SoftwareX 27 (2024) 101821

Contents lists available at ScienceDirect

SoftwareX

journal homepage: www.elsevier.com/locate/softx

Original software publication

GDPR consent management and automated compliance verification tool

Tek Raj Chhetri [a,b,*], Anna Fensel [c,d], Rance J. DeLong [e]

[a] Semantic Technology Institute (STI), Department of Computer Science, Universität Innsbruck, Innsbruck, 6020, Austria
[b] Web and Internet Science Research Group, School of Electronics and Computer Science, The University of Southampton, University Road, Highfield Campus Southampton SO17 1BJ, United Kingdom
[c] Wageningen Data Competence Center, Wageningen University & Research, Wageningen, 6708 PB, The Netherlands
[d] Consumption and Healthy Lifestyles Chair Group, Wageningen University & Research, Wageningen, 6706 KN, The Netherlands
[e] The Open Group, Reading, Berkshire, RG1 1AX, United Kingdom

ARTICLE INFO

Keywords:
GDPR
Consent management
Compliance verification
Data protection
Privacy

ABSTRACT

This paper presents our scalable and interoperable tool for GDPR (General Data Protection Regulation) consent management and automated compliance verification. The tool enables GDPR-compliant data sharing and is beneficial to the industries that process personally identifiable data. The tool has been designed following the GDPR data protection by design principles and has been successfully validated against real-world industrial use case scenarios in smart cities and insurance.

Code metadata

Current code version	v01
Permanent link to code/repository used for this code version	https://github.com/tekrajchhetri/GDPR_compliance_tool/SOFTX-D-23-00287
Legal Code License	MITLicense
Code versioning system used	git
Software code languages, tools, technology and services used	Python, SWI-Prolog, Docker, Flask, Flask-RESTful, SPARQLWrapper, GraphDB, MongoDB, Knowledge graphs and OpenFaaS
Compilation requirements, operating environments & dependencies	Python packages, Docker, OpenFaaS, GraphDB and MongoDB
Support email for questions	tekraj.chhetri@sti2.at and r.delong@opengroup.org (Prolog)

1. Motivation and significance

Data sharing is of utmost importance in today's digitized world, as it helps to unlock the data-driven economy [1], enables the development of new applications [2] and supports data-driven decision-making, such as in healthcare, smart cities, smart homes and autonomous vehicles [3,4]. For example, the sharing of Internet of Things (IoT) data in smart cities contributes to the enhancement of city services, such as city traffic and other policy-level decision making tasks.

However, as the data, for example, from the IoT in smart homes or connected vehicles, includes personally identifiable information (PII), there has been a significant concern over privacy. This has led to the adoption of one of the toughest privacy laws, the General Data Protection Regulation (GDPR) in 2018 [5]. The enforcement of GDPR in 2018 has brought about a paradigm shift in data protection and data sharing. To share or process PII data, it is necessary to comply with GDPR requirements such as obtaining consent. Failure to comply with the GDPR requirements has severe consequences, which includes a fine of *"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). A total of 900 fines totaling €1.32 billion have already been levied for not complying with GDPR [6] including to companies such as Google and Twitter.

GDPR defines six legal bases for lawful data processing: consent, contract, legal obligation, vital interests, public task, or legitimate interests (Article 6), with consent being the most common. In addition to complying with these legal bases, however, additional requirements must be met, such as the implementation of measures to protect PII data. For example, prior to any data processing activities, informed consent must be obtained from the data subject (or user) whose data is being used. However, obtaining consent is only the first step towards

* Corresponding author at: Semantic Technology Institute (STI), Department of Computer Science, Universität Innsbruck, Innsbruck, 6020, Austria.
E-mail addresses: Tek-Raj.Chhetri@uibk.ac.at (Tek Raj Chhetri), anna.fensel@wur.nl (Anna Fensel), r.delong@opengroup.org (Rance J. DeLong).

https://doi.org/10.1016/j.softx.2024.101821
Received 2 May 2023; Received in revised form 2 May 2024; Accepted 4 July 2024
Available online 15 July 2024
2352-7110/© 2024 The Author(s). Published by Elsevier B.V. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

GDPR compliance. Other requirements, such as the right to revoke consent at any time (Article 7 (3)), the implementation of the necessary technical and organizational measures (TOMs) or data protection by default (Article 25), and the demonstration of the processing of only consented data (or auditability) by the data controller (or processor) are required for authority. These requirements of GDPR have posed significant challenges, such as (i) automating compliance verification; (ii) implementing GDPR data protection by default principles; and (iii) translating the regulatory requirements like purpose limitation and storage minimization into code, and have become a factor impeding data sharing and the data economy as a whole. In addition to GDPR there are other challenges such as scalability and interoperability [7,8].

