

How to Improve the GDPR Compliance through Consent Management and Access Control

Said Daoudagh^{1,2}^a, Eda Marchetti¹^b, Vincenzo Savarino³^c, Roberto Di Bernardo³^d
and Marco Alessi³^e

¹*ISTI-CNR, Pisa, Italy*

²*University of Pisa, Pisa, Italy*

³*Engineering Ingegneria Informatica, Italy*

Keywords: Access Control, Consent Management, GDPR, Privacy-by-Design.

Abstract: This paper presents a privacy-by-design solution based on Consent Manager (CM) and Access Control (AC) to aid organizations to comply with the GDPR. The idea is to start from the GDPR's text, transform it into a machine-readable format through a given CM, and then convert the obtained outcome to a set of enforceable Access Control Policies (ACPs). As a result, we have defined a layered architecture that makes any given system privacy-aware, i.e., systems that are compliant by-design with the GDPR. Furthermore, we have provided a proof-of-concept by integrating a Consent Manager coming from an industrial context and an AC Manager coming from academia.

1 INTRODUCTION

The General Data Protection Regulation (GDPR) is the EU Data Protection Regulation (European Union, 2016) in charge of harmonizing the regulation of Data Protection across the EU member states. At the same time, it enhances and arises business opportunities within the Digital Single Market (DSM) space. However, the natural language nature of the GDPR makes most of the provisions to be expressed in generic terms and does not provide specific indication on how they should be actuated. As a consequence, assuring the GDPR compliance, and therefore avoid the related fines, becomes an important research challenge.

Currently, many businesses are struggling in the definition of appropriate procedures and technical solutions for their development process so as to enforce and demonstrate the GDPR compliance (Krenn S. et al., 2020). More precisely, they recognized as a pivotal factor in the availability of automated supports for specifying privacy requirements, controlling per-

sonal data, and processing them in compliance with the GDPR.

From a practical point of view, scientific communities, private companies, and European projects such as CyberSec4Europe (Cyber Security Network of Competence Centres for Europe)¹ are identifying in the consent and security services, the successful elements for automatic specification and enforcing the data protection regulation (Krenn S. et al., 2020).

Indeed, the consent services may allow citizens and companies to manage and track personal data in a straightforward, user-centric, and user-friendly manner; while the security services, and specifically the authorization systems (i.e., Access Control (AC)), can enforce the data protection regulations taking into account additional legal requirements, such as the data usage purpose, user consent, and the data retention period. Therefore, the joint work of the consent and security services may overcome the challenging and error-prone task of extracting legal and machine-readable policies directly from the GDPR's rules.

Currently, different research activities have been devoted to define and implement privacy knowledge and rules (Sforzin A. et al., 2020), but no generic solution is still available. Along these lines, under the

¹<https://cybersec4europe.eu/>

^a <https://orcid.org/0000-0002-3073-6217>

^b <https://orcid.org/0000-0003-4223-8036>

^c <https://orcid.org/0000-0002-2741-5543>

^d <https://orcid.org/0000-0002-4432-5128>

^e <https://orcid.org/0000-0002-1982-606X>

hypothesis that the joint integration of access control systems and consent manager can enhance the controller's and processor's compliance with the regulation, this paper wants to provide the basic architecture of a generic and practical solution to solve the GDPR compliance problem.

In presenting our idea, we focus on the following primary Research Question (RQ):

How a consent manager solution can be improved with access control for assuring compliance with the data protection or privacy regulation?

In answering the above RQ, we present a possible privacy-by-design architecture by integrating AC and consent management systems. Finally, an implementation of the proposed architecture by using real available solutions for the consent management and the Access Control Mechanism (ACM), coming from both industry and academia, is presented.

Outline. Section 2 presents the basic concepts used along the proposal and related works; Section 3 describes the proposed solution by answering our RQ; Section 4 shows the proof-of-concept we implemented by instantiating the proposed solution with real artifacts coming from both industrial and academic contexts; and finally, Section 5 concludes the paper and illustrates future works.

2 BACKGROUND AND RELATED WORK

This section introduces the main concepts used along the present work: the GDPR concepts, Access Control, and Smart ICT Systems; and reports the related work.

The GDPR Concepts. The General Data Protection Regulation (GDPR) (European Union, 2016) defines *Personal Data* as any information related to an identified or identifiable natural person called *Data Subject*. That means that, a data subject is a Natural Person (a living human being), whose data are managed by a *Controller*. The GDPR aims to ensure equal protection of the Human Rights of the European Citizens, to eliminate the barriers for the services to be delivered in the European Union, and to enhance business opportunities within the Digital Single Market (DSM).

