Test-driven Approach Towards GDPR Compliance

This paper has been accepted for publication at SEMANTiCS 2019. Preprint shared under CC-by-4.0

Harshvardhan J. Pandit, Declan O'Sullivan, and Dave Lewis

ADAPT Centre, Trinity College Dublin, Dublin, Ireland
{pandith|declan.osullivan|dave.lewis}@tcd.ie

Abstract. An organisation using personal data should document its data governance processes to maintain and demonstrate compliance with the General Data Protection Regulation (GDPR). As processes evolve, their documentation should reflect these changes with an assessment showing ongoing compliance. Through this paper, we show how semantic representations of processes are useful towards maintaining ongoing GDPR compliance by using a test-driven approach that generates and checks constraints for adherence to GDPR requirements. We first check whether all required information has been documented, and then whether it is compliant. We prototype our testing approach using a real-world website's consent mechanism for GDPR compliance, and persist results towards generating documentation. We use previously-published ontologies to represent processes (GDPRov), consent (GConsent), and GDPR (GDPRtEXT), with SHACL used to test requirement constraints.
Paper and Resources: https://w3id.org/GDPRep/semantic-tests.

Keywords: GDPR · GDPR compliance · consent · SHACL

1 Introduction

Demonstrating compliance towards the General Data Protection Regulation (GDPR) [17] requires documenting information regarding how its various obligations and requirements were met. GDPR explicitly requires documentation of information for records of processing activities (R82, A30), consent (R42, A7-1), and impact assessment (DPIA (A35)). It also requires controllers to implement and periodically review appropriate measures regarding processing (A5-1, A24). Therefore the process of assessing, maintaining, and demonstrating compliance with the GDPR is tightly coupled with operational workflows involving personal data.

Processes change and evolve over time - such as the purpose may change, or the same process is used for other additional purposes, or the assigned processor changes. For GDPR compliance, each such change needs to be documented as a temporally versioned record of processing to demonstrate compliance regarding processing activities at that period in time. It would be considered prudence or good practice to show that the specific change was assessed and verified to be compliant before proceeding with it. This is mandatory under GDPR for certain situations requiring a DPIA (A35).

Semantics, and by extension the semantic-web, has been demonstrated to be of assistance in the management of GDPR compliance. Existing work addresses modelling machine-readable metadata for compliance [8,11,13,14], querying for compliance-related information [16], and maintaining compliant processing logs [8]. Interoperable semantics are beneficial when information is shared between stakeholders such as - controllers and processors, or controllers and certification bodies or supervisory authorities. The interoperability is also helpful towards transparency regarding processing activities to address the discrepancy between requirements of an organisation and compliance [18]. A discussion of four areas where automation can be applied [7], one of which is compliance using checklists, shows possible avenues for further incorporating semantics into the compliance process.

In this paper, we show how semantic representation of processes are useful in a test-driven approach for documenting ongoing compliance with the GDPR. We describe our approach towards generating and testing constraints based on requirements gathered from GDPR and the use of semantics to generate documentation linked with the GDPR. The paper also presents an application of this approach by testing a website's consent mechanism for GDPR compliance and generating compliance documentation. For this, we build on our previous work including ontologies to represent processes (GDPRov [14]), consent (GConsent [12]), and GDPR (GDPRtEXT [13]), and an approach to turn compliance questions into semantic queries [16]. An overview of this was presented in a prior publication [15].

2 Approach

2.1 Generating constraints from requirements

The first step towards compliance is selecting applicable clauses from the GDPR and converting them into tangible requirements. Resources useful for this include information and guidance provided by Data Protection Authorities and professional institutes. Information pertaining to the fulfilment of these requirements is required for compliance documentation.

The next step is to identify information required to assess whether requirements have been met, and then generate constraints that check a) presence of that information, and b) verify its correctness. For the purposes of this paper, we focus on the legal basis of given consent, with a subset of the requirements and constraints presented in Table 1. Checking for presence of information before verification of correctness follows a closed-world assumption where absence of information indicates non-compliance.

Table 1. Subset of Constraints and Assumptions regarding Given Consent

GDPR	Constraint
A4-11	Consent must be associated with only one Data Subject
R32,A4-11	Consent must have one or more categories or types of personal data associated with it
R32,R42	Consent must have one or more purposes associated with it
R32,A4-11	Consent must have one or more processing associated with it
A7-3	Consent must have one and only one state/status
A7-2	Consent is given by exactly one Person
	Given consent must have information on how it was obtained
	Consent must have artefacts associated with how it was obtained
	Consent must have information on what choices provided
	Consent must have statement or affirmative action
	Consent must have information about right to withdraw
R32,A7-2	Consent must not have more than one medium it was provided
	Consent must have a timestamp indicating when it was given
	Purpose or processing associated with Third Party must specify role played by the Third Party
	If data is being stored, it must have information on how long it will be stored for
	Storage of data must have information on its storage location
R71,A9-2c,A22-2	Automated processing of personal data must be clearly indicated
R111,A49-1a	Data transfer to third country or international organisation must specify identity of recipient
R51,A8-2a	Personal data belonging to a special category must be clearly indicated

Constraints that verify correctness, or rather conformance, to requirements are required to be implemented based on underlying information representations (e.g. ontology). Some constraint assessments can be automated whereas others require human intervention, particularly where qualitative requirements are involved. For example, informed consent requires the request to be clear and unambiguous - which needs to be evaluated manually[1].