According to International Association of Privacy Professionals (IAPP) report on 2020 only 47% of the EU (European Union) companies are "fully" or "very" compliant [9], therefore there is a need for a solution that addresses the challenges posed by GDPR such as implementing data protection by default principles and preserving personal privacy while at the same time unlocking the benefits that could be obtained via data sharing. Moreover, Fery and Presidente [10] discovered similar findings in their recent (2024) study: GDPR has impacted company growth by incorporating extra burdens, such as added expenses. The challenges posed by GDPR have resulted in many works, such as [11–18] and projects like SPECIAL,[1] TRAPEZE[2] which provide the privacy-by-design framework for data sharing adhering to GDPR or performing compliance checking operations. However, these works either have different focus or limitations. For example, the work of Ranise et al. [11] was done before GDPR was enacted and is therefore limited. Also, Robol et al. [12] have proposed a privacy-by-design framework but have left implementation to future work. The work of Brodin et al. [13] does not provide automation, and Truong et al.'s [15] work needs to focus on interoperability. Moreover, Bonatti et al. [14] designed a scalable reasoner to provide real-time compliance checking, thereby addressing the SPECIAL's use cases, such as telecom scalability requirements. They also use the description logic policy language to formalize consent and data controller policies. However, their work mainly focuses on the reasoner and does not cover other aspects of GDPR, such as TOMs, the focus of this work. Most importantly, most work does not implement TOMs nor address interoperability issues [15], that our work addresses. Furthermore, our work addresses business case-specific challenges, such as the broken consent chain in the insurance industry due to ownership transfer [19].

In this paper we present our tool that facilitates consent management tasks such as consent creation, revocation, and automated compliance verification to enable GDPR compliant data sharing and processing. The tool adheres to GDPR requirements: lawfulness, fairness, and transparency (Article 5(1)(a)), purpose limitation (Article 5(1)(b)), data minimization (Article 5(1)(c)), storage minimization (Article 5(1)(e)), and accuracy, integrity, confidentiality, storage limitation, and accountability (Article 5(1)(d), Article 5(1)(e), Article 5(1)(f), and Article 5(2)). In addition, the design of the tool follows the principles of data protection by design [7]. The tool supports features such as auditability and interoperability through the use of knowledge graphs (KGs) [20] for consent representation. The tool, which is the key component of the smashHit[3] project, has been successfully tested in real-world connected-car insurance and smart city scenarios. In the smashHit project the tool is referred to as the automatic contracting tool (ACT) [21,22]. The tool enables GDPR-compliant data sharing and processing and is therefore useful for any industry that deals with PII data. Additionally, the tool allows users to view whether the data processing or sharing is in accordance with their consent, allows them to take appropriate action, and helps them to be in control of their data and privacy.

[1] https://specialprivacy.ercim.eu
[2] https://trapeze.ercim.eu/resources/
[3] https://smashhit.eu/

2. Software description

The tool follows the microservices architectural pattern, a well-established architectural pattern that permits scalability [23,24]. The scalability of the tool was evaluated by simulating 52,200 users making a maximum of 241 requests per second (minimum of 100 requests per second) [7] and by the business case partner with a simulation of 200,000 active vehicles, where the tool supported operations such as consent creation and revocation. Moreover, the tool uses Docker,[4] a containerization technology that provides portability and agility. The tool has been developed in Python,[5] except for the privacy and security service, which has been implemented in Prolog.[6] Section 2.1 provides the brief overview of the software architecture and Section 2.2 provides the overview of the functionalities. Our paper [7] and smashHit white paper [21] provide further detail about the tool.