The GDPR is applied to the processing of personal data, whether it is automated (even partially) or

not. It defines, among others, the following principles and demands: *Purposes*, i.e., data should only be collected for determined, explicit and legitimate purposes, and should not be processed later for other purposes; *Accuracy*, i.e., the processed data must be accurate and up-to-date regularly; *Retention*, i.e., data must be deleted after a limited period; *Subject explicit consent*, i.e., data may be collected and processed only if the data subject has given his/her explicit consent.

Access Control. The eXtensible Access Control Markup Language (XACML) (OASIS, 2013) is one of the most widely used AC languages. It provides a reference architecture including specific components for managing policies and access requests. Indeed, the evaluation of the the policy against the request provides response corresponding to the authorization decision. Very briefly, an XACML policy is a specific statement of what is and is not allowed on the basis of a set of rules, defined in terms of conditions on attributes of subjects, resources, actions, and environment, and combining algorithms for establish the precedence among the rules.

In this paper, Access Control mechanism becomes a means for restricting access to *personal data*, based on the GDPR compliant Access Control Policies (ACPs), i.e., a set of rules that specify who (e.g., *Controller*, *Processor* or *Data Subject*) has access to which resources (e.g., *Personal Data*) and under which circumstances (i.e., the GDPR's demands, such as *Purpose* and *Consent*).

Smart ICT System. Smart ICT Systems (or Services) are becoming increasingly important in almost all industries and areas of today's society (Neuhüttler et al., 2020). They rely on the integration and implementation of innovative tools and techniques that make a given system *smart* to strengthen economic needs (Samir Labib et al., 2018). Despite their increasing significance, a distinct definition of Smart ICT has not yet evolved in the scientific literature. Nevertheless, it is possible to identify a very high-level abstract architecture for a standard Smart ICT System, as depicted in Figure 1. Commonly, it is composed of a Smart ICT Core System that offers the main functionalities to Smart Services in terms of both hardware and smart software (e.g., Cloud Computing, Internet of Things, and Big Data). Consequently, developers use these functionalities to conceive and implement Smart Services that end-users consume to achieve a given business or personal needs.

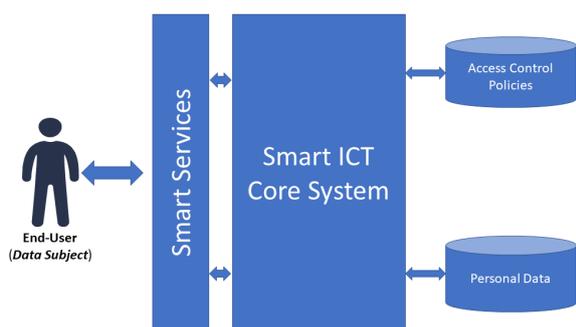


Figure 1: A Smart ICT System.

Smart ICT Core System is also in charge of managing the resource and data access by using either customized facilities or by relying on a specific Access Control System. To this purpose, in Figure 1 an Access Control Policies repository has been considered.

Related Work. Over the last years, different solutions have been proposed for the enforcement of the GDPR compliance into the Smart ICT Systems. They can be roughly divided into the following categories:

- Solutions applicable at Business Processes level, i.e., mainly focused on the behavioral aspect (Bartolini et al., 2019a; Calabrò et al., 2019; Åkerlund and Große, 2020; Sokolovska and Kocarev, 2018).
- Proposals providing supporting facilities for transforming the GDPR’s text into executable access control policies. In this case, the policies are either systematically derived from the GDPR, e.g., (Bartolini et al., 2019c; Dernaika et al., 2020) or generated through intermediate formal structures (Bartolini et al., 2019b; Carauta Ribeiro and Dias Canedo, 2020).
- Proposals easily enforceable into the Smart ICT Systems architecture. They can be roughly classified into: i) those using access control mechanisms for the protection of personal data within Smart ICT Systems perimeters (Greaves et al., 2018); ii) those using Smart ICT Systems users location information for authenticate the customer and manage his/her data (Haofeng and Xiaorui, 2019); and iii) those exploiting specific security attributes for assuring the GDPR compliance (Jensen et al., 2013; Barsocchi et al., 2018; Calabrò et al., 2019).