A test for compliance contains verification of (one or more) constraints where results indicate compliance with identified requirements. By linking the constraint with relevant points or concepts within GDPR, it is possible to generate and document 'coverage' of compliance. For example, for constraints generated from identified requirements, by having their results linked to the GDPR, the number of tests passed indicates compliance with set of linked GDPR points or articles.

[1] While it may be possible to use NLP-based approaches to evaluate the complexity of language to determine whether it is clear and unambiguous, such approaches cannot be assumed to be universally applicable, and therefore require a manual assessment.

Constraints can be linked to each other to formulate dependency relationships. This can make testing for compliance more efficient by identifying common dependencies. It also allows creating logical groupings of related constraints. Such groupings can be based on functionality or relation to GDPR such as association with one concept or one specific article. For example, requirements for validity of consent are grouped from individual constraints for each requirement (e.g. clear, unambiguous), with requirements for explicit consent containing only additional constraints along with the group for valid consent.

2.2 Model of processes

Representing a model or template of processes as machine-readable metadata has advantages in terms of ex-ante verification of compliance. This allows creating constraints that specifically check whether the model of processes follows the requirements gathered from GDPR. This is distinct from verification of compliance using records or logs of processing which constitute as ex-post compliance. For example, verifying whether the consent collection mechanism follows requirements for valid consent is done by representing the mechanism as a model and checking constraints associated with validity of given consent.

The model also allows testing for existence of internal processes regarding handling of data subject rights and data breaches. The metadata representation of model enables creating a persistent snapshot of processes for planning, conducting an impact assessment (DPIA), and inspecting past compliance. Additionally, creating and testing a model allows abstraction of information common to instances such as notice or dialogue for consent - which is common to all or a significant number of data subjects. By abstracting such common information into the model of the process, actual instances of given consent need to be linked only with the relevant attributes and can refer to the model for more information regarding compliance.

Using models also makes the testing process more efficient in terms of reducing the number of tests to be conducted. If a model is verified to be compliant using prior testing, then its instances can be verified to be compliant using only the constraints specific to the instance. For example, when verifying compliance for processing using given consent as a legal basis, the validity of given consent also needs to be evaluated. By abstracting the model of collecting consent and verifying it to be compliant, the given consent used in processing is assumed to be valid. The only constraint that needs to be tested is therefore whether the processing is permitted based on the interpretation of given consent.

2.3 Testing and Documentation

The requirements and constraints by themselves are universal in that they can be expressed without dependence on any technology or information representation. Adapting constraints into an testing framework requires basing it on the underlying models and information representations. For example, where information is defined using RDF+OWL, the testing framework is created using relevant technologies that can query and validate RDF+OWL - such as using SPARQL[19] and SHACL[9] respectively. In this case, the information format (RDF) itself enables the use of semantics which assists in linking the information, constraints, and results with points of relevance within the GDPR. Where the underlying information format does not inherently supporting semantics, these can be added as metadata to the test results to link them with GDPR.

Having the information or metadata format be machine-readable and interoperable allows taking advantage of querying and validation. The testing framework needs to be aware of the vocabularies and technologies used to represent the information and should persist results using machine-readable metadata. Tests should be defined at a granular level to enable actionable constraints such as “personal data (category) should have a source”. These are then combined to create larger and more complex tests, which is similar to the creation of ‘unit’ tests and combining them into modules to test complex functionality. For example, testing whether personal data collected from users and shared with a third party with legal basis of consent adheres to given consent requires verification using constraints that test - a) source of personal data (user) b) third party identity c) legal basis, and d) matching processing with given consent.

The results of tests are associated with articles or concepts within GDPR based on the requirements used to generate constraints. Depending on the extent of machine-readable information used, it is possible to also include information such as a) representation of processes b) testing constraints c) results of internal evaluations d) text of GDPR. The end result of the testing process is a report that lists compliance with GDPR in the form of requirements (un-)fulfilled.

3 Demonstration using Use-Case

3.1 Creating the data graph

For the use-case, we chose the consent mechanism on `quantcast.com` website, depicted in Fig. 1, and modelled the data graph based on information presented in the consent dialogue and the website. The choice of website was made based on Quantcast being a provider of GDPR consent collection mechanism using the IAB consent framework[2]. The website was also one of the few (to the authors' knowledge) that allows changing/withdrawing consent using the same dialogue. We chose to include information from the website about analytics services provided by Quantcast as it uses personal data. More information on the creation of data graph is available online[3].

We used GDPRov[4] (which extends PROV-O [10] and P-Plan [3]) to model personal data and consent workflows, and GConsent[5] to model consent attributes and given consent. GDPRov allowed representing processes and personal data mentioned in the consent dialogue as models. GConsent allowed expressing consent using attributes such as medium and status. Where there was an overlap, such as for personal data and purpose, we used both to define the instance.

We collected personal data categories from the descriptions in the consent dialogue as well as other pages on the website describing various products and services offered by Quantcast. We defined the source of personal data as 'user' where data collection was mentioned in the consent dialogue, and 'third party' where explicitly defined. We defined processes for addressing the rights provided by GDPR using descriptions provided in the privacy policy. Where a URL or email address was provided regarding rights, we defined it as the IRI of the process for handling that right. We defined the IRI for DPO using the contact point provided in the policy.

