).
- **Unambiguous.** Information should be provided in a "clear and plain" language (Rec. 42).
- **Could be withdrawn.** Users must be aware of their right to revoke consent. Further, the revocation option should be clearly stated and easily accessible. Revoking consent must be as easy as granting it from an end-user perspective (Art. 7 (3)), specifically w.r.t. the data to be processed, how it is to be used and the purpose of the processing.

The principle of consent is based on an individual's agreement towards some specified action or intention. In practice, the use of consent as a legal basis for processing of personal data involves several relevant requirements and obligations which affect the interpretation of its validity. For example, informed consent requires provision of relevant information prior to consent. GDPR, being a pan-European regulation, redefined the use and practices surrounding consent by introducing a more stringent definition of consent along with additional requirements regarding the information to be provided and documented towards compliance.

[4]https://www.cnil.fr/en/cnils-missions

In the context of GDPR, when consent is the legal basis, data processing can not begin before consent is obtained from the data subject. Any personal data processing without consent from the data subject (i.e. end-user) is liable for legal action defined by GDPR, highlighting its importance. Despite such importance of consent, to date, there is no single comprehensive collection of information describing requirements regarding consent across various relevant domains. Further, there is a lack of clarity regarding its implications in terms of legal compliance. This brings us to the questions such as how consent could be adopted in the future with the advancing use of technology without having to make many efforts, how the interpretation of privacy policies and visualisation of consent should be made and what the challenges associated with all these actions are. Therefore, there is a need for innovative consent implementation solutions that address the whole consent lifecycle (such as we have depicted in Figure 1) - from its representation, request, comprehension by users, decision-making by users (e.g. to give, to refuse, to withdraw consent) and its use (e.g. for compliance checking).

Semantic technologies, namely ontologies, have been gaining popularity in recent years due to their ability to specify and utilise relationships between entities and across domains and at large scales. Ontologies allow a better knowledge discovery, interpretability, transparency and traceability of data [7–12]. Moreover, semantic web technologies are based on open and interoperable standards such as RDF (Resource Description Framework)[5] for information representation, OWL (Web Ontology Language)[6] for representation of ontological modeling and SPARQL[7] for querying, and are extendable by design - making them suitable for application across use cases. In practice, due to the potential involvement of hundreds of organisations, consent implementation can develop into a complex ecosystem. Furthermore, the ability of semantic web technologies to model complex and dynamic ecosystems makes them suitable for consent implementation [13][14].

Otto et al. [15] present a survey of legal ontologies and approaches used in knowledge modeling. Their work helps to identify the role of various approaches for representation and legal compliance (e.g. deontic logic, symbolic logic, defeasible logic, temporal logic,

[5]https://www.w3.org/RDF/
[6]https://www.w3.org/OWL/
[7]https://www.w3.org/TR/rdf-sparql-query/

access control) along with their strengths and weaknesses. The survey [15] informs how such ontologies can be used in different contexts such as modelling of the regulation itself or information for meeting compliance objectives of regulations. Further, Otto et al. [15] show that legal ontologies have been used in legal and regulatory compliance domains for quite some time.

The research by Rodrigues et al. [16] categorises legal ontologies along dimensions of (i) organisation and structuring of information, (ii) reasoning and problem solving, (iii) semantic indexing and search, (iv) semantic integration and interoperability and (v) understanding of a domain. The research in [16] shows that there are various approaches of legal domain and compliance that are addressed by ontologies and that they also assist in other knowledge and data driven processes.

Legal ontologies are also researched by Leone et al. [17]. The work in [17] investigates legal ontologies along several criteria with the aim of assisting "generic users" and legal experts in selecting a suitable ontology. The main domains of interest here are policies, licenses, tenders & procurements, privacy (including GDPR), and cross-domain (norms, legislations). The methodology in [17] includes the development and ontology engineering process, investigating use of ontological design patterns and reuse, and the relationship of modeling and concepts with legal norms and processes.

However, potential adopters of consent implementation solutions face the difficult question of identifying appropriate existing approaches, ontologies, the aspects of consent they model in terms of GDPR requirements, technical solutions, industry requirements and benefits and the peculiarities of design they utilise. In addition, investigations into whether these approaches can be used for different practical use cases, their scalability, efficiency and potential for adoption in changing requirements within the real-world remains a challenge. With this as the background and motivation, we present a survey comprising the state of the art for the implementation of consent as defined by the GDPR with the use of semantic technology.

The main contributions of our work can be summarised as follows:

- An overview of existing solutions for the semantic representation of consent and its management related to GDPR.
- An overview of graphical consent visualisation solutions aimed at raising one's awareness regarding the implications of giving consent.
- An overview of relevant standardisation efforts.
- A set of best practices and recommendations for using semantic technology for consent representation, management and visualisation to end users.

The paper is organised as follows. Section 1 is an introduction to the topic, while Section 2 presents the followed methodology. Section 3 presents an overview of existing solutions in the fields of semantic models for consent, consent visualisation aimed at raising one's awareness, consent management and current standardisation efforts. Based on the provided literature review, best practices for consent representation with semantic technology, management and visualisation are presented in Section 4. Conclusions are presented in Section 5.

2. Methodology

To create this paper, we followed a typical methodology for doing a survey, following the key principles of systematic reviews (PRISMA)[18]. We have selected the addressed areas, as well as the principles for the overviewed papers, projects and standardisation efforts. Given the motivation for this paper, the scope of work considered is defined as implementing consent (as defined by GDPR) with semantic technology. By implementing consent, we view the processes of consent modeling, consent management and consent visualisation.

Peer-reviewed publications were the primary source of knowledge regarding approaches, and were identified using the scholarly indexing services: Google Scholar[8], IEEE Xplore[9], ACM Digital Library[10], Scopus[11], and DBLP[12]. In addition to these, information was gathered through dissemination networks such as Twitter[13] and public mailing lists, standardisation-related websites, and information portals of the research funding agencies. Searches using keywords such as *Consent Ontology, Informed Consent, Semantic Models for Consent, Consent Management Tools, Consent Visualisation, Consent Ethics, GDPR* were used to identify relevant approaches in these sources.

[8] https://scholar.google.com
[9] https://ieeexplore.ieee.org/Xplore/home.jsp
[10] https://dl.acm.org
[11] https://www.scopus.com/home.uri
[12] https://dblp.uni-trier.de
[13] https://twitter.com

Authors and affiliations of identified publications were also used as keywords to find additional relevant resources. In cases where publications acknowledged funding or projects, an effort was made to identify its online website and access the list of publications. This provided information about the project's aims and objectives, and its future goals and directions. The authors have also been participating themselves in the relevant European and nationally-funded projects, such as H2020 smashHit[14], FFG CampaNeo[15], FFG DALICC[16], and therefore had an insider view on the consent representation and modeling issues, and also found and analysed the information about the related projects on the websites of the funding agencies (European Commission, national funding agencies). Finally, relevant works at standardisation bodies have been overviewed.

In order to understand, analyse and categorise the approaches within the state of the art regarding its relation to consent, we introduce and use a model of 'consent life-cycle' (Figure 1). The consent life-cycle represents the different states and roles of information and semantics in processes associated with consent. It consists of 'Request' as the state at which information must be provided for requesting informed consent, followed by 'Comprehension' where the individual must understand and interpret the provided information. 'Decision' consists of the individual (or agent) making a decision so as to give or refuse consent. Refusing consent requires it to be requested again, whereas giving consent permits its use to process data. 'Consent Management' is responsible (in addition to managing the request and collection of consent) to check the continued validity of consent to permit its use. Consent needs to be requested again if it is: withdrawn, expired, invalidated, revoked or it needs to be: modified, confirmed, or reaffirmed.

In each of these states, requirements related to internal organisational processes as well as legal compliance affect the information and processes involved, and therefore have an impact on the information and artefacts used to execute or implement them. For example, GDPR provides obligations regarding information to be provided to the individual (Art.13), which also affect information to be provided when requesting consent. For data controllers, this information must first be identified and then used to create a notice used

[14]http://www.smashhit.eu
[15]https://projekte.ffg.at/projekt/3314668
[16]https://www.dalicc.net

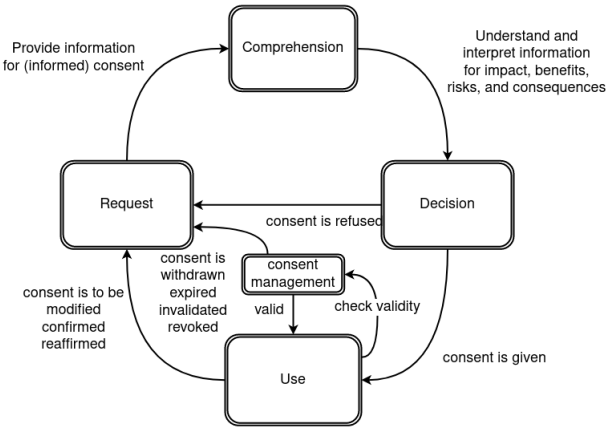

Fig. 1. Model showing life-cycle of steps for consent management

in requesting consent. GDPR also provides obligations regarding the conditions and mechanisms for how consent should be requested which determine its validity as a legal basis (Art.7, Rec.32 and Rec.43). Therefore, the management of information related to consent is important for controllers as a matter of legal compliance. For individuals, the existence and presentation of this information affects its comprehension and therefore impacts the decision regarding consent for processing their personal data. A supervisory authority investigating compliance would want to ensure that the decision made by the individual is accurately represented and used to permit or prohibit the processing of personal data (Rec.42). Such investigations therefore involve information from all states in the life-cycle and can involve multiple industries. Thus, requirements derived from the consent life-cycle span across multiple domains and converge around the use of information. The use of semantics facilitates integration and interoperability of information across states and actors.

Our overview of existing work uses this as motivation to analyse and categorise approaches across fields in terms of their relation to consent representation and management, and the potential for use of semantic technology. In particular, we consider (Section 3):

- Semantic models or ontologies for modeling information related to consent. Within this, we focus on the definition of consent as an ontological concept and other concepts and attributes that are associated with it.
- Approaches for management of information associated with consent, and its subsequent use to permit or prohibit processing.

– Approaches that aim to assist the individual regarding comprehension of information relevant to consent, with a particular focus on visualisation techniques.
– A discussion about relevant standardisation efforts.

Finally, analysing the state of the art from different angles relevant to consent representation, management and visualisation, we identify the current challenges and gaps, as well as the best practice recommendations for the consent modeling, management and visualisation, that are of benefit to the research, developer and practitioner communities. When doing so, we additionally take into account ethical and sociological aspects regarding practices surrounding consent, and its impact on individuals.

3. Overview of Related Work

This section provides an overview of related work in the areas of consent modelling, graphical visualisation of consent to end users, consent management and current standardisation efforts. We view consent representation from a semantic perspective and present semantic models for consent, namely ontologies. Next, we provide an overview of work on graphical consent visualisation to end users aimed at raising one's awareness regarding the implications of giving consent. Further, various existing and developing solutions for consent management based on semantic technology are presented. Finally, a short summary of current standards for consent is presented as well.

