The GDPR Compliance and Access Control Systems: Challenges and Research Opportunities

Said Daoudagh[a] and Eda Marchetti[b]

ISTI-CNR, Pisa, Italy

Abstract: The General Data Protection Regulation (GDPR) is changing how Personal Data should be processed. Using Access Control Systems (ACSs) and their specific policies as practical means for assuring a by-design lawfully compliance with the privacy-preserving rules and provision is currently an increasingly researched topic. As a result, this newly born research field raises several research questions and paves the way for different solutions. This position paper would like to provide an overview of research challenges and questions concerning activities for analyzing, designing, implementing, and testing Access Control mechanisms (systems and policies) to guarantee compliance with the GDPR. Some possible answers to the open issues and future research directions and topics are also provided.

1 INTRODUCTION

The General Data Protection Regulation (GDPR) is the EU legal framework for the protection of Personal Data of European citizens (European Union, 2016). It aims to harmonize the different data protection laws in Europe and strengthen the rights of individuals. Thus, the GDPR precisely defines the involved concepts and roles: *Personal Data* is defined as any information about a *Data Subject*, i.e., an identified or identifiable natural person; data *Controller* and data *Processor* are defined as the persons involved into the data management and processing of Personal Data respectively. The GDPR also imposes several duties, and defines a system of fines to induce the Controller and the Processor to be compliant with the regulation. In particular, they need to:

i) ensure appropriate technical security level of personal data, as dictated by the "Integrity and Confidentiality" principle (Art. 5.1(f));

ii) demonstrate the compliance with the GDPR, as required by the "Accountability" principle (Art. 5.2); and

iii) adapt and rethink their data practices so as to be aligned with the "Data protection by design and by default" approach (Art. 25).

[a] https://orcid.org/0000-0002-3073-6217
[b] https://orcid.org/0000-0003-4223-8036

Despite the simplicity of these statements, their realization is not straightforward, especially when the roles of *Controller* and *Processor* are taken inside are taken inside Small and Medium-sized Enterprises (SMEs). Indeed, one of the most experienced difficulties is the GDPR's technical interpretation (Arfelt et al., 2019). The simplicity of the natural language structure of the GDPR leaves the floor to a concrete difficulty for software architects, developers, and security experts in translating the GDPR 's provisions into technical requirements, especially in case of lack or no sufficient legal expertise

If big organizations have the economic power to overcome this problem (e.g., by investing a large amount of money in both technologies and legal consulting), usually, this is not the same for SMEs. These look for low-cost and easy-to-use solutions for assuring their compliance with the GDPR and for being prepared to comply with the legal provisions. Indeed, for all organizations being (by-design) compliant with the GDPR means having technical (and organizational) solutions that:

(1) are general-purpose;

(2) must take into consideration the regulation by-design;

(3) must integrate with the existing business processes; and finally,

(4) must be rooted in the GDPR principles dictated in Art. 5.

As evidenced by the data collected by the CMS Legal Services EEIG [1], initiatives for lawfully processing personal data are still far from being sufficiently compliant with the regulation. Indeed, the imposed fines are constantly increasing within all the EU state members (currently reaching around 900 fines), and the most encountered type violations are still the "Insufficient legal basis for data processing" and "Insufficient technical and organizational measures to ensure information security."

In this situation, and inspired primarily by the "Integrity and Confidentiality" principle (Art. 5.1(f)), which calls for the adoption of Access Control (AC) to regulate the access to Personal Data, recently a new research field has been defined (Daoudagh, 2021):

> *Leverage AC systems, the de facto mechanisms used to restrict data access, as a technical solution for protecting "personal data by-design", and gaining legal compliance with the GDPR.*

The choice of Access Control Systems (ACSs) has two pivotal aspects: (1) their structure and (2) their applicability. Structurally, ACSs satisfy by construction the principle of Integrity and Confidentiality (Art. 5.1(f)) because they rely on Access Control Policies (ACPs), i.e., a set of rules that specify who has access to which resources and under which circumstances (Sandhu and Samarati, 1994). Considering the applicability, ACSs are general-purpose models supported by a standard and a reference architecture and easily integrated within the existing business processes to decouple the business logic from authorization. Consequently, we can efficaciously and effectively leverage AC systems to protect personal data (*security perspective*) and process them lawfully (*legal perspective*).