We represented the consent collection mechanism on the website as an instance of *gdprov:ConsentAcquisitionStep*. This was defined as a step in the process *QChoice* representing the product Quantcast Choice. Similar processes were defined for Marketing, Advertisement, and Measurement identified from the information on the website. Each top-level description in the consent dialogue, e.g. Personalisation, was modeled as *gdprov:Purpose* and *gc:Purpose* with processing and personal data modeled from its description. The legal basis was defined using GDPRtEXT[6] and was associated at the process (purpose) or step (processing) level. We used given consent as the legal basis for purposes mentioned in the consent dialogue and legitimate interest otherwise.

In the consent dialogue, the use of independent radio buttons was interpreted as allowing the user to consent and withdraw for each individual purpose, which was represented by creating separate instances of consent for each choice. We modelled the dialogue as an instance of *gdprov:ConsentAgreementTemplateBundle* consisting of several *gdprov:ConsentAgreementTemplate* instances to represent multiple individual consent entities. We had difficulty in interpreting the language used for third parties as it suggests the user is giving consent directly to third parties rather than to Quantcast. Pending clarification from legal experts, we chose to represent these as data recipients rather than as Controllers or Joint-Controllers for ease of testing. This allowed us to represent the data sharing processes in a concise manner with each purpose being associated with the hundreds of third parties listed in the consent dialogue rather than defining a separate consent representation for every third party. For testing, we defined an instance of given consent (see Fig 2.) which was then later withdrawn. All resources associated with the data, constraints, and queries are available online[3].

3.2 Testing data graph for compliance

We defined constraints over the data graph using SHACL and its extension SHACL-SPARQL [9]. For testing, we used the SHACL validator binary provided by TopBraid[7]. To distinguish between constraints that could be verified automatically and those that required manual consideration, we subclassed *sh:NodeShape* as *AutomaticallyCheckedConstraint* and *ManuallyCheckedConstraint* where manual tests checked the value of boolean properties. For example, the value of *consentIsBySilence* indicates whether consent is given by silence with valid value being *xsd:false*. The consent collection dialogue was considered as the input for manual tests regarding validity of consent. Appropriate result messages were associated with each constraint using *sh:message*. The property *linkToGDPR* was defined to linking constraints with GDPR using GDPRtEXT. An example constraint is provided in Listing 1.

For evaluation, we defined two sets of constraints following the outline provided in the approach described in Section 2. The first set validated instances of given consent against defined constraints, whereas the second set first validated the model of consent and then validated the instances of given consent using the validated model. For the second set, results

[2] IAB Transparency and Consent Frameworkhttps://advertisingconsent.eu/

[3] Paper and Resources https://w3id.org/GDPRep/semantic-tests

[4] GDPRov Ontology https://w3id.org/GDPRov

[5] GConsent Ontology https://w3id.org/GConsent

[6] GDPRtEXT Ontology and Resource https://w3id.org/GDPRtEXT

[7] TopBraid SHACL https://github.com/TopQuadrant/shacl/

```
:WithdrawConsentConstraints a sh:NodeShape ;
    sh:targetClass m:ManualTest ;
    sh:property :WithdrawConsentEase ;
    sh:property :WithdrawConsentInformation ;
    rdfs:label "Withdraw Consent Constraints" .
:WithdrawConsentEase a sh:PropertyShape, :ManuallyCheckedConstraint ;
    :linkToGDPR gdpr:article7-3 ;
    sh:name "Ease of Withdraw Consent" ;
    sh:path m:withdrawingConsentIsAsEasyAsGivingConsent ;
    sh:hasValue true ;
    sh:message "(M) Consent should be as easy to withdraw as it is to give" .
:WithdrawConsentInformation
    a sh:PropertyShape, :ManuallyCheckedConstraint ;
    :linkToGDPR gdpr:article7-3 ;
    sh:name "Withdraw Consent Information" ;
    sh:path m:withdrawingConsentInformationBeforeGivingConsent ;
    sh:hasValue true ;
    sh:message "(M) Information about withdrawal should be provided before giving consent" .
```

Listing 1: SHACL constraints for manual tests regarding consent withdrawal

from validating the model were persisted in data graph in order to use them as input to validate given consent. A simple bash script was used to construct a pipeline that executed constraints and stored results as a *rdf/turtle* file.

For ease of evaluation, we generated a combined data graph consisting of data from Quantcast and ontologies used (GDPRov, GConsent, GDPRtEXT). We added this data graph along with results of SHACL validation to a triple-store (GraphDB Free Edition[8]) under separate graphs. We then executed SPARQL queries to query the data graph and generate reports.

We used three separate queries to facilitate different actions associated with compliance. The first query listed the distinct messages from failing tests as actionable items. The second query listed the compliance of applicable GDPR articles using links from constraints and their verification. The third query, shown in Listing 2, generated a test report, depicted in Table 2, containing the constraint description, type - automatic (A) or manual (M), link to GDPR, result - pass (P) or fail (F), node (instance in data graph), and failure message (not shown in table). The results from these queries were then used to generate a compliance report to document the state of maintaining compliance and actions required. The report contains results of queries related to compliance [16]. The documentation regarding creating the data graph, constraints, and testing, along with the SPARQL queries and generated report is available online[3]. 3.

4 Related Work

The approach presented in this paper acts on machine-readable metadata representation of processes and workflows associated with personal data and consent. An alternative to this is an approach that uses ODRL policies [5] for assessment of compliance using questions constructed from GDPR [1]. The ODRL policy consists of constraints classified as *Feature*, *Discretional*, and *Dispensation* with *Rule* used to specify them as *Permission*, *Prohibition*, or *Duty*. The policies are linked to the relevant text in GDPR using RDF properties similar to the use of GDPRtEXT in this paper. The questions are used in a tool that incorporates human feedback and generates an assessment report. This is useful to incorporate the manual testing requirements from our approach, as well as to present the results from validation as a feedback process.