3.1. Semantic Models for Consent

Ontologies are some of the most essential semantic web technologies used for representing concepts and the relationships between them in both human-readable and machine-readable formats. Some of the reasons for using ontologies are: to share common understanding of the structure of information among people or software agents, to enable reuse of domain knowledge, to make domain assumptions explicit, to separate domain knowledge from operational knowledge, and to analyse domain knowledge. In the case of consent, an ontology provides a formal conceptualisation that is interpretable by the different entities involved in the data sharing process. We view a semantic model as a consent ontology, if as a minimum, the concepts of consent and its purpose are modelled.

This section provides an overview of consent ontologies by stating (i) the purpose of the ontology, (ii) language used for specification, (iii) how consent is modelled, and (iv) level of detail when modeling personal data for consent (e.g. presence of abstract or specific instances, granularity of concepts, specific taxonomies or instances, domain-specific or use case specific). Further, we used a set of competency questions (Table 1) for evaluating to what extent each ontology is capable of representing information regarding informed user consent. The competency questions were derived by following GDPR requirements for informed consent and already existing sets of competency questions such as the one of GConsent[17]. The ontologies reviewed in this section are CDMM [18], GConsent[17], PrOnto [19], LloPY [20], BPR4GDPR[23], SPL and SPLog [21], ColPri [22] and DPV[27].

3.1.1. Consent and Data Management Model (CDMM)

The CDMM[18] ontology by Fatema et al. [23] utilises a consent ontology written in OWL[6]. The ontology represents a generic model for consent, permissions and prohibitions according to the GDPR and further reuses the PROV-O[19] ontology to express provenance information from different systems [23]. CDMM allows to represent the format in which consent was retrieved such as app based, audio, online form, etc. Keeping track of changes in the state of data, consent and operations is made possible by defining the classes for time, use and action. The ontology models both personal data, such as health data, and non-personal data i.e. any data that is not sensitive according to the given consent. Further, CDMM provides classes for different data formats such as video, audio, picture, text and defines three types of processing (examine, modify and read). CDMM can be used for consent management (e.g. collecting consent, maintaining records of consent).

3.1.2. GConsent

GConsent[17], an ontology written in OWL2[20], models information about consent based on requirements of GDPR compliance [24]. It represents consent as an artefact that can have states indicating its lifecycle - such as requested, given, refused, or withdrawn. The relevant information regarding purpose, personal data

[17] http://openscience.adaptcentre.ie/ontologies/GConsent/docs/ontology
[18] http://purl.org/adaptcentre/openscience/ontologies/consent
[19] https://www.w3.org/TR/prov-o/
[20] https://www.w3.org/TR/owl2-overview/

categories, processing, and parties involved are associated with a central concept representing "consent". Novel aspects of this ontology involve modeling of the context in which consent was requested or given, such as location and medium. The ontology also provides representation of delegation regarding consent, and provides examples of its application in several use-cases. For example, GConsent can be used when modelling information (e.g consent) related to GDPR compliance.

3.1.3. Privacy Ontology (PrOnto)

The PrOnto ontology [19], written in OWL[6], is used for modelling GDPR concepts such as privacy agents, data types, types of processing operations, rights and obligations. Consent is viewed as one of the legal bases used to justify a processing activity. PrOnto models the concepts for purpose, personal data (e.g. health, genetic, ethnic, sexual data), and non-personal data (e.g. anonymous data) in its data model and associates them with a legal basis. The structure of the ontology is based on five modules: (i) documents and data, (ii) actors and roles, (iii) processes and workflow, (iv) legal rules and deontic formula, (v) purposes and legal bases. The ontology provides a significant number of concepts (for combining different ontologies and design patterns) for modelling GDPR-related concepts, but also strives to go beyond the GDPR requirements so that it could be applied in any legal scenario. For example, the ontology can be used for compliance checking during the whole lifecycle of the personal data. [19].

3.1.4. Legal Complaint Ontology to Preserve Privacy for the Internet of Things (LloPY)

The LIoPY [25] ontology, developed with OWL and aimed to be used in the Internet of Things (IoT), follows the NIST (National Institute of Standards and Technology Interagency Report)[21] privacy definition. Consent is viewed from a privacy perspective and is represented as a privacy attribute. The privacy attributes are derived based on GDPR and NISTR [26]. LloPy models the purpose for consent, retention, disclosure, operation, condition, etc. The ontology is utilised by the IoT Resource Management Module of the system presented in [25], which performs data anonymisation, noise addition, etc. In addition to modelling, consent for privacy preservation in smart devices, LloPY reuses the Semantic Sensor Network ontology (SSN)[22], which provides more detailed privacy properties for sensors and their observations. The ontology can be used when one needs to model consent for sensor data sharing in the IoT, for example, in smart cities.

3.1.5. Business Process Re-engineering and Functional Toolkit for GDPR Compliance (BPR4GDPR)

The compliance ontology developed as deliverable D3.1[23] of the BPR4GDPR[24]project aims to provide the fundamental entities, concepts and relationships that are needed for achieving compliance. The ontology was built based on project work done in the legal and technical fields and has a hierarchical data type structure, which allows for the detailed organisation of entities and interrelations. Amongst the core concepts in the ontology are roles, event types, context types and state types. Further, the ontology models the concept of a purpose, which is a GPDR requirement for informed user consent. Having such diversity of data types allows to define consent in detail and a precise compliance check to be performed. The ontology can be used for modelling consent as an access control for compliance checking. Full specification of the Compliance Ontology is available in Deliverable D3.1[23] of the BPR4GDPR project.

3.1.6. SPECIAL's Usage Policy Language (SPL)

The SPECIAL's Usage Policy Language (SPL) [21], developed for the SPECIAL-K compliance platform, is a language for modeling usage policies. SPL encodes the usage policies in OWL2. SPL models data processing, the purpose for processing, description of the operations and the involved entities. A detailed description of the SPL ontology can be found in deliverable D2.1 [27]. The SPL's scope is limited to capturing the permissive nature of given consent in order to compare it with its processing logs to determine (and evaluate) compliance according to the given consent. However, the vocabulary also models purpose, processing, recipients, temporal duration, etc. The main aim of the language is to model data subject's consent and relevant data usage policies in a machine-readable formal way, and to define permissions based on the given consent thus allowing compliance checking and policy verification [21].

[21] https://www.nist.gov/nist-pub-series/nist-interagencyinternal-report-nistir

[22] https://www.w3.org/TR/vocab-ssn/

[23] https://www.bpr4gdpr.eu/wp-content/uploads/2019/06/D3.1-Compliance-Ontology-1.0.pdf

[24] https://www.bpr4gdpr.eu

Table 1
Consent Competency Questions

No.	Question	Relevant Concept(s)	Relevant GDPR Clause(s)
Questions about consent			
1	Who collects the data?	Data Controller, Data Processor	Art. 4 (7), Art. 6, Art. 28
2	For what purpose?	Purpose	Art. 4 (4), Art. 6 (1a, 1f, 4), Art. 7 (32)
3	How to withdraw consent?	Consent Withdrawal	Art. 17, Rec. 63, Rec. 66
4	How long does consent last for?	Consent Duration/Validity/Expiry	Rec. 32, Rec. 42
5	When was consent given/revoked?	Consent Duration/Revocation	Art. 17, Art 19
Questions about personal data			
6	What personal data is collected?	Personal Data Categories	Art. 4 (1), Art. 9
7	How is the personal data being used?	Processing	Art. 4 (2)
8	How is personal data collected?	Data Collection	Art. 12, Art. 13, Art. 14, Rec. 39, Rec. 58, Rec. 62, Rec. 73
9	With whom is personal data shared?	Recipient, Data Sharing	Art. 4 (7), Art. 6, Art. 28
10	Who is responsible for the personal data?	Data Controller	Art. 24, Rec. 74, Rec. 79
11	Where is personal data stored?	Data Storage	Art. 5
Questions about the data controller			
12	Who is the Data Controller?	Data Controller	Art. 4 (7), Art. 28
13	How to contact the Data Controller?	Data Controller, Contact Information	Art. 4 (7), Art 14, Art. 28
14	What are the responsibilities of the Data Controller?	Data Controller, Responsibilities, Obligations	Art. 4 (7), Art 14, Art. 28, Art. 37
Questions about the data subject			
15	Who is the Data Subject?	Data Subject	Art. 4 (1)
Question about third party			
16	Whom to contact?	Contact Information, Third Party	Art.12, Art. 13, Art. 14

Table 2
Overview of Existing Semantic Models for Consent

Ontology	Year of latest update	Availability	Scope	How is consent modelled/viewed?
CDMM	2017	Open-access	Data provenance	Consent is viewed as an entity within a privacy policy.
GConsent	2018	Open-access	GDPR compliance	Consent is modelled as an artefact, which has states (given, not given, refused, withdrawn).
PrOnto	2018	Private	GDPR obligations and requirements	Consent is viewed as one of the legal bases used to justify a processing activity.
LloPy	2018	Private	Privacy and security	Consent is modeled from a privacy perspective as an attribute.
BPR4GDPR	2019	Private	GDPR compliance	Consent is modeled as an event type (provided, revoked, refused).
SPL and SPLog	2019	Open-access	GDPR compliance	Consent is modelled as a policy and is used for compliance checking.
ColPri	2020	Private	Privacy policies in the IoT	Consent is modelled as a privacy policy and has two states (given and ungiven).
DPV	2021	Open-access	Privacy and legal compliance	Consent and its attributes (e.g. expiry time) are modelled as privacy policies for cases such as personal data handling and compliance checking.

Table 3
Overview of Existing Semantic Models for Consent: Classes and Properties representing Consent

Ontology	Classes	Object Properties	Relevant Consent Lifecycle Stage
CDMM	Consent, ConsentFormat, ConsentingParty, ConsentObligation	consent_given_at, consent_given_by, consent_given_for, data_has_format	Request, Comprehension, Decision, Use
GConsent	Consent, Data Subject, Personal Data, Processing, Purpose, Status, Expired, Explicitly Given, Given by Delegation, Implicitly Given, Invalidated Not Given, Refused, Requested, Unknown, Withdrawn	hasStatus, hasConsent, isActionForPurpose, isContextForConsent, isPersonalDataForConsent, isPreviousConsentFor, isPurposeForConsent, isStatusForConsent, isUpdatedConsentFor, wasProvidedConsent, atLocation, atTime, isProvidedToController	Request, Comprehension, Decision, Use
BPR4GDPR	ConsentProvided, ConsentRevoked, ConsentDenied, DataProcessor, DataSubject, DataController, DataProtectionAuthority, DataProtectionOfficer	isSensitive, isExecutive, isPartOf, contains, isOfState, hasStateValue, hasPotentialStateValue, hasStateType	Request, Decision, Comprehension, Use
SPL and SPLog	LogEntry, PolicyEntry, ConsentAssertation, ConsentRevokation	spl:hasData, spl:hasProcessing, spl:hasPurpose, spl:hasStorage, spl:hasRecipient, splog:controller, splog:revoke, splog:recipient, prov:atTime, splog:Processor	Request, Decision, Comprehension, Use
DPV	Consent, Purposes, LegalBasis, DataSubject, DataController, Right	hasConsentNotice, hasExpiry, hasExpiryCondition, hasExpiryTime, hasProvisionBy, hasProvisionByJustification, hasProvisionMethod, hasProvisionTime, hasWithdrawalTime, hasWithdrawalByJustification, hasWithdrawalMethod, hasWithdrawalTime, isExplicit	Request, Decision, Comprehension, Use

The SPLog[25] vocabulary builds upon the existing SPL by reusing existing vocabularies for data provenance such as PROV[19] and represents consent states such as revocation and assertion as types of *"PolicyEntry"*. The class *"ConsentAssertion"* defines the consent received by the data subject, while *"ConsentRevocation"* models the action of consent revocation. These two classes, being subclasses of *"PolicyEntry"*, which is also a subclass of *"LogEntry"* allow for the direct linking of consent to the data subject and vice versa. Both vocabularies can be used for modelling consent as system logs in privacy policies in order to restrict data usage and processing [21].