For the purpose of providing researchers and practitioners guidelines for facing this new field of research, in this position paper the current state of the practice is analyzed. In particular, a classification of the challenges (Section 2) and feasible research questions (Section 3) and their possible answers are provided (Section 4), to focus the research activity on the most important aspects. Finally, the conclusion and future work are depicted (Section 5).

---

[1] https://www.enforcementtracker.com/ (Last Access 2021.12.20)

2 CHALLENGES

In using AC as a technical solution for protecting "personal data by-design" and gaining legal compliance with the GDPR, several challenges have to be faced up. By referring to (Daoudagh, 2021; Sforzin A. et al., 2020) for a detailed description, the most important ones with respect to the data privacy aspects are:

Performing Data Protection Impact Assessment.
Performing Data Protection Impact Assessment (DPIA) according to the GDPR is pivotal to promote and achieve privacy-by-design. Hence, fulfilling the GDPR requirements is an integrated part of the business of different organizations. The challenge here is that the GDPR's requirements are often too vague and open. That makes them subject to interpretation. Therefore, it might be challenging to correctly and completely comply with them (Sforzin A. et al., 2020).

GDPR-based Development Life Cycle. The available development life cycles do not completely incorporate the privacy-by-design principles, and proposals targeting the GDPR's demands are still needed. Therefore, a reference GDPR-based development life cycle - for the specification, implementation, and testing of software systems and applications - which takes into account (European) legal requirements is needed.

Enforcing and Demonstrating the Privacy: Principles Compliance. The peculiarities and the complexity of the currently available systems and applications call for specific automatic approaches, facilities, and tools for enforcing and demonstrating compliance with the privacy principles. That is a crucial aspect for the successful and lawful privacy-by-design process development.

Considering, in particular, the access control aspects, the main challenges are:

Modeling the Law. Using Access Control elements and extensions to address concepts related to a given law requires formal translations to avoid misinterpretation or errors. Thus, the necessity of automatically enforceable matching of actual attributes gathered from legal use cases and the resulting policies to comply with the GDPR's obligation of "data protection by design and by default."

Enforcing Privacy (Security) Policies. A reference access control architecture to support context-aware security policies should be defined so as to assure the enforcement of the privacy

policies throughout different kinds of systems and environments. Additionally, methods for leveraging the integration of the access control and business processes as well as mechanisms to guarantee the GDPR compliance during business activities of data management and analysis should be conceived.

Verification & Validation. The GDPR is changing how Personal Data should be processed. Part of the scientific and industrial worlds are replying to these requirements by modifying the Access Control Mechanisms (ACMs) and the way they are managing and writing their policies. Consequently, specific testing strategies or validation approaches should be defined to assure that the generated GDPR-based policies are aligned with the GDPR. Failing this task can lead to developing ACPs that allows an unauthorized user to access protected personal data (*security perspective*) and consequently result in unlawful processing (*legal perspective*). Therefore, the need for developing facilities for verifying that the derived policies are compliant with the requirements expressed in the GDPR.

3 RESEARCH QUESTIONS

In replying to the challenges mentioned in the previous section, software engineering research activities are focusing on the definition of procedures and best practices for joining together Access Control (AC), Data Protection by-Design, and AC Testing into a unique *Privacy-By-Design* methodology. However, due to the variety of aspects included in those research activities, we have structured our investigation into the following open Research Questions (RQs) (Daoudagh, 2021).

> *Research Question 1 (RQ 1)*
> How can authorization systems, and in particular AC, be used for guaranteeing compliance with the GDPR?

Authorization systems are a cornerstone of security, and they are being used for a long time to protect classified resources. They have also been used for dealing with different privacy concepts such as purpose and consent. Consequently, they can be leveraged for protecting personal data and satisfying compliance with the GDPR. However, practical solutions need to face several open questions. Are there comprehensive methodologies or set of guidelines to fa-

cilitate the adoption of AC in the state of the practice? Are there concepts and knowledge belonging to other disciplines that can be exploited to customize systematically existing authorization systems? And how to encode the GDPR's obligations in the authorization systems? Additionally, to provide a systematic approach for designing and using authorization systems in the context of the GDPR, accurate analysis of their current adoption in other legal frameworks and into the industry needs to be also performed.