The Scalable Policy-aware Linked Data Architecture For Privacy, Transparency and Compliance (SPECIAL) is an European H2020 project that provides a semantic-web framework for the generation of logs that enable ex-post GDPR compliance verification [8]. Their compliance engine can also be used to perform ex-ante compliance checks [2] using a model-based approach similar to the one advocated by GDPRov. The compliance assessment in SPECIAL focuses on determining whether the specified use of purposes, processes, and personal data is allowed by the specified legal basis such as consent. This can be incorporated in our approach to determine the validity of constraints related to use of given consent for data processing operations.

Other related work includes PrOnto [11] - a legal ontology of concepts related to privacy agents, personal data types, processing operations, rights and obligations. Based on the examples shown in its associated publications, PrOnto can be used

[8] GraphDB Triple-Store http://graphdb.ontotext.com/

Table 2. Report showing constraints, validation results, and link to GDPR

Name	Type	GDPR	Result	Node
Consent ≠ Inactivity	M	R32	P	
Consent ≠ Pre-ticked Boxes	M	R32	P	
Consent ≠ Silence	M	R32	P	
Consent → Data Subject	A	A4-11	P	
Consent → Given To	A		P	
Consent → Location	A		P	
Consent → Medium	A	A7-2	P	
Consent → Personal Data	A	A4-11,R32	P	
Consent → Processing	A	A4-11,R32	P	
Consent → Provided By	A	A7-2	P	
Consent → Purpose	A	R32,R42	P	
Consent → Status	A		P	
Consent → Timestamp	A		F	Q:Consent20190415120753
Consent → Timestamp	A		F	Q:Consent20190415140000
Consent ≡ Choice	M		P	
Consent ≡ Freely Given	M	A4-11	P	
Consent ≡ Specific	M	A4-11	P	
Consent ≡ Statement of Clear Action	M	A4-11	P	
Consent ≡ Unambigious	M	A4-11	P	
Consent Generating Activity	A		P	
Consent Request ≡ Clear	M	R32	P	
Consent Request ≡ Concise	M	R32	P	
Consent Request ≡ Not Disruptive	M	R32	P	
Consent Template	A		P	
Ease of Withdraw Consent	M	A7-3	P	
Many Processing x One Purpose	A	R32	P	
One Processing x Many Purposes	A	R32	F	Q:Consent20190415120753
One Processing x Many Purposes	A	R32	F	Q:Consent20190415140000
Personal Data → Storage Period	A	A13-2-a	F	Q:CATQInfoStorageAccess
Personal Data → Storage Period	A	A13-2-a	F	Q:CATTPInfoStorageAccess
Personal Data → Storage Period	A	A13-2-a,R39	F	Q:Consent20190415120753
Personal Data → Storage Period	A	A13-2-a,R39	F	Q:Consent20190415140000
Right to Withdraw	A	A7-3	P	
Separation of Processing	M	R43	P	
Third Party Categories	A	A44	P	
Third Party Identities	A	A13-1-e	P	
Third Party Identities	A	A30-1-d	P	
Third Party Identities	A	A44	P	
Third Party Safeguards	A		P	
Withdraw Consent Information	M	A7-3	P	

```
PREFIX c: <http://example.com/Quantcast/shapes#>
PREFIX rdfs: <http://www.w3.org/2000/01/rdf-schema#>
PREFIX sh: <http://www.w3.org/ns/shacl#>
PREFIX xsd: <http://www.w3.org/2001/XMLSchema#>
SELECT DISTINCT ?name ?test ?gdpr ?result ?node ?msg
WHERE {
    ?x a c:Constraint .
    ?x sh:name ?name .
    BIND(IF(EXISTS{
        ?x a c:AutomaticallyCheckedConstraint},
        "Automatic"^^xsd:string, "Manual"^^xsd:string)
        as ?test)
    OPTIONAL { ?x c:linkToGDPR ?gdpr }
    BIND(IF(EXISTS{
        ?y sh:sourceConstraint ?x},
        "FAIL"^^xsd:string, "PASS"^^xsd:string)
        as ?result)
    OPTIONAL {
        FILTER EXISTS { ?y sh:sourceConstraint ?x }
        ?y sh:focusNode ?node .
            ?y sh:resultMessage ?msg .
        }
} ORDER BY ?name
```

Listing 2: SPARQL query for report listing validation results linked with GDPR

to define the underlying data graph and the constraints for compliance validation. The W3C Community Group for Data Protection Vocabularies and Controls[9] (DPVCG) is currently working on taxonomies for purposes, data processing, consent, personal data, technical and organisational measures, and legal basis which will provide a vocabulary for the representation and documentation of such processes. Layered Privacy Language (LPL) [4] can be used to model privacy properties such as personal privacy, user consent, data provenance, and retention management for the GDPR, and can be used to define the constraints using its authorisation-based modeling.

5 Discussion

In this section, we provide a broad discussion of how our test-driven approach can be used as a practical tool by stakeholders and the challenges in its adoption for real-world cases. Considering that processes and activities in an organisations are traditionally documented without semantics, it could be tedious and cumbersome to adopt the semantic-web based framework described in this paper. However, as mentioned earlier, the test-based approach can also be used with existing representations by adding semantics to the test results and reports to link them with relevant information such as the articles in GDPR. This is also applicable towards persisting outputs of reports generated from tools [1] and conformity assessments (CAP) [6].