2.1. Software architecture

Fig. 1 shows a high-level overview of the software architecture of the GDPR consent management and automated compliance verification tool. Additionally, Fig. 2 provides information on a more granular level regarding the interactions of different services (or components) of our tool as well as external entities to perform compliance check operations. The tool exposes the REST (representational state transfer) API (application programming interface) endpoints, allowing other software or applications to interact with the backend core. The core further interacts with other microservices, including the security and privacy service, the logging service, the scheduler, and the graph database, GraphDB.[7] Additionally, the logging service, which implements serverless functions using OpenFaaS,[8] interacts with MongoDB[9]. The logging service stores the tools decisions, such as consent creation and consent revocation results, which can then be used later for auditability purpose. The GraphDB is used for storing the consent information represented in KGs.

Access to the functionalities of the tool can only be made through API endpoints with valid Javascript Object Notation (JSON) Web Token(JWT)[10] tokens and organizational tokens. The organizational token is set at the time of deployment and enables role-based access to the API endpoints. Moreover, the tool implements a customizable hybrid layered encryption scheme using Rivest–Shamir–Adleman (RSA) [25] and Advanced Encryption Standard (AES) [26], thereby enabling the query of the encrypted consent information without exposing any details from the GraphDB. The security and privacy service provides domain customizable functionalities such as privacy policy comparisons and policy decision making based on an implementation of Next Generation Access Control [27], an attribute based access control standard.

2.2. Software functionalities

The tool provides the following functionalities:

- **Data protection by design:** The tool embodies the principle of data protection by design, implementing features such as secure querying over the encrypted consent information stored in the GraphDB and an adjustable hybrid multi-layered encryption scheme using RSA and AES algorithms. Moreover, the tool implements a JWT token to enable secure access to the API endpoints.

[4] https://www.docker.com/
[5] https://www.python.org/
[6] https://www.swi-prolog.org/
[7] https://www.ontotext.com/products/graphdb/
[8] https://www.openfaas.com/
[9] https://www.mongodb.com/
[10] https://jwt.io/

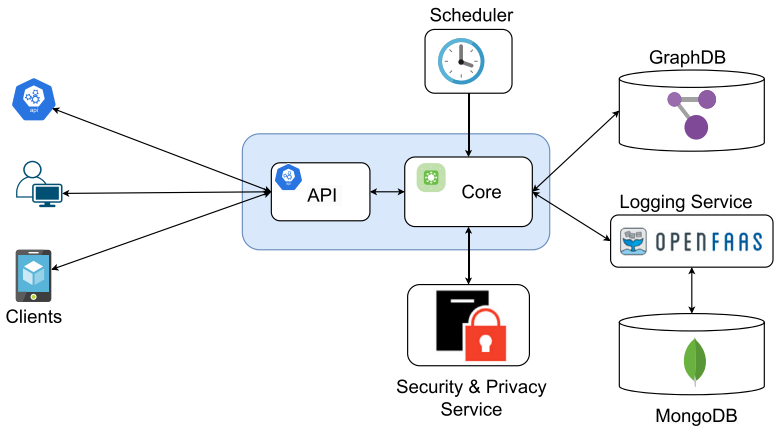

Fig. 1. Overview of the software architecture of the consent management and automated compliance verification tool.