> *Research Question 2 (RQ 2)*
> To what extent can the GDPR's obligations be represented and enforced using Access Control Technologies?

Legal requirements are expressed in natural language, and they are agnostic to the available technologies presented in our time. Therefore, they can be too vague to be automatically implemented within a reference system or technology. However, by defining the "Integrity and Confidentiality" principle, the GDPR implicitly calls for adopting ACSs. Indeed, ACSs are usually regulated by ACPs, which specify who, what, when, where, how, and why (i.e., the 5W1H) a user is denied or allowed to access to a given asset. This information also includes Personal Data. Thus, the question of how to identify, extract and define the ACPs that are by-design compliant with the GDPR is not straightforward. Therefore, proposals need to answer the following questions. How to model AC policies according to the GDPR? How to identify AC requirements from the GDPR? How many AC requirements can the GDPR encode?

> *Research Question 3 (RQ 3)*
> Is it possible to gather technical requirements from the legal specifications defined in the GDPR?

The GDPR, as any other law, is intrinsically expressed in legal jargon, even if it targets the organizations that process personal data. Even though its natural language provisions are far from being immediately interpreted as technical requirements, the "personal data by design" obligation the GDPR forces organizations to implement system by-design aligned with the GDPR. That causes a general re-think of the organizations' data practices and continuous and expensive research of ad-hoc technical solutions to guarantee compliance with the GDPR's obligations. Therefore, a key aspect is the availability of facilities able to automatically extract, from the legal specifi-

cations, all and only the required information and interpret them into technical requirements that can be easily implemented.

> **Research Question 4 (RQ 4)**
> For accomplishing compliance with the GDPR, which are the supporting technologies that could be integrated with AC?

The continuous growth of interest for compliance with the GDPR is fostering the realization of different solutions in both industry and academia contexts. Therefore, accurate analysis of the available proposals and an evaluation of their effectiveness in achieving compliance with the GDPR are necessary to provide solutions able to be profitably integrated into the ACS. Additionally, to promote the adoption of the solutions into real context, further research questions are: is the proposal based on open standards? Can available solutions for achieving compliance with the GDPR's demands be integrated? And in case, how is this possible?

> **Research Question 5 (RQ 5)**
> Which are the most suitable application domains for applying Access Control Technologies able to achieve the GDPR compliance?

The GDPR is potentially applicable to every domain: any context processing personal data are obliged to obey the GDPR's principles. At the same time, in Information and Communication Technologies (ICTs) systems, also the ACSs is having a widespread adoption for ruling the resources and data access. Thus, the synergistic union between the GDPR and ACSs could be the crucial point for developing adaptable solutions everywhere. In evaluating the feasibility of the different proposals, the following questions should also be considered: are AC really suitable for different application domains? Can ACSs be easily integrated in preexisting processes/environments? Is it possible to enable the authorization as a service paradigm? And more specific, is it possible to decouple business logic from the authorization one?

> **Research Question 6 (RQ 6)**
> Is it possible to realize an integrated test environment for the validation of (GDPR-aware) access control systems?

The high-security level is a crucial attribute for many environments. Thus, discovering the criticalities of a system is always an effective means for

putting in practice efficacious and corrective actions to improve its overall security. That is very true and important for ACSs (both ACPs and Access Control Mechanisms (ACMs)) because their security and privacy vulnerabilities could insert either the risk of releasing inadequate security solutions. These could allow unauthorized access (*security perspective*) or to enable unlawful processing of personal data (*legal perspective*). At the state of the practice, most of the time, the criticalities detection is achieved through the application of effective and efficient testing approaches. Therefore, the testing solutions should be guided by the following research questions: is it possible to realize a test environment specifically conceived for ACSs? Is it possible to develop specific test strategies? Is it possible to provide facilities for test cases generation and selection? Is it possible to develop an integrated environment for the automatic test cases execution and results collections? Is it possible to define an oracle for speeding up the test results evaluation? Is it possible to statistically evaluate the effectiveness of the applied testing strategies?

4 POSSIBLE ANSWERS TO RQs

In this section, without claiming to provide a complete survey of all available proposals, we provide an overview of a selection of possible solutions answering the research questions presented in the previous section. We refer to (Daoudagh, 2021) for a complete state-of-the-art survey and additional details.