The advantages of representing processes with semantics goes beyond testing for compliance as representation of processes are also useful for planning of operations and internal documentation. Semantic representations of processes can assist in automating the generation of documentation such as privacy policies where processes are listed along with their purpose, legal basis, and use of personal data. Privacy policy generators that generate boilerplate policies exist online, but do not incorporate semantics. The use of semantics allows queryable machine-readable metadata that can be used in tools towards understanding and evaluating complex policies for users and authorities.

The modeling of third parties as data recipients in Section 3.1 shows the challenges in representing complexities when it comes to GDPR compliance. A report of cases regarding data protection [20] further shows instances where individual use-cases differ significantly, which could indicate that an universal ontology to represent such processes may not be feasible. A more practical approach could be to create taxonomies and use them in ontology design patterns for compliance. The DPVCG taxonomies could be used alongside existing ontologies to create compliance design patterns to address GDPR requirements. This follows open technological solutions such as the SPECIAL project that drive adoption of semantics in the regulatory compliance space.

[9] DPVCG https://www.w3.org/community/dpvcg/

6 Conclusion

This paper demonstrates the benefits of using a test-driven approach towards maintaining ongoing GDPR compliance by using semantic representations of processes. The approach generates and checks constraints for adherence to GDPR requirements and persists the results towards compliance documentation. The prototype demonstration provides an example of testing using a real-world website's consent mechanism using previously-published ontologies to represent processes (GDPRov), consent (GConsent), and GDPR (GDPRtEXT), with SHACL used to test requirement constraints.

In conclusion, the generation of compliance reports by incorporating semantics into the testing process is useful to maintain and document the state of compliance at a given time as well as to demonstrate the ongoing compliance for changes to the data processes within an organisation. While the demonstration in this paper only covers a small set of requirements for GDPR, namely those associated with given consent, it is sufficient to demonstrate the value of the approach and the use of semantics for compliance.

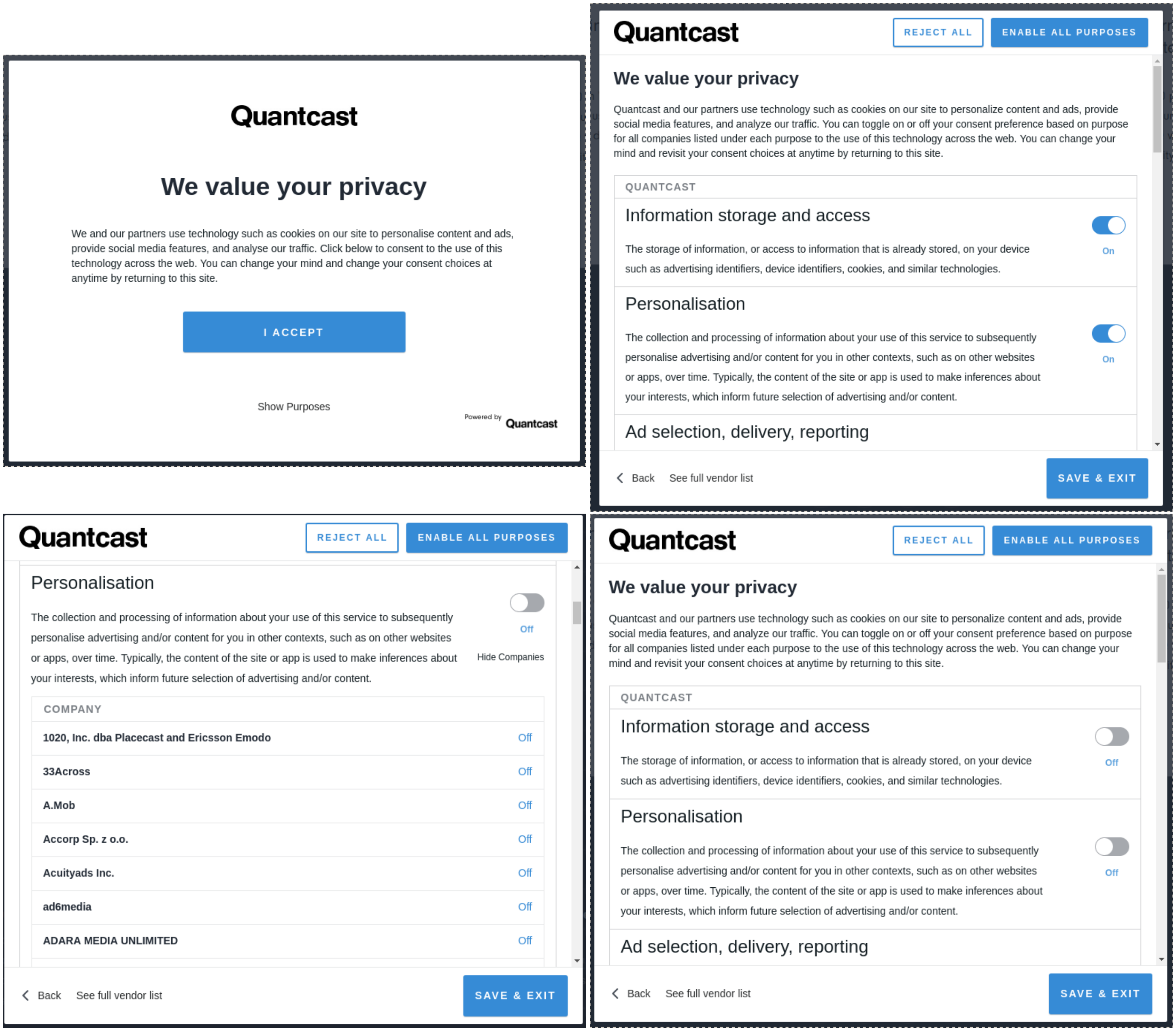
Acknowledgements

This work is supported by the ADAPT Centre for Digital Content Technology which is funded under the SFI Research Centres Programme (Grant 13/RC/2106) and is co-funded under the European Regional Development Fund.