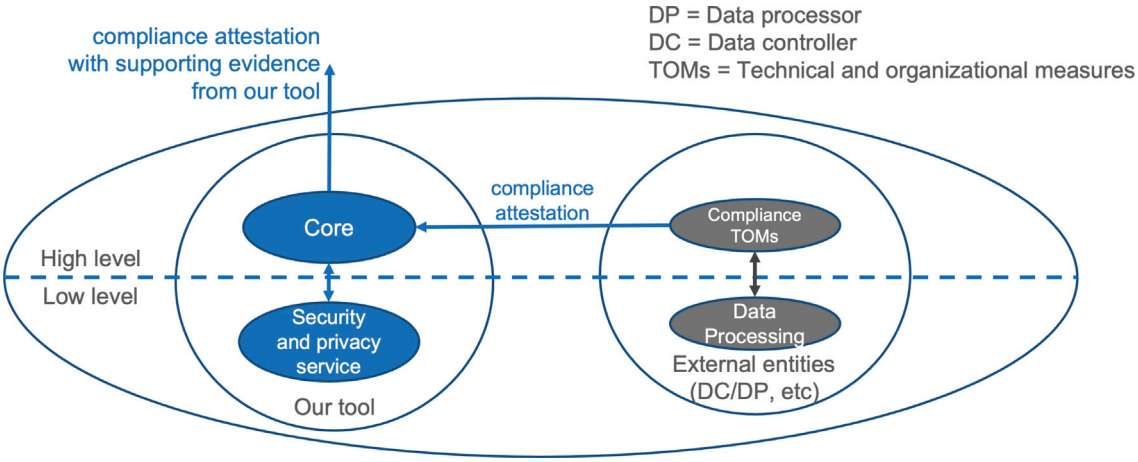

Fig. 2. Interaction between various components (or service) of our tool and external entities in order to carry out compliance checking operations.

- **Ease of integration:** The application is simple to integrate. In particular, integration can be accomplished readily via API endpoint calls. In addition, Swagger documentation[11] for API endpoints is automatically generated upon deployment, facilitating comprehension of API endpoints, their parameters and responses, further easing integration.
- **Role-based access to API endpoints:** The tool enables role-based access to the API endpoints using a decorator. Examples of role-based access include providing access only to API endpoints with view rights (e.g., view consent information) and providing access to API endpoints with create and delete permissions (e.g., consent creation and revocation).
- **Interoperability:** The tool maintains interoperability using KGs [21], which provide consistent and uniform consent representation. In particular, interoperability is achieved using the smashHitCore [28] ontology that defines the necessary concepts relating to GDPR and data processing. The smashHitCore ontology and the KGs used by the tool have been developed in collaboration with the legal team from the smashHit project. In addition, interoperability is bolstered by the use of standardized methods, such as the OpenAPI Specification[12] (formerly Swagger Specification) for REST API documentation.
- **Consent management:** The major consent management functionalities offered by the tool are: (i) the creation of consent represented by KGs; (ii) consent revocation; (iii) storing consent in a secure manner such that no information about the data subject (or consent) can be gained by a third party; and (iv) handling broken consent chains [19].
- **Event logging:** The tool logs all information, such as the actions performed by the tool for consent creation and revocation operations. These details can later be used for auditability purposes.
- **Triggering alert:** Upon the detection of a consent violation during automated compliance checks, the tool triggers an alert so that timely action can be taken. The alert is a notification that transmits a message to inform humans, such as data processors, of a data processing violation. The alert is transmitted to the software agent that has been configured to receive alert notifications.
- **Compliance verification:** The tool provides functionality to perform both manual and automated compliance verification. By adjusting the time in the scheduler, the automated compliance verification can be configured to run daily, weekly, or monthly. To perform the compliance verification, the tool also interacts with the external systems of the data controller or processor. The compliance verification task is performed against the consented information, such as data processing operations that have been consented to, the purpose, data processor privacy policies, and data subject privacy preferences [7]. The compliance verification task trusts that the external entity (data controller or processor processing PII data) is reputable and provides accurate data processing information. With this assumption, i.e., that the provided information can be relied upon and is accurate, the tool guarantees accuracy of the compliance verification, as validated by

[11] https://swagger.io/solutions/api-documentation/
[12] https://swagger.io/docs/specification/about

```python
class Revoke(MethodResource, Resource):
    @ccc_required(fresh=True)
    @doc(description='Revoke consent.', tags=['Consent'])
    @marshal_with(ReturnSchema)
    def delete(self, consent_id):
```

Fig. 3. Example of using decorator, @ccc_required, to allow role-based API endpoint access. The decorators (or roles) can be customized, i.e., added or removed as necessary, by editing the file JWTDecorator.py. The term "ccc" has no special significance; it was adopted based on the smashHit project in order to designate the research collaborator (or integrating software component from research collaborator) and can be changed as needed. The term "required" is used to denote required criteria.

regression tests with known answers. The compliance checking operation can be performed based on individual consent or based on the data subject (also referred to as the "data provider" in our work). In the case of the data provider, the compliance check is performed against all the given consents.

- **Auditing:** The tool provides auditing functionality. The auditing operations (or auditing) generate a report of all the operations performed, including the granting of consent and the results of compliance verification. Auditing can be performed either partially (a partial audit) or fully (a full aduit) based on consent or the data provider.