4.1 Answering RQ 1

Inspired by the "Data Protection by Design" obligation (Art. 25), one of the most promising answers to this question is focusing on by-design proposals. In the literature, both by-design GDPR-based Life Cycle for developing access control systems in compliance with the GDPR (Daoudagh and Marchetti, 2020b) and reference architectures for its (semi)-automation are available (Davari and Bertino, 2019; Daoudagh and Marchetti, 2020b; Dernaika et al., 2020). The intent is to provide support for defining GDPR-based use cases, developing, testing, deploying, and reviewing both ACPs and ACMs (Daoudagh, 2021).

4.2 Answering RQ 2

Systematic approaches to gathering access control requirements from the GDPR are currently available (Davari and Bertino, 2019; Bartolini et al., 2019b). Usually, they focus on improving and joining

academic proposals with methods adopted in the industrial environment. From a practical point of view, these proposals include three phases: the translation of the most suited GDPR's articles into GDPR-based ACP templates; the definition of a customized legal use case for each GDPR article related to ACP; and finally, the generation of enforceable ACPs in a given language. The adaptation of the different proposals to other AC models (e.g., Role-Based Access Control (RBAC)) and other AC languages, and the representation through AC technologies of any legal text that encodes data protection specifications, still remain crucial challenges.

4.3 Answering RQ 3

Among the proposal trying to answer this question, the most promising ones rely on Agile methodologies to gather AC requirements from the GDPR (Daoudagh, 2021). Indeed, Agile methodologies yield a more broad spectrum since they can be applied to different data protection frameworks that encode ACPs specification (Chowdhury et al., 2012). These proposals use the concept of User Stories (Lucassen et al., 2016) for data protection requirements representations. In parallel, solutions providing conceptual models of GDPR-based User Stories are emerging (Douglas Teodoro and Morley-Fletcher, 2017; Bartolini et al., 2019a; Miri et al., 2018). In this case, the GDPR's structure of the mandatory articles is unfolded into basic and concrete elements and used to automatically translate the User Stories into AC policies.

4.4 Answering RQ 4

Thanks to the peculiarity of the AC, supporting facilities to perform specific functionalities can be easily integrated into the different available proposals. Usually, for accomplishing compliance with the GDPR, the widespread considered are Semantic Web (in particular legal ontologies) (Palmirani et al., 2018; Pandit et al., 2019; Davari and Bertino, 2019) and Consent Management (Kurteva et al., 2021). The former is used to express GDPR concepts and relationships among them, whereas the latter is usually considered for managing the consent given by the data subject. To this purpose, some of the available proposals are currently leveraging the Kantara GDPR Explicit Consent Record (Group., 2018) as a reference format for collecting, managing, and classifying the GDPR's concepts. Other proposals that can be exploited for this purpose use the Model-Driven Engineering (MDE) approach for modeling data protec-

tion regulations such as the GDPR (Torre et al., 2020).

4.5 Answering RQ 5

The widespread adoption of ACSs in ICTs made them ideal candidates for being adopted in different application domains. Currently, Smart ICT Systems, Business Processes and Indoor Localization Systems (ILSs) are the most promising application domains (Basin et al., 2018; Zaman and Hassani, 2020; Daoudagh et al., 2021). In particular, in Smart ICT Systems, appropriate supports to aid controllers in developing Privacy-By-Design Smart Services are provided. In this case, the generic architecture of Smart ICT Systems is enhanced with a new layer. That allows (i) a user-friendly interaction with the end-users of the Smart ICT system (i.e., Interested and Smart Services), (ii) the management of activities dependent on the domain, and finally, (iii) the automatic derivation of ACPs according to the collected consents.

Considering the Business Processes, they can be leveraged to automatically enforce the GDPR provisions during the activities related to data management and analysis (Arfelt et al., 2019; Calabrò et al., 2019). In some cases, the business process includes a GDPR-based access control mechanism that protects personal data during the Business Process Model and Notation (BPMN) modeling and execution.

Finally, considering the ILSs, reference architectures able to guarantee compliance with the GDPR through the integration of specialized access control systems enforcing the GDPR provisions are currently under development (Lopes et al., 2020; Daoudagh and Marchetti, 2021). The adoption of this GDPR-aware ILSs for the social distancing purpose is also an ongoing activity (Barsocchi et al., 2021).