3.1.7. Collaborative Privacy Knowledge Management Ontology for the Internet of Things (ColPri)

The ColPri ontology [22], developed with OWL[6] and using the SKOS[26] vocabulary, aims to provide a collaborative IoT knowledge base which enables one to configure privacy policies. Consent is viewed from a privacy perspective and is modeled as a privacy attribute with two states: *given* and *ungiven*. The purpose of consent is defined as either *Advertising* or *"ApplicationFunctioning"*. Further, the ontology allows one to specify if information disclosure to entities such as developers and third parties is allowed. Regarding personal data, ColPri follows SKOS and models different data categories such as personal, pseudo anonymous and anonymous data. Personal data could be further specified as sensitive (e.g. criminal, health, habit and identity) and nonsensitive. ColPri differs from other ontologies by using both OWL and SKOS thus allowing flexible data categorisation and privacy policy handling based on user consent. The ontology can be used for modeling data privacy preferences in smart cities, specifically in smart homes.

3.1.8. Data Privacy Vocabulary (DPV)

The Data Privacy Vocabulary (DPV)[27], is an outcome and deliverable of the W3C Data Privacy Vocabulary and Controls Community Group (DPVCG)[28]. The DPVCG was formed as an activity of the SPECIAL project, and represents a broad consensus amongst experts from the domains of data protection, privacy, legal compliance, and semantic web. DPV provides a vocabulary of concepts based primarily on GDPR, along with hierarchical top-down taxonomies for specifying purposes, processing categories, personal data categories, technical and organisational measures, and GDPR's legal basis (as an extension called DPV-GDPR). The representation of consent in DPV is through the concept *Consent* along with properties enabling representing notice, expiry, provision, with-

[25] https://ai.wu.ac.at/policies/policylog/
[26] https://www.w3.org/2004/02/skos/
[27] https://w3.org/ns/dpv
[28] https://www.w3.org/community/dpvcg/

Table 4
Evaluation of the Ontologies with the Competency Questions

Question	CDMM	GConsent	BPR4GDPR	SPL and SPLog	DPV
1	✓	✓	✓	✓	✓
2	✓	✓	✓	✓	✓
3	✓	✓	✓	✓	✓
4	✓	✓	✓	✓	✓
5	✓	✓	✓	✓	
6	✓	✓	✓	✓	✓
7	✓	✓	✓	✓	✓
8	✓	✓	✓	✓	✓
9	✓	✓	✓	✓	✓
10	✓	✓	✓	✓	✓
11		✓		✓	✓
12	✓	✓	✓	✓	✓
13		✓	✓	✓	✓
14					
15	✓	✓	✓	✓	✓
16				✓	✓

drawal, and whether it is explicit. The association of purposes, processing, personal data categories and other relevant information is represented through the *PersonalDataHandling* class which associates consent as the legal basis used for a particular instance of processing. The modeling of consent within DPV is based on the requirements of GDPR for recording and documenting given consent and the *Consent Receipt* specification. DPV can be used for representing responsibilities and obligations in privacy policies and to "support automated checking of legal compliances of data handling ex ante (prior to processing), or ex post (i.e. check compliance after processing)" [27].

3.1.9. Summary

A summary of the ontologies that were discussed in this section, their scope and the way each one models consent is presented in Table 2. The specific classes and object properties used for modelling consent, for each ontology (based on resources available online) from Table 2 are presented in Table 3. Table 4 presents the evaluation of the ontologies from Section 3, with the competency questions from Table 1. A "check sign" (✓) is used if the ontology is able to answer the question (i.e. the concept is present in the ontology), and an empty space is used where concepts were not found, while acknowledging they could be added later e.g. through an update. The findings show that the existing ontologies are quite diverse based on their scopes and when it comes to their abilities to model consent.

GConsent[17], SPL [28] and BPR4GDPR[23] are aimed at modeling consent while taking into account GDPR requirements. DPV [27] also models consent (from privacy perspective), but the main focus if on GDPR as a whole. PrOnto [19], ColPri [22] and LloPY [25] are developed from a privacy perspective and view consent as an attribute that helps preserve data privacy. Similarly, CDMM[18] models consent as an entity within a privacy policy and further allows for the capturing of data provenance. From a technical standpoint, the OWL[6] standard is followed, with an exception of the ColPri ontology which further utilises the SKOS[26] organisation system. Regarding the ability to represent informed user consent, the ontologies reviewed in this section are still somewhat generic, have a specific scope (Table 2) and achieving such level of detail while being compliant with GDPR requires combining several ontologies. By far, GConsent, PrOnto and BPR4GDPR have the potential to be both GDPR compliant and to represent informed user consent in detail. In conclusion, various ontologies for consent have been developed in the past, however, common limitations are present.

3.2. Consent Visualisation

When talking about consent and its representation with semantic technology, one should also consider how it is visualised (e.g. via a user interface (UI) or graphically) to the end users in an informative way as no process can start without one's consent. However, having users' informed consent does not mean that the user understands the consequences of his or her action. The desire for convenience, fast and easy interactions may make one disregard important information regarding consent and simply agree to anything that is required without being aware of the consequences. Bechmann [29] defines this as a *"culture of blind consent"*. The issue is also addressed by Joergensen et al. [30] who examined the user's understanding of privacy policies, data control and the importance of social media as a whole. The results showed that the need to be accepted is enough to influence users to consent. Users had a general common sense of what types of information should and should not be shared online but they lacked knowledge regarding data sharing on a company level and the related privacy risks. The study validated Bechmann's point [29] that users lack knowledge about what it means to consent and that they are more concerned with how they would be perceived by others. Human Computer Interaction (HCI) [31] is a broad field by itself thus we limit the scope of this section to research and projects that focus specifically on

visualising informed user consent (via a UI) to raise one's awareness. An overview of the following UIs is presented below: Data Track [32], The Privacy Dashboard [33], CoRe [34], CURE [35].

3.2.1. Data Track

Angulo et al. [32] developed a tool for visualising data disclosures called Data Track (Figure 2). The tool's development was initially part of the European PRIME[29] and PrimeLife[30] projects and then continued as part of the A4Cloud[31] project. The motivation for the tool is to enable transparency and raise awareness regarding what is happening to one's data. Data Track's main goals are to allow users (i) to monitor how their data is being used by different online services and (ii) to exercise their rights. Monitoring of the data flow is achieved by providing users with a graphical visualisation, which the authors refer to as "trace view". The main concept of the trace view is that the user is at the center of everything thus making one feel as if the interface focuses on them. The interface itself is divided in two panels. The bottom panel allows one to view information provided to each service, while the top one displays the information currently being shared. Further, upon selecting a specific service a user is presented with a new window displaying a more detailed overview of what data is being shared and is given the possibility to edit permissions. Users deemed the interface as useful as it helped them become more aware of what is happening to their data. However, the evaluation showed that even users, who were knowledgeable about the web, lacked understanding about how their data is collected, shared and used.

3.2.2. The GDPR-compliant and Usable Privacy Dashboard

Raschke et al. [33] develop a privacy dashboard that enables users to execute their rights according to GDPR. The implementation of the user interface follows Nielsen's Usability Engineering Lifecycle [36]. The authors start by analysing the user's and the tasks they need to complete and then develop several parallel versions of the privacy dashboard. The prototype (Figure 3), namely a single page that consists of three main building blocks (general functionalities, data overview and general information), was developed with JavaScript and React. The general functionalities plane allows the user to review given consent,

[29] http://www.prime-project.eu.
[30] http://primelife.ercim.eu/.
[31] http://www.a4cloud.eu.

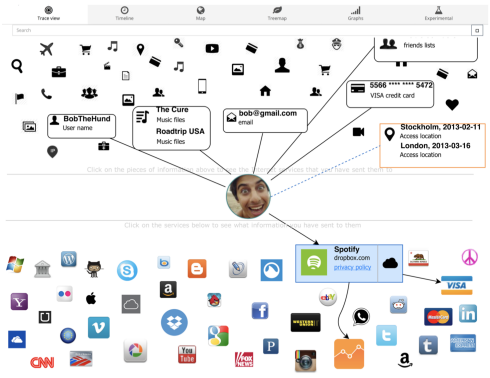

Fig. 2. The Data Track Tool by Angulo et al. [32]

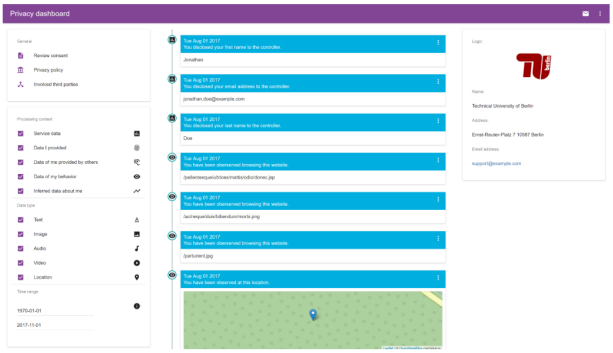

Fig. 3. The GDPR-compliant and Usable Privacy Dashboard by Rashcke et al. [33]

request information about involved entities, view privacy policies, etc., while the data overview plane visualises the data flows with the help of an interactive graph, which is implemented with the vis.js library. The general information section, located on the right-side of the dashboard, provides details about third-parties such as name and address. The privacy dashboard has proved to be useful as it made users more aware about their rights. The authors suggest that future improvements of the design to minimise information overload are needed [33].

3.2.3. The CoRe and CURE User Interfaces

Drozd and Kirrane [34][35] address consent and the challenge of its representation to end-users by developing the CoRe UI [34] (Figure 4) and its third iteration called CURE [35] (Figure 5). The CoRe UI is based on GDPR requirements and aims to minimise the issue of information overload that is present in existing solutions. As discussed there, most of the existing work is focused on developing GDPR privacy policies and not

on the representation of consent and its visualisation to the end user, thus a new methodology for achieving this is presented. The methodology is based on the Action Research (AR), which requires a problem to be defined first. Following a sample use case, several UI prototypes were developed with Angular[32] and D3.js[33] and then tested with users both remote and onsite. Regarding consent representation, the *"all or nothing"* approach is put aside and users are given full flexibility to customise their consent. The UI enables users to explore possible consent paths via a hierarchical visualisation done with D3.js and to select a specific one they wish to follow. Further, understandability is addressed by avoiding the commonly used legal jargon and instead focusing on simple sentence structure.