3. Illustrative example

The instructions for the deployment are available in the GitHub[13] repository. The details about the required input are available in the Swagger[14] documentation that is automatically generated upon successful deployment. As an illustrative example, we show four functionalities of our tool.

The first one is the enabling of role-based access to API endpoints using a decorator. Fig. 3 shows the use of the decorator to enable role-based access to a API endpoint. Similarly, the second example is the creation of consent. Listing 1 shows the input that is passed to our tool via API for the creation of the consent, and similarly, Listing 2 shows the information that is logged into the MongoDB database for consent creation operation, and Fig. 4 shows the consent in a KG representation stored in encrypted form in GraphDB.

The third example is the revocation of consent that can be performed using the consent ID (Identity Document) via the API endpoint */consent/consent_id/revoke*. Listing 3 shows the response to the revocation of consent. The fourth example is the auditing operation, which can be performed either based on consent using a consent ID or by a data provider (or data subject) using a data provider ID. Fig. 5 shows the response to the auditing operation performed based on the data provider.

Moreover, the smashHit white papers [29,30] provide more details about the insurance and the smart city use cases where our tool was tested. In addition to the white papers, video[15] demonstrations are also available on the smashHit website for connected-car insurance and smart city use cases from the use case partners LexisNexis, Volkswagen, and Arctic Machine Oy (previously Infotripla) using the smashHit platform. The smashHit platform integrates our tool at the back-end to support the demonstrated operations relating to consent to enable data sharing.

[13] https://github.com
[14] https://swagger.io
[15] https://smashhit.eu/demonstrator-videos/


```json
{
  "Agents": [
    {
      "id": "60a55c9dd79dbc757698041ea",
      "role": "controller"
    }
  ],
  "DataProcessing": [
    "analysis",
    "marketing"
  ],
  "GrantedAtTime": "2023-04-29T12:47:44.950Z",
  "Medium": "mobile",
  "Purpose": "marketing",
  "Resource": {
    "SensorDataCategory": [
      {
        "data": [
          "gps",
          "speed"
        ]
      }
    ]
  },
  "city": "Innsbruck",
  "consentid": "CS1241X581",
  "country": "Austria",
  "dataprovider": "TEST_ILLUSTRATIVE_EG",
  "expirationTime": "2023-11-30T13:01:49.617Z",
  "state": "Tyrol"
}
```


Listing 1: An example of input consent data that is passed to our tool via */consent/create* API endpoint for the creation of consent, which is then transformed into a KG representation and stored in an encrypted manner in GraphDB.

Fig. 4. KG representation of consent that is stored in GraphDB in an encrypted format.