4.6 Answering RQ 6

Recently, testing frameworks capable to formally validate both ACPs and ACMs have been presented (Zhang and Zhang, 2017; Khamaiseh et al., 2018; Daoudagh et al., 2020b). In some cases Controlled Experiments (CEs) in the context of AC have been also proposed (Daoudagh et al., 2020a; Daoudagh and Marchetti, 2020a). Usually, the different proposals focus on: test strategy selection and derivation, test case execution and result evaluation, and finally, Oracle definition (Felderer et al., 2016; Xu et al., 2020). Additionally, for assessing GDPR-based test cases generation strategies, generic methodology based on mutation analysis have also been proposed (Daoudagh and Marchetti, 2021).

5 CONCLUSION AND FUTURE WORK

Pairing up Data Privacy and Data Security is becoming pivotal for promoting trustworthiness in services and products managing personal data and for guaranteeing the data subject's rights (Daoudagh, 2021). By defining the "Integrity and Confidentiality" principle (Art. 5.1(f)), the European legislator poses security at the heart of the GDPR. It dictates that personal data must be protected from unauthorized or unlawful processing. One of the cornerstones of security is access control, which is ruled by access control policies specifying who is allowed to access Personal Data.

However, the security of processing is not an isolated obligation but comes together with the GDPR's "Accountability" principle (Art. 5.2). Indeed, according to this principle, security measures are at the same time an obligation and a technical means to implement other data protection obligations. Additionally, the GDPR imposes to the controllers and processors to adopt the Data Protection by Design and by Default (Art. 25), highlighting the necessity of engineering solutions for enforcing data privacy requirements into ICT services.

According to the challenges presented in this paper (see Section 2), leveraging the AC systems, the de facto mechanisms used to restrict data access, as a technical means for protecting "personal data by-design" and gaining legal compliance with the GDPR, promote several research activities. Those activities contributed to:

1. define a GDPR-based Life Cycle for authorization systems and a reference architecture, enabling data protection by-design;

2. leverage the state-of-the-art about legal ontology by defining a GDPR-based AC ontology useful for building ACPs in compliance with the GDPR;

3. define a GDPR profile for a standardized AC language;

4. define a systematic approach for gathering and developing ACPs compliant-by-design with the regulation;

5. advance the notion of *Data Protection Backlogs* by introducing specific User Stories focused on the GDPR's provisions and their technical requirements;

6. enable an Agile development of ACSs;

7. define a comprehensive testing framework for validating both the GDPR-based and traditional ACSs;

8. promote the application of ACSs in different contexts.

However, despite the accuracy devoted to investigating the challenges and the related research questions, future works are still possible:

Standardization of the XACML GDPR Policy Profile. In its original structure, the profile is not sufficiently adequate for representing all the GDPR's requirements: indeed, it targets just the concept of purpose. A possible extension of the attributes of the XACML Privacy Profile for encoding GDPR's concepts in XACML policies needs to be defined. For this aim, recently, we have already advanced an *XACML GDPR Policy Profile* proposal that provides standard attributes according to the GDPR concepts (Daoudagh, 2021).

Discussions with Legal Experts. All the available and future proposals should be guided by, and sometimes developed together with, data protection legal experts to guarantee internal and external validation. Specifically, independent legal experts should be put in the loop to validate whether the developed ACPs can capture and express the legal meaning of the related GDPR's provisions. That will also quantify the completeness and the correctness of the translation of the norms.

Methodology to Verify and Demonstrate the Compliance with the GDPR. The accountability principle dictates that "controller shall be responsible for, and be able to demonstrate compliance with" the other principles of the regulation. However, future works involve providing tools, methodologies, and strategies for demonstrating compliance with the GDPR. Furthermore, there is still the necessity to provide solutions dealing with the auditability and accountability demands.

Release the Reference Architecture. Even if different implementations of architectures have been provided, a standardized reference architecture that could be easily customized for different applications (e.g., Calling and Messaging, Networking Applications (Kalapodi and Sklavos, 2021)) is still necessary.

User Stories Templates in Other Contexts. Investigating a comprehensive Data Protection Impact Assessment (DPIA) methodology (which is one of the legal requirements of the GDPR (Art. 35)) for leveraging the conceived Data Protection Backlog is also part of our future work.