What differentiates the CURE UI [35](Figure 5) from other interfaces and consent forms is that it focuses on mobile device interaction and personalisation. Users have full control over their consent specification and data. In comparison to CoRe [34], that is based on the AR methodology, CURE follows the Design Science Research (DSR) paradigm, which is usually used for improving existing software [35]. The front-end was developed with Angular and D3.js, while Java[34] and PostgreSQL[35] were used on the back-end. Similarly to CoRe, the main objectives of the CURE UI are customisation, understandability and revocation. Customisation is achieved by allowing users to select what information they want to receive/share (e.g. health data) and for which purposes. In addition to using, as described, "simple" phrases, the UI provides users with feedback on demand upon each interaction in order to minimise the data overload and help understandability. Further, as in CoRe, a graphical representation of the consent process is provided. Consent revocation is done either by sliding the pointer up or by deselecting some of the options.

3.2.4. Summary

The work on the CoRe [34], CURE [35], The Privacy Dashboard [33] and the Data Track [32] UIs (see Table 5) show that visualisation helps to raise one's awareness about consent and the implications that follow. In addition, visualisation of the data helps achieve transparency, which is key for making well-informed decisions such as giving consent.

[32] https://angular.io
[33] https://d3js.org
[34] https://www.java.com
[35] https://www.postgresql.org

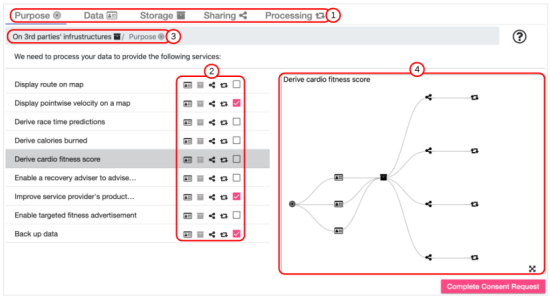

Fig. 4. The CoRe UI by Drozd and Kirrane [34]

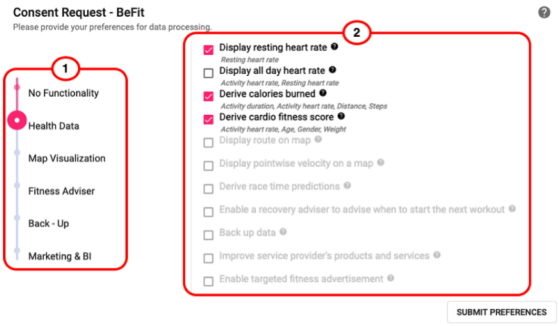

Fig. 5. The CURE UI by Drozd and Kirrane [35]

3.3. Consent Management

Having modeled consent semantically and visualised it graphically to the end user, one should next consider how to manage it. However, one can also consider or wish to manage consent without visualising it. Consent management could be viewed from both individual and system perspective, however, both are interlinked. While users must be able to perform actions such as giving and withdrawing consent at any time, the system must be able to handle them. Consent management, as defined by Pallas and Ulbricht [37], is a collection of processes that *"allow or integrate queries upon multiple and autonomous data sources, taking into account data subjects' individually given, purpose- and utilizer-specific, and dynamically adjustable consent"*. Consent management, in most cases, refers to the controller managing the state or processes associated with consent in terms of whether it has been requested and obtained for the intended purposes and processing of personal data associated with it. It also refers to the use of (given) consent as permissions or access control to control the processes based on it. From a legal compliance perspective, consent management also refers to evaluating

Table 5
Graphical Consent visualisation via a UI

Name	Year	What is visualised?	How is it visualised?
Data Track	2015	Personal data processing, user rights.	Personal data and its processing is visualised with a tracing graph on a UI.
The Privacy Dashboard	2018	Consent, data privacy rights, processing.	A UI enables the chronological and interactive graphical representation of data processing.
CoRe and CURE	2019	Consent, purpose, data, storage, processing, sharing.	Consent requests are visualised on a UI with the help of interactive graphs.

and maintaining the validity of consent and its associated processes based on obligations derived from law. The individual's perspective involves tracking what consent was given, its withdrawal for the same set of information. Evidently, the processes should be adequately designed. Such a consent management system should particularly take into account the current policies and laws that need to be followed [38]. In the context of GDPR, consent management must comply with the obligations for personal data processing that are defined in GDPR's Chapter 2 (Art. 5-11) . For example, consent management operating within the EU or dealing with EU citizens must follow GDPR directives such as "Lawfulness of processing", "Conditions for consent", etc. as described in Art. 6, Art. 7 respectively. This section describes technological solutions for consent management that assist in the storage, use, evaluation, and documentation of consent based on requirements of GDPR compliance. We begin by providing an overview of each solution by specifying its scope, main goals and the motivation behind it. Next, we provide information about how consent management is achieved, followed by possible real-world applications.

3.3.1. EnCoRe

EnCoRe[36] is a collaborative project between researchers in the UK that aims to develop a mechanism for consent revocation that could be successfully adopted by any business, and for raising awareness regarding one's rights over their personal data. Regarding the architecture of the solution, the "Personal Consent and Revocation Assistant" provides users with the opportunity to give consent or revoke consent via a user interface, which also keeps record of one's actions. Upon giving consent, the user data is sent to a virtual instance of a database called "Virtual Data Registry" and is further managed with the help of the Data Viewer and Manager component. Prohibitions, obligations and permissions are defined by the Privacy-aware Policy Enforcement, which together with the Disclosure and Notification Manager keep track of changes in the data flow. Changes in the state of the consent are recorded by the "Audit" component. The "Trust Authority" deals with compliance checks and certification of digital certificates, while the "Risk Assurance" component, which could be used offline as well, provides insights about security and privacy risks and suggestions on how to avoid them.

[36]https://www.hpl.hp.com/breweb/encoreproject/index.html

3.3.2. ADvoCate

ADvoCATE [39] is a consent management platform based on blockchain technology, with the goal to provide information about data, detect violations of privacy policies and manage the data processing in an Internet of Things (IoT) ecosystem [39]. The platform is used as a medium between the end-user and the industry and consists of (i) a consent management component, (ii) a consent notary component, and (iii) an intelligence component. Consent representation, updates and withdraws are managed by the consent management component with the data protection ontology by Bartollini et al. [40] according to GDPR requirements. The consent notary component ensures compliance and consent validity by using reasoning, supported by Fuzzy Cognitive Maps (FCM), over the Ethereum blockchain, which manages the integrity and the versioning of consent, while the intelligence component identifies conflict in personal data sharing policies with the help of Fuzzy Cognitive Maps (FCM) [41], the Intelligent Policies Analysis Mechanism (IPAM) and the Intelligent Recommendation Mechanisms [39]. The final solution is a framework that is able to record, validate and store user consent by combining semantic technologies, namely ontologies, and blockchain. The primary use of blockchain in the project is (i) for smart contracts, which are signed digitally using private key and (ii) for managing hashes. The mapping of data can be performed by using the unique id provided for each IoT device, which has been registered in the ADvo-

Cate platform. The authors conclude that a more detailed ontology for consent and improvements of the intelligence component will be needed in the future.

3.3.3. SPECIAL-K

The SPECIAL-K is a framework developed under SPECIAL[37] (Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance) EU H2020 project for automatic compliance verification based on usage control policies for data processing and sharing. The motivation comes from the lack of consent management solutions that successfully execute its withdrawal. The main goal of the project is thus to have a framework that monitors consent and enables actions such as withdrawal to be immediately executed even after years of data sharing, while being compliant with current laws [21].

The framework in [21] consists of three primary SPECIAL components: (i) Consent Management Component, (ii) Transparency and Compliance Component, and (iii) Compliance Component. The Consent Management Component is responsible for obtaining consent from the data subject and representing using SPECIAL usage policy vocabulary [21]. The Transparency and Compliance Component is responsible for presenting data processing and sharing events to the user following SPLog vocabulary (Section 3.1.6). The Compliance Component focuses is used to verify the compliance of data processing and sharing with usage control policies.

The implementation uses SPL[38], which is encoded using web ontology language (OWL2) to represent the policies, MongoDB[39] to store data about consent, embedded HermiT [40] reasoner to determine the compliance based on usage control policies, Elasticsearch[41] for browsing logs serialised using JSON-LD and Apache Kafka[42] to carry out processing of application logs and to save the result of reasoning in new Kafka topic.

3.3.4. GDPR Compliance Privacy Framework by Davari et al.

Davari et al. [20] present a GDPR privacy protection framework for an access control system that utilises XACML (an OASIS standard for expressing policies). The main aim of the research is to provide a solution that supports data privacy protection based on GDPR. The presented compliance validation model uses the PROV-O[19] ontology for semantically modelling consent according to GDPR. The consent model itself is built by extracting all GDPR relevant rules. The management of the consent and the personal data is done by utilizing the blockchain framework Hyper-ledger Fabric[43]. For imposing consent on all entities involved in the data sharing process, the authors use cryptography technology. Each party involved, such as the data subject, data processor, the data controller, is assigned an asymmetric key pair, and it is used as an identity mechanism. However, in addition to blockchain, MongoDB[39] is used for storing data. The main reason, as explained by Davari et al. is that blockchain is immutable thus data cannot be deleted once stored. Although this supports traceability and transparency, it is in collision with the user's right to "erasure" given by GDPR.

3.3.5. CampaNeo

CampaNeo[44], a German-Austrian collaboration project with duration of three years (2019-2022) that aims to develop a platform for sensor data sharing between multiple entities. The platform's main goal is to provide the industry with an outlet for publishing data requests for user's vehicle sensor data in the form of campaigns. CampaNeo utilises machine learning for detection of driving behaviour, finding driver's efficiency scores, predicting car accidents, traffic regions etc. and knowledge graphs for the campaign data modelling. The CampaNeo ontology defines the concepts of campaign, data, processing, third-party entities, users and consent. Knowledge graphs are used for achieving process transparency and data traceability by recording consent and its provenance. Further, a UI that focuses on consent visualisation with the help of forms is being currently developed (as of 2020). The UI aims to present users with information about consent such as its purpose, data regarding it, the organisation making the request, thus achieving GDPR compliance.

3.3.6. Blockchain-based Consent Model by Jaiman et al.

Jaiman et al. [42] present a dynamic GDPR consent model for health data sharing in a distributed environ-

[37] https://www.specialprivacy.eu/
[38] https://www.w3.org/community/dpvcg/wiki/SPECIAL_usage-policy/
[39] https://www.mongodb.com/
[40] http://www.hermit-reasoner.com/
[41] https://www.elastic.co/elasticsearch/
[42] https://kafka.apache.org/
[43] https://www.hyperledger.org/use/fabric
[44] https://projekte.ffg.at/projekt/3314668

ment, that utilises blockchain. The main motivation for their work is improving accountability in health data sharing, which has proven to be a challenge due to the large volumes of data constantly being collected by consumer wearables. The developed blockchain-based consent model reuses the Data Use Ontology (DUO)[45], which allows describing data use conditions for research data in the health/clinical/biomedical domain. Further, Jaiman et al. [42] reuse the Automatable Discovery and Access Matric (ADA-M) [43] ontology for classifying data use conditions and permissions. The consent statement itself is modelled with DUO then saved as a smart contract and added to the existing blockchain. Upon a data request from a third party, the ADA-M ontology is used for finding matching contracts. Once a match between the user consent statement and the data request is found access is granted to the requestor. When it comes to specific technology, the Solidity language for smart contracts and the LUCE platform for data sharing, which builds upon the Ethereum [46] blockchain, were used [42].