References

1. Agarwal, S., Steyskal, S., Antunovic, F., Kirrane, S.: Legislative Compliance Assessment: Framework, Model and GDPR Instantiation. In: Medina, M., Mitrakas, A., Rannenberg, K., Schweighofer, E., Tsouroulas, N. (eds.) Privacy Technologies and Policy. pp. 131–149. Lecture Notes in Computer Science, Springer International Publishing (2018)
2. Fernández, J.D., Ekaputra, F.J., Ruswono, P., Kiesling, E., Azzam, A.: Privacy-aware Linked Widgets. In: 1st Workshop on Fairness, Accountability, Transparency, Ethics, and Society on the Web. In conjunction with The Web Conference 2019. p. 8 (2019)
3. Garijo, D., Gil, Y.: The P-Plan Ontology (Mar 2014), http://vocab.linkeddata.es/p-plan/
4. Gerl, A., Bennani, N., Kosch, H., Brunie, L.: LPL, Towards a GDPR-Compliant Privacy Language: Formal Definition and Usage. In: Hameurlain, A., Wagner, R. (eds.) Transactions on Large-Scale Data- and Knowledge-Centered Systems XXXVII, pp. 41–80. Lecture Notes in Computer Science, Springer Berlin Heidelberg, Berlin, Heidelberg (2018). https://doi.org/10.1007/978-3-662-57932-9_2, https://doi.org/10.1007/978-3-662-57932-9_2
5. Iannella, R., Villata, S.: ODRL Information Model 2.2 (Feb 2018), https://www.w3.org/TR/odrl-model/
6. Kamara, I., Leenes, R., Lachaud, E., Stuurman, K., van Lieshout, M., Bodea, G.: Data Protection Certification Mechanisms - Study on Articles 42 and 43 of the Regulation (EU) 2016/679. Tech. rep., Directorate –General for Justice and Consumers, Unit C.3 Data Protection and Unit C.4 International Data Flows and Protection (Feb 2019)
7. Kingston, J.: Using artificial intelligence to support compliance with the general data protection regulation. Artificial Intelligence and Law **25**(4), 429–443 (Dec 2017). https://doi.org/10/gfxvtc, https://link.springer.com/article/10.1007/s10506-017-9206-9
8. Kirrane, S., Fernández, J.D., Dullaert, W., Milosevic, U., Polleres, A., Bonatti, P., Wenning, R., Drozd, O., Raschke, P.: A Scalable Consent, Transparency and Compliance Architecture. In: Proceedings of the Posters and Demos Track of the Extended Semantic Web Conference (ESWC 2018) (2018). https://doi.org/10/gfxvsf
9. Knublauch, H., Kontokostas, D.: Shapes Constraint Language (SHACL), https://www.w3.org/TR/shacl/
10. Lebo, T., Sahoo, S., McGuinness, D., Belhajjame, K., Cheney, J., Corsar, D., Garijo, D., Soiland-Reyes, S., Zednik, S., Zhao, J.: PROV-O: The PROV Ontology (2013)
11. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: PrOnto: Privacy Ontology for Legal Reasoning. In: Kő, A., Francesconi, E. (eds.) Electronic Government and the Information Systems Perspective. pp. 139–152. Lecture Notes in Computer Science, Springer International Publishing (2018)
12. Pandit, H.J., Debruyne, C., O'Sullivan, D., Lewis, D.: GConsent - A Consent Ontology based on the GDPR (in-press,to-appear). In: 16th European Semantic Web Conference (ESWC 2019). Porotoz, Slovenia (2019), http://openscience.adaptcentre.ie/ontologies/gconsent/main.html
13. Pandit, H.J., Fatema, K., O'Sullivan, D., Lewis, D.: GDPRtEXT - GDPR as a Linked Data Resource. In: The Semantic Web - European Semantic Web Conference. pp. 481–495. Lecture Notes in Computer Science, Springer, Cham (Jun 2018). https://doi.org/10/c3n4, https://link.springer.com/chapter/10.1007/978-3-319-93417-4_31
14. Pandit, H.J., Lewis, D.: Modelling Provenance for GDPR Compliance using Linked Open Data Vocabularies. In: Proceedings of the 5th Workshop on Society, Privacy and the Semantic Web - Policy and Technology (PrivOn2017) (PrivOn) (2017), http://ceur-ws.org/Vol-1951/PrivOn2017_paper_6.pdf