Other Legal Frameworks. Applying and adapting the different proposals to other legal requirements, such as the new coming ePrivacy regulation as well as to the eIDAS regulation, seems to be an interesting future development.

ACKNOWLEDGEMENTS

REFERENCES

Arfelt, E., Basin, D., and Debois, S. (2019). Monitoring the gdpr. In *European Symposium on Research in Computer Security*, pages 681–699. Springer.

Barsocchi, P., Calabrò, A., Crivello, A., Daoudagh, S., Furfari, F., Girolami, M., and Marchetti, E. (2021). COVID-19 & privacy: Enhancing of indoor localization architectures towards effective social distancing. *Array*, 9:100051.

Bartolini, C., Daoudagh, S., Lenzini, G., and Marchetti, E. (2019a). Gdpr-based user stories in the access control perspective. In *Quality of Information and Communications Technology - 12th International Conference, QUATIC 2019, Ciudad Real, Spain, September 11-13, 2019, Proceedings*, pages 3–17.

Bartolini, C., Daoudagh, S., Lenzini, G., and Marchetti, E. (2019b). Towards a lawful authorized access: A preliminary gdpr-based authorized access. In *14th International Conference on Software Technologies (IC-SOFT 2019), Prague, Czech Republic, July 26-28, 2019.*, pages 331–338.

Basin, D., Debois, S., and Hildebrandt, T. (2018). On purpose and by necessity. In *Proceedings of the Twenty-Second International Conference on Financial Cryptography and Data Security (FC)*.

Calabrò, A., Daoudagh, S., and Marchetti, E. (2019). Integrating access control and business process for GDPR compliance: A preliminary study. In *Proceedings of the Third Italian Conference on Cyber Security, Pisa, Italy, February 13-15, 2019.*

Chowdhury, O., Chen, H., Niu, J., Li, N., and Bertino, E. (2012). On xacml's adequacy to specify and to enforce hipaa. In *Proceedings of the 3rd USENIX Conference on Health Security and Privacy*, HealthSec'12, pages 11–11, Berkeley, CA, USA. USENIX Association.

Daoudagh, S. (2021). The GDPR Compliance Through Access Control Systems. [PhD Dissertation, University of Pisa]. https://etd.adm.unipi.it/theses/available/etd-07112021-124810/.

Daoudagh, S., Lonetti, F., and Marchetti, E. (2020a). Assessing testing strategies for access control systems:

A controlled experiment. In *Proceedings of ICISSP 2020, Valletta, Malta, February 25-27, 2020.*

Daoudagh, S., Lonetti, F., and Marchetti, E. (2020b). XACMET: XACML testing & modeling. *Softw. Qual. J.*, 28(1):249–282.

Daoudagh, S. and Marchetti, E. (2020a). Defining controlled experiments inside the access control environment. In Hammoudi, S., Pires, L. F., and Selic, B., editors, *Proceedings of the 8th International Conference on Model-Driven Engineering and Software Development, MODELSWARD 2020, Valletta, Malta, February 25-27, 2020*, pages 167–176. SCITEPRESS.

Daoudagh, S. and Marchetti, E. (2020b). A life cycle for authorization systems development in the GDPR perspective. In Loreti, M. and Spalazzi, L., editors, *Proceedings of the Fourth Italian Conference on Cyber Security, Ancona, Italy, February 4th to 7th, 2020*, volume 2597 of *CEUR Workshop Proceedings*, pages 128–140. CEUR-WS.org.

Daoudagh, S. and Marchetti, E. (2021). Graduation: A gdpr-based mutation methodology. In *Quality of Information and Communications Technology - 14th International Conference, QUATIC 2021, Faro, Portugal, September 8-11, 2021, Proceedings*, pages –.

Daoudagh, S., Marchetti, E., Savarino, V., Bernabe, J. B., García-Rodríguez, J., Moreno, R. T., Martinez, J. A., and Skarmeta, A. F. (2021). Data protection by design in the context of smart cities: A consent and access control proposal. *Sensors*, 21(21).

Davari, M. and Bertino, E. (2019). Access control model extensions to support data privacy protection based on gdpr. In *2019 IEEE International Conference on Big Data (Big Data)*, pages 4017–4024.