3.3.7. Automated GDPR Compliance using Policy Integrated Blockchain by Mahindrakar et al.

Mahindrakar et al. [44] present a blockchain-based approach to facilitate GDPR compliance for real-time automated data transfer operations between consumers and providers. The main aim of their work is to ensure valid data transfer operations while maintaining GDPR compliance. The presented work uses both semantic technology and blockchain. Two ontologies are used, namely a GDPR ontology built by the authors and the privacy policy ontology by Joshi et al. [45], which represents consent from a privacy perspective. Management of consent, namely its validation, is done by querying the privacy policy ontology by Joshi et al. [45] using SPARQL[7] and based on the result, further processing (e.g. data transfer) is allowed or not. The developed GDPR ontology by Mahindraker, itself, holds the information about GDPR articles. The relevant articles between consumers and providers are queried using SPARQL to create a GDPR knowledge graph, which is then used for reasoning with smart contracts. Regarding the implementation, the solution uses Natural Language Processing (NLP) techniques, the private blockchain network Ganache-CLI[47] for Ethereum and encryption mechanisms (i.e. The Advanced Encryption Standard algorithm). Similarly to Davari et al. [20], the authors address the issue of the immutability of blockchain and how it affects GDPR compliance. To overcome this, data is saved in an external encrypted file, which is stored in a relational database. All the involving parties are registered on the blockchain network and are assigned a unique account number and a private key. By decrypting using the public key, the data owner is able to use the transaction hash stored in an encrypted file to access the transaction details.

3.3.8. smashHit

smashHit[48] is an ongoing Horizon 2020 project that ends in December 2022 with the primary objective of creating a secure and trustworthy data sharing platform with focus on consent management in a distributed environment such as the automotive industry, insurance and smart cities. smashHit proposes to use semantic models of consent, such as ontologies and knowledge graphs and legal rules for consent management. The vision of smashHit is to overcome obstacles in the rapidly growing data economy, which is characterised by heterogeneous technical designs and proprietary implementations, locking business opportunities due to the inconsistent consent and legal rules among different data-sharing platforms actors and operators.

3.3.9. Summary

We summarise the overviewed research (completed and ongoing) from this section in Table 6. Looking back at the scope and main goal for each research project, it becomes clear that consent management is a complex multi-action process that is closely connected to the fields of data privacy and security.

Table 6 shows the overviewed solutions for consent management. Most of the projects and studies make use of semantic technology, namely ontologies and knowledge graphs, showing semantic technology as helpful data models for consent due to their ability to represent relationships between concepts. The projects SPECIAL-K [21], CampaNeo[44] and studies by Rantos et al. [39], Jaiman et al. [42], Davari et al. [20], Mahindrakar et al. [44] using ontologies and knowledge graphs have demonstrated the value of semantic technology, namely knowledge graphs and ontologies for consent management. Further, considering the advantage of semantic technology, new projects like smashHit[48] are also making use of ontologies and

[45] http://www.obofoundry.org/ontology/duo.html

[46] https://ethereum.org/en/

[47] https://docs.nethereum.com/en/latest/ethereum-and-clients/ganache-cli/

[48] https://www.smashhit.eu

Table 6
Consent Management Projects and Research Work

Project/research work	Duration	Use Case	How is technology used?
EnCoRe	2008-2011	An end-user discloses personal data along with consent/privacy preferences; employees and/or applications try to access data for specific purposes; data subject changes their consent/privacy preferences; personal data is disclosed to a third party.	XML for structuring data; MongoDB for storing data.
ADvoCATE	2015-2019	Consent management in IoT environment.	Data protection ontology by Bartolini et al. [40]; Ethereum blockchain to maintain consent integrity and versioning.
SPECIAL-K	2017-2019	Consent for municipality road layout optimisation; sending bank travel insurance; sending traffic condition warning.	SPLog ontology modelling consent; MongoDB for storing data.
Davari et al.	2019	Management of consent and smart contracts with blockchain technology when Multi-National Companies (MNC) are involved.	XACML based access control model for implementing privacy framework; Blockchain framework Hyper-ledger Fabric for smart contract; PROV-O ontology for modelling consent according to GDPR; MongoDB for storing data.
CampaNeo	2019-2022	Consent for vehicle sensor data sharing.	Knowledge graphs for data modelling; CampaNeo ontology to define the concepts of campaign, data, processing, third-party entities, users and consent; GraphQL as an access point and schema for data.
Jaiman et al.	2020	Individual consent model for health data sharing platforms.	Data Use Ontology (DUO) for modelling consent and describing data use conditions; Discovery and Access Metric (ADA-M) ontology for classifying data use conditions and permissions; Ethereum blockchain for smart contract using the Solidity language.
Mahindrakar et al.	2020	GDPR compliance in real time; enforce data privacy policy when data is shared with third parties.	Privacy policy ontology for consent representation; GDPR ontology for GDPR articles; Ethereum private blockchain network - Ganache-CLI for smart contract; natural language processing for extracting privacy policies; AES encryption for encrypting data files.
smashHit	2020-2022	Consent for sensor data sharing in a smart city and for insurance purposes.	Ontologies for contract modelling; knowledge graphs for storing data about users, consent and contracts.

knowledge graphs for consent management. In addition to knowledge graphs and ontologies, studies like [20, 39, 42, 44] also make use of blockchain technology. The use of blockchain technology is adding value due to its ability to provide traceability and automatic code execution using a smart contract. In particular, the smart contract was used for executing the task of consent verification.

However, the research by Davari et al. [20] and Mahindrakar et al. [44] highlights the limitation that arises with the use of blockchain for storing data. The limitation is because of the immutability nature of the blockchain, which contradicts the user rights such as *"the right to be forgotten"*[49] whenever the data subject revokes the consent. To deal with limitations due to immutability of the blockchain, external storage like a relational database, the file system is used for storing the data, and only the hashes are stored in the blockchain.

[49]https://gdpr-info.eu/issues/right-to-be-forgotten/

3.4. Standardisation Initiatives and Efforts

This section presents the current status of standards and standardisation efforts related to consent, namely Consent Receipts v1.1 [46], ISO/IEC 29184:2020[50] and IAB Transparency and Control Framework[51].

3.4.1. Consent Receipts v1.1

The Consent Receipt v1.1specification[52] [46], published in 2018, provides an interoperable and transparent "record" of consent similar to a receipt after payment/sale of goods - for benefit to both Data Controllers and individual. The specification uses terms and definitions from ISO 29100:2011[53] to describe consent, purposes, organisations, and recipients, and is structured as a flat-list or non-hierarchical schema with an implementation using JSON which adopters must implement for conformance. It lacks the neces-

[50]https://www.iso.org/standard/70331.html
[51]https://iabeurope.eu/tcf-2-0/
[52]https://kantarainitiative.org/file-downoads/consent-receipt-specification-v1-1-0/
[53]https://www.iso.org/standard/45123.html

sary fields to represent and conform with requirements from recent laws such as GDPR. However, it provides a useful direction for creating and maintaining shared documentation for representation of consent that can be utilised by both the individual and controllers.

There is work underway to update the Consent Receipt with the recent developments and requirements, such as for GDPR. For this, Kantara has initiated the Advanced Notice & Consent Receipts Working Group[54] (ANCR). ISO/IEC have similarly initiated work on a new standard - ISO/IEC 27560[55] Consent Record Information Structure.

3.4.2. ISO/IEC 29184:2020

ISO/IEC 29184:2020[50] standard, published recently in June 2020, concerns the provision of privacy notices and requesting consent in an online context. It specifies requirements for information provided in a notice, its form and manner for comprehension, and role in validity of consent. It also dictates the process for the collection of consent in order for it to be valid. The standard notably raises the requirement of consent to be 'explicit' as the default, specifies risk assessment information, and advocates privacy and individual centric measures in both notice and consent related information and processes. 29184 specifically acknowledges the role of semantics and machine-readability for consent requests and records, and uses the Consent Receipt [46] specification as an example.

3.4.3. IAB Transparency and Control Framework

The Interactive Advertising Bureau (IAB)[51] is a non-profit organisation that creates and maintains standards for use within the online advertising network that involves some of the largest data operators and consent framework providers such as Google, Oracle, Adobe, Quantcast, OneTrust. Its 'Transparency and Control Framework' (TCF)[56] specification provides a protocol and data model for representing collected consent and its use within the online marketplace for ads based on the Real-Time Bidding (RTB)[57] process. TCF consists of a controlled list of purposes, recipients, third-parties for data sharing, and controls associated personal data and based on use of legitimate interest and consent.

3.4.4. Summary

The standards and standardisation regarding consent is notably limited in terms of practical usage to IAB's TCF framework. It is currently unclear what role such standards play in legal compliance, and their validity in different use-cases. However, the publication of ISO/IEC 29184, its acknowledgement of semantics and machine-readability for interoperable consent records, and the renewed interest in interoperable and machine-readable Consent Receipts shows promising developments in the future. This provides further motivation for inclusion of semantics in the consent management process based on these standards and their modeling of proposes and use-cases.

4. Best Practices and Recommendations

On the basis of the surveyed literature, this section is divided into subsection that present best practices for each of the four stages of the consent life-cycle (Figure 1) - request, comprehension, decision and use. The best practices are to provide guidelines on the ways to implement consent in organisations, as well as an input to researchers and policy makers on the possible future research. The following recommendations focus on the semantic and technical aspects of consent implementation, while considering standards (see Section 3.4), ethics and law (i.e. GDPR).