4. Impact

While a number of studies have been conducted since the adoption of the GDPR, most of the work previously performed does not include compliance verification, does not implement TOMs, is not sufficiently scalable to meet real-world industrial requirements, and has not been tested in heterogeneous real-world use cases [7]. Our tool addresses limitations such as scalability, interoperability, consent management, and compliance verification, thereby enabling data sharing, which is crucial to economic viability and the preservation of personal privacy. The tool was a central component of the smashHit project and has also been recognized by the EU innovation radar as one of its key

```
{
    "act_status_code": 7200,
    "decision": "AUDIT_SUCCESS",
    "decision_token":
        "868069e0f07a6e7ca13b0c8ec30128b1203f5f99c82c86f4ebe44f798bab383df9f768dfdb5387846c81ee8bfb20ff555f67abf5cd627226faccad3
        f44075f43",
    "message": "{'data_provider': 'DPTEST1234', 'consent_decision': [{'_id': {'$oid': '63f7e266ff7c8ec5c5e2e245'},
        'act_status_code': 7100, 'decision': 'CONSENT_CREATION_SUCCESS', 'decision_token':
        '4bd376a288ac9661564fdb8491dae9a4a9f558f1e04bebecaaef36bf4ee6c0b4ff69bbfe00d3bbf17c22f3a45e78189da9dd6389d9114794e267707
        8cf115dea', 'timestamp': 1677189734.434367, 'consent_id': 'CID123_REVOCATIONTEST1'}], 'consent_data':
        {'CID123_REVOCATIONTEST1': [{'DataController': '60a55c9dd79dbc757698041ea'}, {'Purpose': 'marketing'}, {'Data':
        [\"SensorDataCategory-{'data': ['gps', 'speed']}\"]}, {'Duration': \"'2022-11-30 13:01:49.617000+00:00^^xsd:dateTime'\"}
        , {'DataProcessor': 'None'}, {'City': 'Innsbruck'}, {'DataProcessing': ['marketing', 'analysis']}, {'DataProvider':
        'DPTEST1234'}, {'DataRequester': 'None'}, {'Medium': 'mobile'}, {'State': 'Tyrol'}, {'Country': 'Austria'},
        {'GrantedAtTime': \"'2022-09-18 16:47:44.950000+00:00^^xsd:dateTime'\"}], 'CID123_ACT1': [{'DataController':
        '60a55c9dd79dbc757698041ea'}, {'Purpose': 'marketing'}, {'Data': [\"SensorDataCategory-{'data': ['gps', 'speed']}\"]},
        {'Duration': \"'2022-11-30 13:01:49.617000+00:00^^xsd:dateTime'\"}, {'DataProcessor': 'None'}, {'City': 'Innsbruck'},
        {'DataProcessing': ['marketing', 'analysis']}, {'DataProvider': 'DPTEST1234'}, {'DataRequester': 'None'}, {'Medium':
        'mobile'}, {'State': 'Tyrol'}, {'RevokedAtTime': \"'1677191548.544772^^xsd:dateTime'\"}, {'Country': 'Austria'},
        {'GrantedAtTime': \"'2022-09-18 16:47:44.950000+00:00^^xsd:dateTime'\"}]}}",
    "timestamp": "1677191687.475697"
}
```


Fig. 5. A snippet of response for a full audit operation based on the data provider.


```
{
  "_id": {
    "$oid": "644ba526ae697879cdf95f17"
  },
  "act_status_code": 7100,
  "decision": "CONSENT_CREATION_SUCCESS",
  "decision_token": "50ac901c67fd9fb13b07d30ad4d0d6df53d95598a0844
  5766ce646d191ab6bdba6a258309b2a313bfd5f4c812f8b77a951994fd354a0
  15d7f45ee43946c598af",
  "timestamp": 1682679077.786106,
  "consent_id": "CS1241X581"
}
```


Listing 2: A snapshot of the information logged in MongoDB for the consent creation operation.


```
{
"act_status_code":8000,
"decision":"CONSENT_REVOCATION_SUCCESS",
"decision_token":"ca4085f38cde2d68694e3e20ccba389549dc5730bd151688
e6dd364b02b309aae3ce22b50c66ae32e96af6a1f8fb9c06775f26eba90b78372
5a8b62a4d8d8fa9",
"timestamp":"1682685344.315328"
}
```


Listing 3: A snapshot of response from our tool for consent revocation.

innovations.[16] The tool can be used in practice because it was developed in close collaboration with the legal and industrial partners from the smashHit project and was successfully evaluated in heterogeneous real-world connected-car insurance [30] and smart city [29] use cases. Importantly, the tool is adaptable to other statutes, such as CCPA (California Consumer Privacy Act) and domains such as healthcare, and thus has the potential to have a greater impact. This work has resulted in a journal publication [7] and has also been the basis for other scientific works, such as [31]. In addition, a number of additional publications utilizing this work are in progress.

5. Conclusion

We have presented our scalable and interoperable GDPR consent management and automated compliance verification tool, which was developed in close collaboration with legal experts and industrial partners, and tested against real-world use case scenarios. The tool is useful for any industry that processes PII data, as it enables GDPR-compliant processing and sharing of the data. Moreover, the tool is also useful to individuals, as it helps them be aware of whether the data processing activities are happening as per their consent. The potential for the tool's commercial exploitation and standardization for the security and privacy service components are being pursued. The source code is freely available under the MIT license. As a future work, we intend to develop comprehensive documentation for the tool as well as parameterize its configuration settings via API endpoints, which will further ease the configuration setup and use of the tool.