15. Pandit, H.J., O'Sullivan, D., Lewis, D.: Exploring GDPR Compliance Over Provenance Graphs Using SHACL. In: Proceedings of the Posters and Demos Track of the 14th International Conference on Semantic Systems co-located with the 14th International Conference on Semantic Systems (SEMANTiCS 2018). Vienna, Austria (2018), http://ceur-ws.org/Vol-2198/paper_120.pdf
16. Pandit, H.J., O'Sullivan, D., Lewis, D.: Queryable Provenance Metadata For GDPR Compliance. In: Procedia Computer Science. Proceedings of the 14th International Conference on Semantic Systems 10th – 13th of September 2018 Vienna, Austria, vol. 137, pp. 262–268 (Jan 2018). https://doi.org/10/gfdc6r, http://www.sciencedirect.com/science/article/pii/S1877050918316314
17. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union **L119**, 1–88 (May 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC
18. Schiffner, S., Berendt, B., Siil, T., Degeling, M., Riemann, R., Schaub, F., Wuyts, K., Attoresi, M., Gürses, S.F., Klabunde, A., Polonetsky, J., Sadeh, N.M., Zanfir-Fortuna, G.: Towards a Roadmap for Privacy Technologies and the General Data Protection Regulation: A Transatlantic Initiative. In: Privacy Technologies and Policy - 6th Annual Privacy Forum, APF 2018, Barcelona, Spain, June 13-14, 2018, Revised Selected Papers. pp. 24–42 (2018). https://doi.org/10/gfxk7t, https://doi.org/10.1007/978-3-030-02547-2_2
19. SPARQL 1.1 Query Language, https://www.w3.org/TR/sparql11-query/
20. Zanfir-Fortuna, G.: Processing personal data on the basis of legitimate interests under the GDPR: Practical Cases. Tech. rep., Nymity (2018)



We value your privacy

We and our partners use technology such as cookies on our site to personalise content and ads, provide social media features, and analyse our traffic. Click below to consent to the use of this technology across the web. You can change your mind and change your consent choices at anytime by returning to this site.

We value your privacy

Quantcast and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. You can toggle on or off your consent preference based on purpose for all companies listed under each purpose to the use of this technology across the web. You can change your mind and revisit your consent choices at anytime by returning to this site.

QUANTCAST

Information storage and access — On

The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.

Personalisation — On

The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.

Ad selection, delivery, reporting

We value your privacy

Quantcast and our partners use technology such as cookies on our site to personalize content and ads, provide social media features, and analyze our traffic. You can toggle on or off your consent preference based on purpose for all companies listed under each purpose to the use of this technology across the web. You can change your mind and revisit your consent choices at anytime by returning to this site.

QUANTCAST

Information storage and access — Off

The storage of information, or access to information that is already stored, on your device such as advertising identifiers, device identifiers, cookies, and similar technologies.

Personalisation — Off

The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.

Ad selection, delivery, reporting

Personalisation — Off

The collection and processing of information about your use of this service to subsequently personalise advertising and/or content for you in other contexts, such as on other websites or apps, over time. Typically, the content of the site or app is used to make inferences about your interests, which inform future selection of advertising and/or content.

COMPANY	
1020, Inc. dba Placecast and Ericsson Emodo	Off
33Across	Off
A.Mob	Off
Accorp Sp. z o.o.	Off
Acuityads Inc.	Off
ad6media	Off
ADARA MEDIA UNLIMITED	Off

Fig. 1. Consent dialogues on `quantcast.com` (clockwise from top-left) (a) first screen (b) default options on selecting "I Accept" (c) default options on selecting "Show Purposes" (c) Third parties listed for purpose "Personalisation"