Before making specific recommendations, we would like to highlight that GDPR is just one of the many laws aimed at user's privacy and rights. In Europe, for example, before the GDPR, the ePrivacy Directive[58] was (and still is) one of the laws for personal data processing and privacy protection. ePrivacy and its derivative laws require consent for cookies, which is often combined with consent for personal data processing. In addition, each country has its own laws related to the matter. Reviewing them is not in the scope of this paper, however, we list several laws that one might want to consider. For example, Austria's Data Protection Law (DSG)[59] and Germany's Federal Data Protection Act (BDSG)[60] in Europe. Examples of laws regarding data privacy outside the EU are California's Consumer Privacy Act (CCPA)[61], The Notifiable Data

[54] https://kantarainitiative.org/confluence/pages/viewpage.action?pageId=140804260

[55] https://www.iso.org/standard/80392.html

[56] https://iabeurope.eu/transparency-consent-framework/

[57] https://www.iab.com/guidelines/openrtb/

[58] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

[59] https://www.dsb.gv.at/recht-entscheidungen/gesetze-in-oesterreich.html

[60] https://www.gesetze-im-internet.de/englisch_bdsg/

[61] https://oag.ca.gov/privacy/ccpa

Table 7
Recommendations for the Request of Consent

Request of Consent		
	Recommendations	**Relevant Sections**
Semantic Models for Consent	• **Know the (i) relevant domain, (ii) desired level of details, and (iii) specific laws and their requirements.** • **Use standards for ontology development** such as OWL, RDF and RDFS and organisation systems such as SKOS, Schema.org and RIF. • **Understand which standards for consent already exist**. Standards relevant to consent and its collection that one might consider are Consent Receipt v1.1 and ISO/IEC 29184:2020. Consent Receipt provides a list of information fields and categories for information related to consent, while ISO/IEC 29184:2020 specifies what information needs to be provided in privacy policies and the role in validity and consent. • **Model consent according to the GDPR when deadling with the data of European citizens.** We propose having a closer look at the existing GConsent[17] and BPR4GDPR[23] ontologies, which focus on representing consent and its states (i.e. given, not given and withdrawn) as defined by GDPR (Art. 7 and Rec. 72). • **Modelling consent and data provenance.** The CDMM[18] ontology models data provenance by reusing the PROV-O ontology, consent and the format in which it was retrieved (e.g. app based, audio, online) thus specific classes could be reused in addition to already existing consent models to achieve better granularity. CDMM is suitable in cases where the context under which consent was given could change overtime, for example, to check who is allowed or denied to do some activity on what data. • **Modelling consent for compliance checking.** The SPECIAL vocabularies [21] could be reused as both are aimed at GDPR compliance checking and model consent as an artefact of privacy policies. Other ontologies built for GDPR compliance checking are LloPy [25], ColPri [22] and DPV[27].	Section 1 (Tables 1, 2, 3), Section 3.1, Section 3.4
Consent Visualisation	• **Allow customisation of consent through interaction.** The CoRe [34] and CURE [35] UIs allow one to select for what purpose the consent will be given. Further, CoRe allows to view how a data sharing process could look like via a graphical visualisation included in the consent request form. • **Graphical visualisation of the data.** Graphs, for example, can be interactive and can allow one to view what giving consent for a specific purpose will result in. Using graphs as visualisation tools has proven useful in [34][35], however, issues such as information overload [47] might still be present. • **Avoid legalese.** It is recommended that complex legal jargon is avoided. The information should be written in a simpler form that is understandable by users from different educational backgrounds and levels. This will also help minimise the information overload in individuals. • **Avoid dark patterns.** For example, pre-checked boxes and highlighted fields. According to GDPR, individuals should be able to choose freely for themselves and not feel forced.	Section 3.2
Consent Management	• **Reuse of existing solutions**. We recommend looking for existing solutions and technology that might fit one's needs and if found to adapt them according to the specific needs. This concept is also prominently used in software development, where before implementation, the usability of existing relevant libraries is checked. A similar concept is demonstrated by the use of existing technologies (e.g. MongoDB, blockchain, semantic technology) for managing the requested consent by Davari et al [20], ADvoCATE [39] and SPECIAL-K [21]. • **Consider storage limitations.** Based on the selected type of storage (e.g. blockchain), one could be in violation of GDPR. For example, the use of blockchain to store consent will violate user's "right to erasure" (Art. 17)[20][44].	Section 3.3

Breach (NDB)[62] in Australia, Brazil's Lei Geral de Proteçao de Dados (LGPD)[63].

4.1. Request of Consent

Requesting consent can be seen as one of the most important stages in the consent life-cycle (Figure 1) as it defines whether or not data processing can begin. A successful consent request, which we view as one that results in receiving individual's consent, should be GDPR compliant. Having a semantic model for consent, which represents GDPR information in both human-readable and machine-readable format, would be beneficial to any system. Such model can be build with ontologies as shown in Section 3.1. However, consent requests are made to the user thus a visualisation of the request itself is needed as well. Further, once requested and given by the individual the consent needs to be managed, for example, when stored in the system for future reference if compliance checking is performed. Table 7 presents a summary of recommendations for requesting consent based on the overviewed literature in this paper. The recommendations are divided into three sections: semantic model for consent, consent visualisation and consent management, all of which relate to the request of consent.

4.2. Comprehension of Consent

Semantic technology helps achieve a common understanding between multiple entities by representing information in both human-readable and machine-readable formats. For a machine, representing the concepts with languages such as OWL or RDF is enough, however, this is not the case with end users.

[62] https://www.oaic.gov.au/privacy/notifiable-data-breaches/
[63] https://gdpr.eu/gdpr-vs-lgpd/

Table 8
Recommendations for the Comprehension of Consent

Comprehension of Consent		
	Recommendations	**Relevant Sections**
Semantic Models for Consent	• **Understand the domain.** An ontology would reflect the ontology engineer's understanding of a specific domain.Begin by selecting an ontology engineering methodology e.g. of Noy and McGuiness [48]. We recommend deriving all important concepts and how they might be related. Once this is clear one can translate the knowledge into an ontology by following different methodologies as presented in. • **Select an ontology language based on the desired functionality.** Most of the consent ontologies in Section 3.1 are built with OWL. In comparison to OWL, OWL2 offers more expressivity by allowing the use of keys, property chains qualified cardinality restrictions, richer data ranges, asymmetric, reflexive, disjoint properties, and enhanced annotation capabilities. Other languages such as RDFs, KIF and DAML+OIL, and popular upper level ontologies such as Dublin Core can be used as well. For example, a combination of several ontology syntaxes is possible as well. The Colpri [22] ontology is built with both OWL and SKOS. A detailed comparison of ontology languages is presented in [49].	Section 3.1
Consent Visualisation	• **Use graphical visualisations to represent the data flow.** For example, graphs can be easier to understand by humans than text, as they provide a visualisation of the main entities and the connections between them. The graphical visualisations in the overviewed tools have proven to be useful and to provide individuals with the information in an easily comprehensible way. • **Include the end-user.** In the Data Track tool [29], the end user is visualised at the centre of the graph. This has resulted in individuals feeling more involved and interested in what is happening to their data. • **Allow interactivity.** The Data Track tool [32], CoRe [34] and CURE [35] UIs and the Privacy Dashboard [33] have all included interactive elements in their visualisations. For example, Data Track allows individuals to explore the provided graphical visualisation by expanding andcollapsing certain UI fields and the graph itself. CoRe and CURE both allow interactivity when individuals give consent - one can select for what purpose to give consent and to follow the data flow for that purpose. • **Accessibility**. Individuals should be able to understand what is presented and also be able to interact with it directly. Individuals with disabilities should be considered as well. For example, developing interfaces that recognise one's speech and also allow dictation of text and similar features (e.g. n the MAC iOS operating system) would be beneficial for individuals who suffer from blindness.	Section 3.2
Consent Management	• **Use semantic technology.** Consent management can be performed automatically by any machine at any time, however, without semantics a machine simply executes commands specified by an individual and yields a result. It does not actually understand what the data or the commands mean. Semantic technology changes this as it adds value to things and helps machines become aware. By enhancing machines with semantics one would be able to climb higher in the so-called DIKW (data, information, knowledge, wisdom) [50] hierarchy and reach the knowledge level.	Section 3.1, Section 3.3

End-users have different needs and understanding of information. Further, one's knowledge of the semantic web could also be a challenge thus a simple yet effective visualisation of consent is needed. This visualisation is directly linked to GDPR's consent requirement regarding requesting consent (Section 1). Humans are visual creatures thus a visualisation of the required data would be more efficient in comparison to presenting one with long privacy policies written in legal jargon. In this section we provide guidelines (Table 8) for visualising information to end-users based on the reviewed literature (Section 3.2) in the area of consent visualisation for improving comprehension. In addition, we present recommendations (Table 8) on how to enhance a machine's understanding of things with semantic technology. The recommendations are divided into three sections: semantic model for consent, consent visualisation and consent management, all of which relate to the comprehension of consent.

4.3. Decision about Consent

When it comes to giving consent, the decision rests in the hands of the user. All people are biased in their own way due to their upbringing and current environment. While some users might give consent just to be "done" with the process, the choice of others could be affected by many factors such as the information that is presented, the level of detail, specific interface design [29]. By reviewing existing information-sharing and institutional privacy concerns, Marwick et at. [52] conclude that 'trust' is the key factor that affects one's choice. Users are more likely to share personal and general data if they trust the website or the purchase provider. Further, Woodruff et al. [54] show that people are less likely to share data if it could have a negative personal impact. The recommendations in Table 9 are divided into three sections: semantic model for consent, consent visualisation and consent management, all of which relate to the decision about consent.

4.4. Use of Consent

User's consent can be used in many ways (e.g. compliance checking, reasoning, as a proof of contract) and each way requires different system functionalities. All these actions performed with consent, could be sum-

Table 9
Recommendations for the Decision about Consent

Decision about Consent		
	Recommendations	**Relevant Sections**
Semantic Models for Consent	• **Decide which decisions will be recorded by your system and which not.** For example, this includes the need to record the individual's decision to not give consent. Recording a refusal of consent might be important in some use cases such as for insurance purposes for evaluating an individual's credibility. Further, implement the requirements from applicable laws. • **Model consent and the processing it could involve.** Have a semantic model not only for consent but also for decisions related to it. As a guideline we suggest viewing the GConsent[17] ontology, which models the status of the consent not only as given but also as expired, explicitly given, given by delegation, implicitly given, invalidated, not given, refused, requested, unknown and withdrawn. If such level of detail is not needed, the BPR4GDPR[23] defines only three consent states: provided, denied and revoked.	Section 3.1
Consent Visualisation	• **Build trust among users.** Specifically, transparency should be aimed at, dark patterns avoided and instead clearly acknowledge the implications of their actions (Table 8). • **Know the end-users.** Understand one's needs, background, main bias regarding data sharing, in order to create successful incentives [51]. • **Specify the benefit/positive outcome of sharing data.** Users are more willing to share data if there is a clear benefit for them [52]. For example, improved personalisation of services as presented by Marwick et al. [52] • **Use incentives to raise one's engagement**. Incentives can be a way of attracting one's interest and can potentially lead to one wanting to gain a better understanding about what it means to give consent and the implications that can arise. An example is the the gamification mechanism adopted by Comtella [51], in which users are rewarded with points once they perform a specific task. The results of the evaluation of this mechanism showed a significant but short-term increase of participation. Personalised incentives have a higher success rate but could be complex to develop.	Section 3.2, Section 4.2
Consent Management	• **Handle decisions in a reasonable amount of time.** The developed system must be able to handle it within a reasonable amount of time.For recording given consent, this could take milliseconds. However, decisions such as consent withdrawal might be more time-consuming depending on how many entities are involved and how much data has been shared. Another factor affecting the execution of the decision could be the type of technology that was selected. For example, the blockchain used in can become slow with time as more data is added. • **Be transparent.** Laws such as GDPR put focus on transparency. Therefore, achieving transparency in order to be compliant with laws like GDPR is essential. However, different types of transparencies such as access and location exist. An overview of the different types of transparencies is presented in [53]. Further, transparency could be achieved on many levels. For example, on an algorithmic level (i.e. how decisions are made within the system). In the case of consent decision making, one can achieve transparency by presenting the data subject with relevant information about the required data, the involved entities and the purpose of the consent request. Transparency could also be extended to the data sharing process itself by using auditable technology like blockchain, as presented by Mahindrakar et al. [44]	Section 3.3

marised as consent management (see Section 3.3). The recommendations in Table 10 are divided into three sections: semantic model for consent, consent visualisation and consent management, all of which relate to the use of consent.