[16] https://www.innoradar.eu/innovation/44562

CRediT authorship contribution statement

Tek Raj Chhetri: Conceptualization, Investigation, Methodology, Resources, Software, Validation, Visualization, Writing – original draft, Writing – review & editing. **Anna Fensel:** Funding acquisition, Investigation, Writing – review & editing. **Rance J. DeLong:** Conceptualization, Data curation, Formal analysis, Investigation, Resources, Software, Validation, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

The link to the source code has been included in the manuscript.

Acknowledgments

This study was supported by the smashHit European Union project, which was funded by Horizon 2020 Grant 871477. We would like to extend our gratitude to the industrial use case partners, Volkswagen AG, LexisNexis, Forum Virium Helsinki, and Infotripla, for assisting us with the project's use cases. Additionally, we want to express our gratitude for the support from the legal professionals at the University of Hannover (LUH/IRI). In addition, we would like to express our gratitude to the entire smashHit consortium, its members, as well as our former scientific publication collaborators.

References

[1] Sadowski J. When data is capital: Datafication, accumulation, and extraction. Big Data Soc 2019;6(1):2053951718820549. http://dx.doi.org/10.1177/2053951718820549.

[2] Byabazaire J, O'Hare G, Delaney D. Data quality and trust: Review of challenges and opportunities for data sharing in IoT. Electronics 2020;9(12):2083. http://dx.doi.org/10.3390/electronics9122083.

[3] Philip NY, Rodrigues JJPC, Wang H, Fong SJ, Chen J. Internet of things for in-home health monitoring systems: Current advances, challenges and future directions. IEEE J Sel Areas Commun 2021;39(2):300–10. http://dx.doi.org/10.1109/JSAC.2020.3042421.

[4] Anan SR, Hossain MA, Milky MZ, Khan MM, Masud M, Aljahdali S. Research and development of an IoT-based remote asthma patient monitoring system. J Healthc Eng 2021;2021:2192913. http://dx.doi.org/10.1155/2021/2192913.