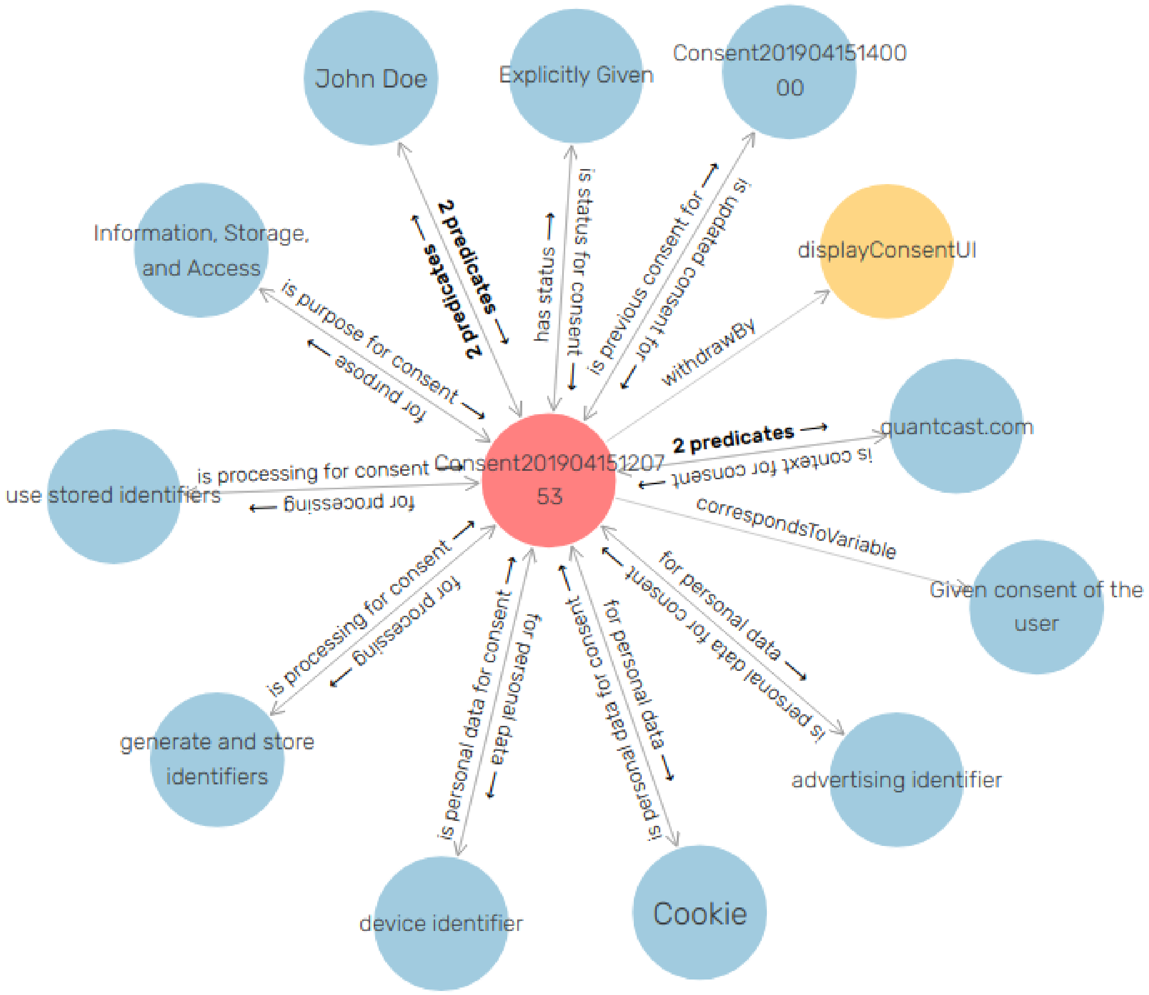


Fig. 2. Visualisation of Given Consent in the data graph (using GraphDB)

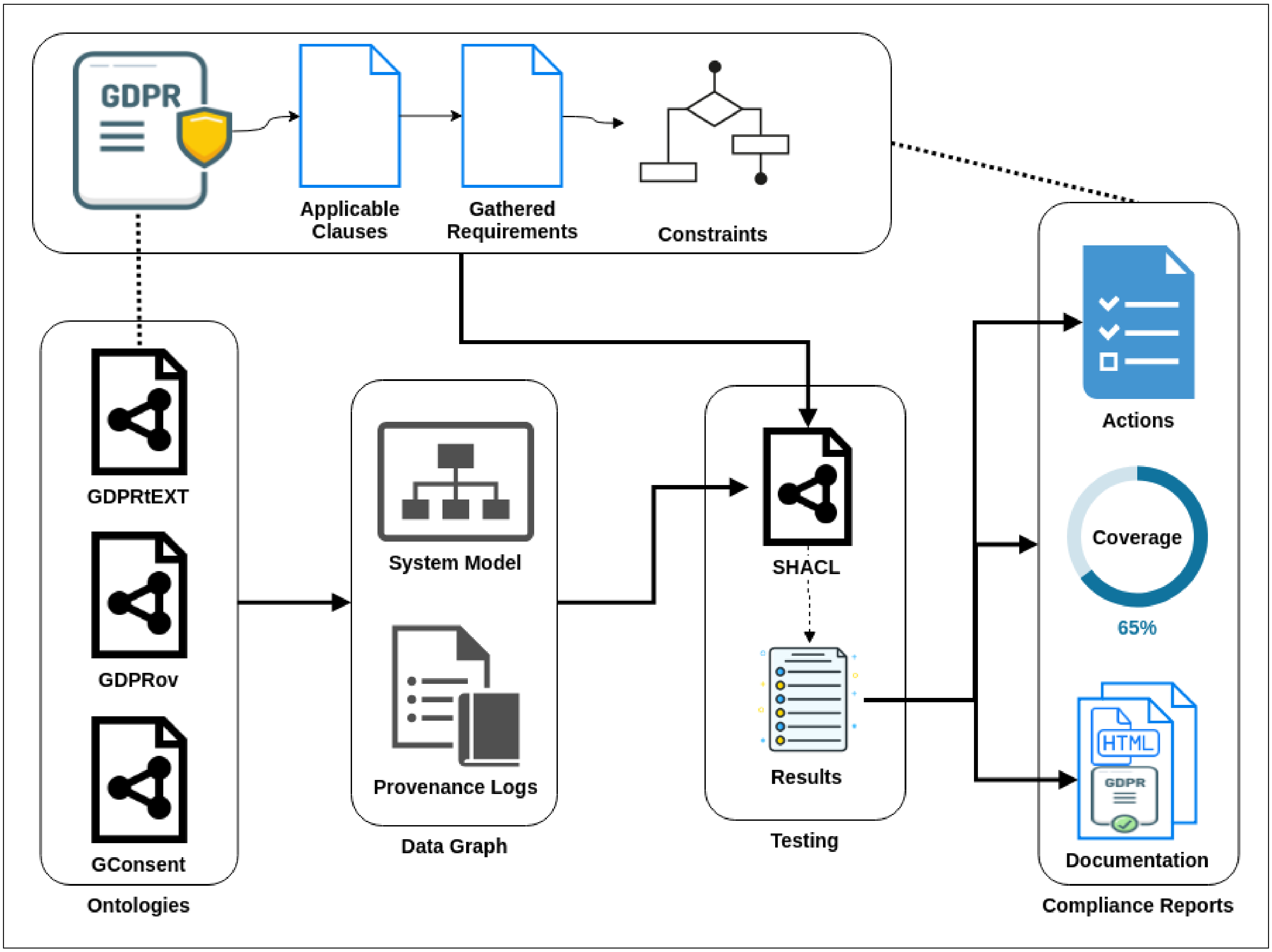


Fig. 3. Overview of testing process