5. Conclusions

Semantic technology such as ontologies are the key to achieving a common understanding between machines and humans. Although they have been around for many years, there is much more to discover about their possible applications in different fields. For example, understanding the benefit of semantics in the law domain, which we address by specifically looking at semantic technology for consent implementation according to GDPR.

In this paper we presented an overview of existing semantic solutions for implementing consent and recommendations for implementing consent with semantic technology. To be specific, we provided guidelines for building a semantic model for consent, graphically visualising consent to individuals for better comprehension and for consent management.

As we have shown with the overviewed work, it is possible and useful to have a semantic model for consent in the form of an ontology that models consent through its whole life-cycle (Figure 1). For the request of consent, a semantic model provides a description of all the information required by laws (e.g. GDPR) for informed consent, thus it provides a common understanding of the law requirements that both machines and humans understand and need to follow. Based on the underlying semantics a machine is able to create the links between the consent decision and all information related to it. During the comprehension step, the semantic model helps to translate the human knowledge into machine knowledge and to establish a common understanding of the meaning of consent, the risks and consequences associated with it to other humans. An ontology can also model different states of consent, for example consent revocation and the rules that apply in such situation so that a machine is able to handle the consent state change in compliance with

Table 10
Recommendations for the Use of Consent

Use of Consent		
	Recommendations	**Relevant Sections**
Semantic Models for Consent	• **Model consent with semantic technology.** Semantics provide the machine with extra knowledge about what each concept means and how it is connected to other concepts. For example, a consent ontology would provide an insight of what consent is, how it is represented and related concepts that could be affected when a machine uses consent in any way. We suggest looking at Section 3.1, which presents existing semantic models for consent and at Section 4.1 where we provide recommendations for building such consent models.	Section 3.1, Section 4.1, Table 7
Consent Visualisation	• **Visualise the use of consent with graphs.** How consent is used could be visualised with a graph either before or after consent is given. CoRe [34] visualises the consent request by using an interactive graph, which presents the end user with a visualisation of how their data will be used and by whom based on their consent preferences (see Figures 4 and 5). The Privacy Dashboard [33], on the other hand, visualises the use of consent by using a timeline graph that shows how the data flow after consent is given. The Privacy Dashboard allows one to view what is happening to their data, after consent was given (see Figure 3), at each stage and further to adjust one's privacy settings. • **Consider who will use the visualisation.** The reviewed literature in Section 3.2 presents a graphical visualisation aimed at easing end-users' comprehension of consent and its usage. However, different users might need different level of detail from a visualisation. In comparison to an end-user with no experience in the field, a data processor or controller has some legal experience thus might be interested and might need a much more detailed visualisation of the information.	Section 3.2, Section 4.2
Consent Management	• **Understand how each component of your system will be affected.** This is specifically relevant to consent withdrawal. Upon a request for a consent withdrawal, user's data must be deleted from all entities that use it as soon as possible. Consider what happens if the data is currently used for a specific process and how to terminate it, and further, how to make sure there is no data leftovers in the system. The SPECIAL-K [21] project, for example, utilises Apache Kafka for transparency and compliance and has developed its own compliance checker based on the Hermit Reasoner. Consent and event logs are stored in the Virtuoso Triple Store as described in [55], while the connections between components is achieved by using a micro-service called mu.semte.ch. • **Consider ethics.** This is especially crucial in certain fields, such as health and medical applications where there are already many relevant developments, and particularly areas that look into the details of the relation of the private and public [56]. With the regulations such as GDPR and data management under it, the topic is getting a new dimension and also becomes highly present in other sectors. For example, in the EU, the topics related to the data protection and transparent data management for the users have been assessed as very important by the stakeholder groups involved in the construction of the road map covering a broad spectrum of sectors [57]. There is also clarity that different stakeholders have different interests in consent representation and management. Particularly, businesses look for solutions that encourage the data owners (e.g. end users) to consent to sharing of various data as much as possible, the states are interested in the protection and fair use of their data and economy and enforcement of the basic human rights, and the end users among other are interested in the privacy of their data and also in the added value the sharing of their data potentially provides. These varying and at times conflicting interests should be accounted for and balanced in the representation and management of consent. • **Look outside of the box**. Single technology may not be self-sufficient to provide a complete solution for consent management as in itself the latter is not only one process. Therefore, different technologies that complement each other's limitations (e.g. semantic technology and blockchain) are used together to provide a robust solution. In the case of the consent management solutions, based on the reviewed solutions, we suggest considering combining blockchain and semantic technology as done in [20][44]. The main reason for this suggestion is that blockchain has the ability to provide transparency, data traceability and the ability to execute consent management automatically via smart contracts. However, as the research in [20][44] has shown, these advantages could be also seen as disadvantages due to the immutability of blockchain. Other disadvantages of blockchain use include high computational costs, in terms of money, time and CO2 output, and this also should be considered when building solutions. Further, other studies on blockchain such as [58][59][60] have also highlighted the issue of computational complexity.	Section 3.3

the law and most of all in a meaningful way. Finally, the use of consent or also called in this paper "consent management", benefits from the tracebility, transparecy and faster and easier knowledge discovery that a semantic model offers.

All of these semantic model capabilities can be utilised when actions such as consent validation and compliance checking need to be performed. Although a semantic model offers many advantages, the difficulty of implementing informed consent is still present due to the need for one to not only understand and model laws such as GDPR, but to also integrate them with suitable technologies (e.g. blockchain is not a suitable storage for informed consent as defined by GDPR [20][44]). Further, complex issues regarding consent that need to be addressed are traceability and compliance checking.

As mentioned in Section 4, the jurisdictional limitation of laws that means there are several relevant laws that regulate consent in relation with data processing - applicable within their own jurisdiction or domain. For example, the California Consumer Privacy Act (CCPA)[61] (effective since January 2020) applies to companies in the state of California, USA and is consumer and privacy oriented as compared to GDPR's focus on data protection. Ontologies and semantics in general can help organisations to identify and address common requirements across such laws, for example

similarities between GDPR and CCPA [61]. The challenge for such approaches lies with the law-specific terms and requirements, such as the notion of 'do-not-sell' under CCPA which permits individuals to opt-out of data sharing (termed 'selling' under CCPA) to third parties. One possible solution for this could be to utilise a common ontological framework and build extensions for specific legal requirements - such as the approach taken by the Data Privacy Vocabulary (DPV) vocabulary.

In conclusion, this survey paper focused mainly on ontologies as a semantic model for consent and how they could be used for consent management. The evolution of the models and techniques built on them will include semantic models such as schemas that have been used for many years already, as well as newer solutions built with knowledge graphs [62], addressing the desired systems' functionalities.

6. Acknowledgements

This research has been supported by the smashHit European Union project funded under Horizon 2020 Grant 871477. Harshvardhan J. Pandit is funded by the Irish Research Council Government of Ireland Postdoctoral Fellowship Grant GOIPD/2020/790, by European Union's Horizon 2020 research and innovation programme under NGI TRUST Grant 825618 for Privacy as Expected: Consent Gateway project, and through the ADAPT SFI Centre for Digital Media Technology which is funded by Science Foundation Ireland through the SFI Research Centres Programme and is co-funded under the European Regional Development Fund (ERDF) through Grant 13/RC/2106_P2.

References

[1] World Economic Forum, Personal Data: The Emergence of a New Asset Class, 2011, Last Accessed 16-10-2020. http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf.

[2] S. Yu, Big privacy: Challenges and opportunities of privacy study in the age of big data, *IEEE Access* **4** (2016), 2751–2763. doi:10.1109/ACCESS.2016.2577036.

[3] Regulation (EU) 2016/679 of the European Parliamentand of the Council of 27 April 2016 on the protectionof natural persons with regard to the processing of per-sonal data and on the free movement of such data, andrepealing Directive 95/46/EC (General Data ProtectionRegulation), *Official Journal of the European Union, L119* (May 2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[4] V. Mangini, I. Tal and A.-N. Moldovan, An empirical study on the impact of GDPR and right to be forgotten-organisations and users perspective, *Proceedings of the 15th International Conference on Availability, Reliability and Security* (2020), 1–9. doi:10.1145/3407023.3407080.

[5] C. Tankard, What the GDPR means for businesses, *Network Security* **2016**(6) (2016), 5–8. doi:10.1016/S1353-4858(16)30056-3.

[6] Commission Nationale de l'Informatique et des Libertés (CNIL), *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against GOOGLE LLC*, 2019 (Accessed in September 2020), Available at: "http://engineering.purdue.edu/~mark/puthesis".

[7] H. Jung, H. Yoo and K. Chung, Associative context mining for ontology-driven hidden knowledge discovery, *Cluster Computing* **19**(4) (2016), 2261–2271. doi:10.1007/s10586-016-0672-8.

[8] N. Freire and S. de Valk, Automated interpretability of linked data ontologies:: an evaluation within the cultural heritage domain, *IEEE International Conference on Big Data (Big Data)* (2019), 3072–3079, IEEE. doi:10.1109/BigData47090.2019.9005491.

[9] S. El-Sappagh, J.M. Alonso, F. Ali, A. Ali, J. Jang and K. Kwak, An Ontology-Based Interpretable Fuzzy Decision Support System for Diabetes Diagnosis, *IEEE Access* **6** (2018), 37371–37394. doi:10.1109/ACCESS.2018.2852004.

[10] S. de Lusignan, S. Shinneman, I. Yonova, J. van Vlymen, A.J. Elliot, F. Bolton, G.E. Smith and S. O'Brien, An ontology to improve transparency in case definition and increase case finding of infectious intestinal disease: database study in english general practice, *JMIR medical informatics* **5**(3) (2017). doi:10.2196/medinform.7641.

[11] C. König, A. Mengist, C. Gamble, J. Höll, K. Lausdahl, T. Bokhove, E. Brosse, O. Möller and A. Pop, Traceability in the Model-based Design of Cyber-Physical Systems, *Proceedings of the American Modelica Conference* (2020). doi:10.3384/ECP20169168.

[12] M.S. Murtazina and T. Avdeenko, An ontology-based approach to support for requirements traceability in agile development, *Procedia Computer Science* **150** (2019), 628–635. doi:10.1016/j.procs.2019.02.044.

[13] A. Lakehal, A. Alti and P. Roose, A semantic event based framework for complex situations modeling and identification in smart environments, *International Journal of Advanced Computer Research* **9**(43) (2019), 212–221. doi:10.19101/IJACR.PID33.

[14] A.N. Lam and Ø. Haugen, Applying semantics into service-oriented iot framework, *IEEE 17th International Conference on Industrial Informatics (INDIN)* **1** (2019), 206–213, IEEE. doi:10.1109/INDIN41052.2019.8972295.

[15] P.N. Otto and A.I. Anton, Addressing Legal Requirements in Requirements Engineering (2007), 5–14. doi:10.1109/RE.2007.65.

[16] C. Rodrigues, F. Freitas, E. Barreiros, R. Azevedo and A.A. Filho, Legal ontologies over time: A systematic mapping study, *Expert Syst. Appl.* **130** (2019), 12–30. doi:10.1016/J.ESWA.2019.04.009.