Dernaika, F., Cuppens-Boulahia, N., Cuppens, F., and Raynaud, O. (2020). Accountability in the A posteriori access control: A requirement and a mechanism. In *Quality of Information and Communications Technology - 13th International Conference, QUATIC 2020, Faro, Portugal, September 9-11, 2020, Proceedings*, volume 1266 of *Communications in Computer and Information Science*, pages 332–342. Springer.

Douglas Teodoro, Emilie Pasche, P. R. and Morley-Fletcher, E. (2017). Deliverable 1.1 initial list of main requirements. http://www.myhealthmydata.eu/wp-content/themes/Parallax-One/deliverables/D1.1_Initial-List-of-Main-Requirements.pdf.

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). *Official Journal of the European Union*, L119:1–88.

Felderer, M., Büchler, M., Johns, M., Brucker, A. D., Breu, R., and Pretschner, A. (2016). Chapter one - security testing: A survey. volume 101 of *Advances in Computers*, pages 1–51. Elsevier.

Group., K. I. C. . I. S. W. (2018). Consent receipt specification 1.1.0. kantara initiative technical specification recommendation. https://kantarainitiative.org/file-downloads/consent-receipt-specification-v1-1-0/.

Kalapodi, A. and Sklavos, N. (2021). The concerns of personal data privacy, on calling and messaging, network-

ing applications. In Thampi, S. M., Wang, G., Rawat, D. B., Ko, R., and Fan, C.-I., editors, *Security in Computing and Communications*, pages 275–289, Singapore. Springer Singapore.

Khamaiseh, S., Chapman, P., and Xu, D. (2018). Model-based testing of obligatory abac systems. In *2018 IEEE International Conference on Software Quality, Reliability and Security (QRS)*, pages 405–413.

Kurteva, A., Chhetri, T. R., Pandit, H. J., and Fensel, A. (2021). Consent through the lens of semantics: State of the art survey and best practices. *Semantic Web*, (Preprint):1–27.

Lopes, H., Pires, I. M., Sánchez San Blas, H., García-Ovejero, R., and Leithardt, V. (2020). Priada: Management and adaptation of information based on data privacy in public environments. *Computers*, 9(4).

Lucassen, G., Dalpiaz, F., van der Werf, J. M. E. M., and Brinkkemper, S. (2016). Improving agile requirements: the quality user story framework and tool. *Requirements Engineering*, 21(3):383–403.

Miri, M., Foomany, F. H., and Mohammed, N. (2018). Complying with gdpr: An agile case study. *ISACA Journal*, 2.

Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., and Robaldo, L. (2018). Legal ontology for modelling gdpr concepts and norms. In *Legal Knowledge and Information Systems: JURIX 2018*, volume 313, page 91. IOS Press.

Pandit, H. J., Debruyne, C., O'Sullivan, D., and Lewis, D. (2019). Gconsent - a consent ontology based on the gdpr. In Hitzler, P., Fernández, M., Janowicz, K., Zaveri, A., Gray, A. J., Lopez, V., Haller, A., and Hammar, K., editors, *The Semantic Web*, pages 270–282, Cham. Springer International Publishing.

Sandhu, R. S. and Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48.

Sforzin A. et al. (2020). Deliverable D3.11: Definition of Privacy by Design and Privacy Preserving Enablers. https://cybersec4europe.eu/publications/deliverables/.

Torre, D., Alferez, M., Soltana, G., Sabetzadeh, M., and Briand, L. (2020). Model driven engineering for data protection and privacy: Application and experience with gdpr. *arXiv preprint arXiv:2007.12046*.

Xu, D., Shrestha, R., and Shen, N. (2020). Automated strong mutation testing of xacml policies. In *Proceedings of the 25th ACM Symposium on Access Control Models and Technologies*, SACMAT '20, page 105–116, New York, NY, USA. Association for Computing Machinery.

Zaman, R. and Hassani, M. (2020). On enabling gdpr compliance in business processes through data-driven solutions. *SN Computer Science*, 1(4):1–15.

Zhang, Y. and Zhang, B. (2017). A new testing method for xacml 3.0 policy based on abac and data flow. In *2017 13th IEEE International Conference on Control & Automation (ICCA)*, pages 160–164. IEEE.