[5] European Parliament and Council. 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). Off J Eur Union, L119 2016. URL https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[6] Daigle B, Khan M. The changing tides of data protection regulation and enforcement in Europe. Office of Industries, US International Trade Commission; 2022.
[7] Chhetri TR, Kurteva A, DeLong RJ, Hilscher R, Korte K, Fensel A. Data protection by design tool for automated GDPR compliance verification based on semantically modeled informed consent. Sensors 2022;22(7). http://dx.doi.org/10.3390/s22072763.
[8] Ryan P, Crane M, Brennan R. GDPR compliance tools: Best practice from RegTech. In: Filipe J, Śmiałek M, Brodsky A, Hammoudi S, editors. Enterprise information systems. Cham: Springer International Publishing; 2021, p. 905–29. http://dx.doi.org/10.1007/978-3-030-75418-1_41.
[9] IAPP. IAPP-FTI consulting privacy governance report 2020. Tech. rep., 2020, https://iapp.org/media/pdf/resource_center/IAPP_FTIConsulting_2020PrivacyGovernanceReport.pdf.
[10] Frey CB, Presidente G. Privacy regulation and firm performance: Estimating the GDPR effect globally, Econ Inquiry, arXiv:https://onlinelibrary.wiley.com/doi/pdf/10.1111/ecin.13213, URL https://onlinelibrary.wiley.com/doi/abs/10.1111/ecin.13213, http://dx.doi.org/10.1111/ecin.13213.
[11] Ranise S, Siswantoro H. Automated legal compliance checking by security policy analysis. In: Tonetta S, Schoitsch E, Bitsch F, editors. Computer safety, reliability, and security. Cham: Springer International Publishing; 2017, p. 361–72. http://dx.doi.org/10.1007/978-3-319-66284-8_30.
[12] Robol M, Salnitri M, Giorgini P. Toward GDPR-compliant socio-technical systems: Modeling language and reasoning framework. In: Poels G, Gailly F, Serral Asensio E, Snoeck M, editors. The practice of enterprise modeling. Cham: Springer International Publishing; 2017, p. 236–50. http://dx.doi.org/10.1007/978-3-319-70241-4_16.
[13] Brodin M. A framework for GDPR compliance for small-and medium-sized enterprises. Eur J Secur Res 2019;4(2):243–64. http://dx.doi.org/10.1007/s41125-019-00042-z.
[14] Bonatti PA, Ioffredo L, Petrova IM, Sauro L, Siahaan IR. Real-time reasoning in OWL2 for GDPR compliance. Artificial Intelligence 2020;289:103389. http://dx.doi.org/10.1016/j.artint.2020.103389, URL https://www.sciencedirect.com/science/article/pii/S0004370220301399.
[15] Truong NB, Sun K, Lee GM, Guo Y. GDPR-compliant personal data management: A blockchain-based solution. Trans Inf Sec 2020;15:1746–61. http://dx.doi.org/10.1109/TIFS.2019.2948287.
[16] Piras L, Al-Obeidallah MG, Praitano A, Tsohou A, Mouratidis H, Crespo BG-N, et al. DEFeND architecture: a privacy by design platform for GDPR compliance. In: International conference on trust and privacy in digital business. Springer; 2019, p. 78–93. http://dx.doi.org/10.1007/978-3-030-27813-7_6.
[17] Arfelt E, Basin D, Debois S. Monitoring the GDPR. In: Sako K, Schneider S, Ryan PYA, editors. European symposium on research in computer security. Cham: Springer International Publishing; 2019, p. 681–99.
[18] Vargas, Camilo J. Blockchain-based consent manager for GDPR compliance. 2019, p. 165–70, URL https://dl.gi.de/items/315873bb-470c-4190-ab0a-9abc0690863c.
[19] The smashHit project. Public report D1.3 public innovation concept. 2021, https://www.smashhit.eu/wp-content/uploads/2021/03/smashHit_D1.3_Public_Innovation_Concept_v100.pdf.
[20] Hogan A, Blomqvist E, Cochez M, D'amato C, Melo GD, Gutierrez C, et al. Knowledge graphs. ACM Comput Surv 2021;54(4). http://dx.doi.org/10.1145/3447772.
[21] smashHit consortium. Smashhit concept (white paper). 2022, http://dx.doi.org/10.5281/zenodo.7870318, White paper is part of the smashHit project deliverable D2.2 smashHit Methodology (final).
[22] smashHit consortium. smashHit User & Developer Guidelines Data Provider & Data Processor. 2022, http://dx.doi.org/10.5281/zenodo.7870766, User guide part of the smashHit project deliverable D2.2 smashHit Methodology (final).
[23] De Lauretis L. From monolithic architecture to microservices architecture. In: 2019 IEEE international symposium on software reliability engineering workshops. ISSREW, 2019, p. 93–6. http://dx.doi.org/10.1109/ISSREW.2019.00050.
[24] Hasselbring W, Steinacker G. Microservice architectures for scalability, agility and reliability in E-commerce. In: 2017 IEEE international conference on software architecture workshops. ICSAW, 2017, p. 243–6. http://dx.doi.org/10.1109/ICSAW.2017.11.
[25] Koç ÇK, Özdemir F, Ödemiş Özger Z. Rivest-Shamir-Adleman algorithm. In: Partially homomorphic encryption. Springer; 2021, p. 37–41.
[26] Selent D. Advanced encryption standard. Rivier Acad J 2010;6(2):1–14.
[27] International Committee for Information Technology Standards, Cyber security technical committee 1. American national standard for information technology—Next generation access control (NGAC). 2020, (Available at https://standards.incits.org/apps/group_public/project/details.php?project_id=2328).
[28] Kurteva A, Chhetri TR, Tauqeer A, Hilscher R, Fensel A, Nagorny K, et al. The smashHitCore ontology for GDPR-compliant sensor data sharing in smart cities. Sensors 2023;23(13):6188. http://dx.doi.org/10.3390/s23136188.
[29] smashHit consortium. D7.5 demonstrator of services using integrated traffic, smart city and CPP data. 2022, http://dx.doi.org/10.5281/zenodo.7868230.
[30] smashHit consortium. D6.5 - demonstrator of services using integrated CPP and insurance data. 2022, http://dx.doi.org/10.5281/zenodo.7867998.
[31] Tauqeer A, Kurteva A, Chhetri TR, Ahmeti A, Fensel A. Automated GDPR contract compliance verification using knowledge graphs. Information 2022;13(10). http://dx.doi.org/10.3390/info13100447.