[17] V. Leone, L.D. Caro and S. Villata, Taking stock of legal ontologies: a feature-based comparative analysis, *Artificial Intelligence and Law* **28** (2019), 207–235. doi:10.1007/s10506-019-09252-1.

[18] D. Moher, A. Liberati, J. Tetzlaff, D.G. Altman and T.P. Group, Preferred Reporting Items for Systematic Reviews and Meta-Analyses: The PRISMA Statement, *PLOS Medicine* **6**(7) (2009), 1–6. doi:10.1371/journal.pmed.1000097.

[19] M. Palmirani, M. Martoni, A. Rossi, B. Cesare and R. Livio, Pronto: Privacy ontology for legal compliance, *Proceedings of the European Conference on e-Government, ECEG* (2018), 142–151. doi:10.1007/978-3-319-98349-3.

[20] M. Davari and E. Bertino, Access control model extensions to support data privacy protection based on GDPR, *IEEE International Conference on Big Data (Big Data)* (2019), 4017–4024, IEEE. doi:10.1109/BigData47090.2019.9006455.

[21] S. Kirrane, J.D. Fernández, P. Bonatti, U. Milosevic, A. Polleres and R. Wenning, The SPECIAL-K Personal Data Processing Transparency and Compliance Platform, *arXiv preprint arXiv:2001.09461* (2020).

[22] A. Toumia, S. Szoniecky and S. Imad, ColPri: Towards a Collaborative Privacy Knowledge Management Ontology for the Internet of Things, *Fifth International Conference on Fog and Mobile Edge Computing (FMEC)* (2020), 150–157. doi:10.1109/FMEC49853.2020.9144927.

[23] K. Fatema, E. Hadziselimovic, H.J. Pandit, C. Debruyne, D. Lewis and D. O'Sullivan, Compliance through Informed Consent: Semantic Based Consent Permission and Data Management Model, *Privacy and the Semantic Web - Policy and Technology workshop (PrivOn 2017).co-located with ISWC 2017* (2017).

[24] H.J. Pandit, C. Debruyne, D. O'Sullivan and D. Lewis, GConsent - A Consent Ontology Based on the GDPR, *The Semantic Web. ESWC 2019. Lecture Notes in Computer Science* **11503** (2019), 270–282. doi:10.1007/978-3-030-21348-0_18.

[25] F. Loukil, C. Ghedira, K. Boukadi and A. Benharkat, LIoPY: A Legal Compliant Ontology to Preserve Privacy for the Internet of Things, *IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)* **02** (2018), 701–706. doi:10.1109/COMPSAC.2018.10322.

[26] N.S. Grid, Introduction to NISTIR 7628 guidelines for smart grid cyber security, *Guideline, Sep* (2010).

[27] P.A. Bonatti, S. Kirrane, I. Petrova, L. Sauro and E. Schlehahn, SPECIAL Deliverable D2.1, Policy Language V1, 2017, Last Accessed 01-10-2020. https://www.specialprivacy.eu/images/documents/SPECIAL_D21_M12_V10.pdf.

[28] S. Kirrane, J.D. Fernández, P. Bonatti, U. Milosevic, A. Polleres and R. Wenning, The SPECIAL-K Personal Data Processing Transparency and Compliance Platform, *arXiv:2001.09461* (2020). http://arxiv.org/abs/2001.09461.

[29] A. Bechmann, Non-Informed Consent Cultures: Privacy Policies and App Contracts on Facebook, *Journal of Media Business Studies* **11**(1) (2014), 21–38. doi:10.1080/16522354.2014.11073574.

[30] R.F. Joergensen, The unbearable lightness of user consent, *Internet Policy Review* **3** (2014). doi:10.14763/2014.4.330.

[31] A. Dix, Human-Computer Interaction, in: *Encyclopedia of Database Systems*, 2018.

[32] J. Angulo, S. Fischer-Hübner, T. Pulls and E. Wästlund, Usable Transparency with the Data Track, *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (2015), 1803–1808. doi:10.1145/2702613.2732701.

[33] P. Raschke, A. Küpper, O. Drozd and S. Kirrane, Designing a GDPR-Compliant and Usable Privacy Dashboard, *Privacy and Identity Management. The Smart Revolution. Privacy and Identity 2017. IFIP Advances in Information and Communication Technology* (2017). doi:10.1007/978-3-319-92925-5_14.

[34] O. Drozd and S. Kirrane, I Agree: Customize Your Personal Data Processing with the CoRe User Interface, *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (2019), 17–32. ISBN 9783030278120. doi:10.1007/978-3-030-27813-7_2.

[35] O. Drozd and S. Kirrane, Privacy CURE: Consent Comprehension Made Easy, *35-th IFIP International Conference on ICT Systems Security and Privacy Protection* (2020). ISBN 978-3-030-58200-5. doi:10.1007/978-3-030-58201-2_9.

[36] J. Nielsen, The Usability Engineering Life Cycle, *IEEE Xplore Computer* **25** (1992), 12–22. doi:10.1109/2.121503.

[37] M.-R. Ulbricht and F. Pallas, CoMaFeDS: Consent Management for Federated Data Sources, *2016 IEEE International Conference on Cloud Engineering Workshop (IC2EW)* (2016), 106–111. doi:10.1109/IC2EW.2016.30.

[38] S. Tokas and O. Owe, A Formal Framework for Consent Management, *International Conference on Formal Techniques for Distributed Objects, Components, and Systems* (2020), 169–186.

[39] K. Rantos, G. Drosatos, K. Demertzis, C. Ilioudis, A. Papanikolaou and A. Kritsas, ADvoCATE: a consent management platform for personal data processing in the IoT using blockchain technology, *International Conference on Security for Information Technology and Communications* (2018), 300–313, Springer. doi:10.1007/978-3-030-12942-2_23.

[40] C. Bartolini, R. Muthuri and C. Santos, Using Ontologies to Model Data Protection Requirements in Workflows (2017), 233–248. ISBN 978-3-319-50953-2.

[41] Fuzzy cognitive maps, *International Journal of Man-Machine Studies* **24**(1) (1986), 65–75. doi:10.1016/S0020-7373(86)80040-2.

[42] V. Jaiman and V. Urovi, A Consent Model for Blockchain-Based Health Data Sharing Platforms, *IEEE Access* **8** (2020), 143734–143745. doi:10.1109/ACCESS.2020.3014565.

[43] J. Woolley, E. Kirby, J. Leslie, F. Jeanson, M.N. Cabili, G. Rushton, J.G. Hazard, V. Ladas, C. Veal, S.J. Gibson, A.-M. Tassé, S. Dyke, C. Gaff, A. Thorogood, B. Knoppers, J. Wilbanks and A. Brookes, Responsible sharing of biomedical data and biospecimens via the "Automatable Discovery and Access Matrix" (ADA-M), *NPJ Genomic Medicine* **3** (2018). doi:10.1038/s41525-018-0057-4.

[44] A. Mahindrakar, K.P. Joshi et al., Automating GDPR Compliance using Policy Integrated Blockchain, *IEEE 6th International Conference on Big Data Security on Cloud (BigDataSecurity 2020)* (2020). doi:10.1109/BigDataSecurity-HPSC-IDS49724.2020.00026.

[45] K.P. Joshi, A. Gupta, S. Mittal, C. Pearce, A. Joshi and T. Finin, Semantic approach to automating management of big data privacy policies, *IEEE International Conference on Big Data (Big Data)* (2016), 482–491, IEEE. doi:10.1109/BigData.2016.7840639.

[46] M. Lizar and D. Turner, Consent Receipt Specification v1.1.0, Technical Report, Kantara Initiative, 2017.

[47] B.M. Gross., The Managing of Organizations: The Administrative Struggle, *The ANNALS of the American Academy of Political and Social Science* **360**(1) (1965), pp. 197–198. doi:10.1177/000271626536000140.

[48] N. Noy, Ontology Development 101: A Guide to Creating Your First Ontology, 2001.

[49] D. Kalibatiene and O. Vasilecas, Survey on Ontology Languages, *Lecture Notes in Business Information Processing* **90** (2011), 124–141. doi:10.1007/978-3-642-24511-4_10.

[50] M.H. Frické, Encyclopedia of Big Data. Data-Information-Knowledge-Wisdom (DIKW) Pyramid, Framework, Continuum (2018), 1–4. ISBN 978-3-319-32001-4. doi:10.1007/978-3-319-32001-4_331-1.

[51] J. Vassileva, Motivating participation in social computing applications: A user modeling perspective, *User Modeling and User-Adapted Interaction* **22** (2012), 177–201. doi:10.1007/s11257-011-9109-5.

[52] A. Marwick and E. Hargittai, Nothing to hide nothing to lose Incentives and disincentives to sharing information with institutions online, *Information, Communication & Society ISSN:* **22** (2019), 1697–1713. doi:https://doi.org/10.1080/1369118X.2018.1450432.

[53] Cambridge University, Transparencies, Last Accessed 10-10-2020. https://www.cl.cam.ac.uk/~jac22/books/ods/ods/node18.html.

[54] R.B. Woodruff, E. Cadotte and R. Jenkins, Modeling Consumer Satisfaction Processes Using Experience-Based Norms, *Journal of Marketing Research* **20** (1983), 296–304. doi:10.2307/3151833.

[55] S. Kirrane, P. Bonatti, J.D. Fernández, C. Galdi, L. Sauro, D. Dell'Erba, I. Petrova and I. Siahaan, Transparency and Compliance Algorithms V2, Last Accessed 13-10-2020. https://www.specialprivacy.eu/images/documents/SPECIAL_D28_M23_V10.pdf.

[56] L. Lee, C. Heilig and A. White, Ethical Justification for Conducting Public Health Surveillance Without Patient Consent, *American journal of public health* **102** (2011), 38–44. doi:10.2105/AJPH.2011.300297.

[57] M. Cuquet and A. Fensel, The societal impact of big data: A research roadmap for Europe, *Technology in Society* **54** (2018), 74–86–. doi:10.1016/j.techsoc.2018.03.005.

[58] A. Jabbar and S. Dani, Investigating the link between transaction and computational costs in a blockchain environment, *International Journal of Production Research* **58**(11) (2020), 3423–3436.

[59] L.A. Franke, M. Schletz and S. Salomo, Designing a Blockchain Model for the Paris Agreement's Carbon Market Mechanism, *Sustainability* **12**(3) (2020), 1068.

[60] F.R. Batubara, J. Ubacht and M. Janssen, Challenges of blockchain technology adoption for e-government: a systematic literature review, in: *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age*, 2018, pp. 1–9.

[61] L. Jehl and A. Friel, CCPA and GDPR Comparison Chart, *Practical Law* (2018). https://iapp.org/media/pdf/resource_center/CCPA_GDPR_Chart_PracticalLaw_2019.pdf.

[62] D. Fensel, U. Şimşek, K. Angele, E. Huaman, E. Kärle, O. Panasiuk, I. Toma, J. Umbrich and A. Wahler, *Knowledge Graphs. Methodology, Tools and Selected Use Cases*, Springer, 2020. ISBN 978-3-030-37439-6.