Our answer to the RQ wants to merge the best practices of the identified above research areas. Indeed, we are proposing the integration of the consent and access control management for enhancing the business process execution with specific activities able to modeling and enforcing the GDPR legal framework.

3 A PRIVACY-BY-DESIGN PROPOSAL FOR SMART ICT SYSTEMS

In this section, we answer the RQ presented in the introduction of this paper by integrating consent and access control management for assuring compliance with a reference data protection legal framework, i.e., the GDPR.

In the remainder of this section, details about the proposed reference architecture are provided. Indeed, they are our positive answer to the RQ. Additionally, to remark the feasibility of the proposed solution, we also provide its possible instantiation by using two real-world systems coming from both industrial and academic contexts. Details of this integration are reported in Section 4.

3.1 A Privacy-by-Design Smart ICT System

In this section, we describe the *Privacy-By-Design Smart ICT System* layer, that provides features for interacting directly with smart services and end-users of the system to guaranteeing compliance with the EU regulation.

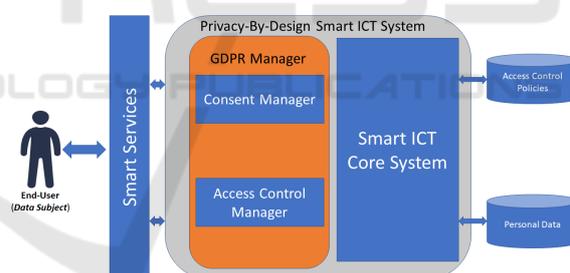


Figure 2: A Privacy-By-Design Smart ICT System Proposal.

By referring to Figure 1, the extended architecture is schematized in Figure 2, where the *Privacy-By-Design Smart ICT System* is represented by the external grey square. As in the figure, this layer has the responsibility to interact with end-users (in our case Data Subject and the Smart Services) of the Smart ICT system. It is also in charge of managing all the domain dependent activities that are necessary for the end-users interactions. More precisely, the *Privacy-By-Design Smart ICT System* includes: (1) the components already part of the Smart ICT core systems (described in Section 2) and represented as blue square labeled *Smart ICT Core System*; and (2) a new layer called *GDPR Manager*, that is in charge of the translation and enforcement of executable access

control policies. This is represented by the orange square labeled *GDPR Manager*, and detailed more in the remainder of this section.

3.2 GDPR Manager

The *GDPR Manager* includes two main components (see Figure 2): *Consent Manager* that translates the textual consent into structured representation, and *Access Control Manager* that provides enforceable access control policies.

Consent Manager. The aim of Consent Manager is to manage and control personal data during the interaction among Data Subjects and public and private services as Data Controller and Processors (e.g., PA, Social, IoT, B2C). It provides facilities for lawful data sharing processes, with the ability to grant and withdraw consent to third parties for accessing own personal data. Concerning Smart Services, the Consent Manager should allow them to define specific purposes for each operation (i.e., processing activities) and the data needed to accomplish the required tasks lawfully. Thus, the Consent Manager should include a consent-based, user-centric interface enabling: (1) the data subjects to manage, trace their own data and its associated consent; (2) the data controllers/processors to use consent to data sharing among digital services using personal data and meet the GDPR's requirements. Additionally, Consent Manager should guarantee by-design the compliance with the GDPR's demands, such as data minimization and purpose limitation principles.

Access Control Manager. Access Control Manager has the responsibility of creating Access Control Policies (ACPs) that are compliant by-design with the GDPR. It works in collaboration with the Consent Manager by receiving, as input, the machine-readable specification of services definitions and the related Data Subjects' consents. More precisely, it uses: Personal Data related to Data Subject classified in categories as required by the GDPR; information about the Controller of each service and the defined purposes; the consent given by the Data Subject in terms of relation between Personal Data and Purposes. Based on that information, Access Control Manager is able to create specific Access Control Policies, each related to a specific article of the GDPR. The peculiarities of the Access Control Manager are the possibility to (a) be integrated with different Consent Managers, and (b) to collaborating with different Access Control systems. This in order to guarantee the independence with specific input and

output formats, and to be easily enhanced with standardized Access Control Systems, such as the one offered by the XACML standard, e.g., when this component is missed in the *Smart ICT Core System*.

4 PROOF-OF-CONCEPT

In this section, we provide an instantiation of the architecture presented in the previous section by using real artefacts coming from both industrial and academic contexts described in Section 4.1 and 4.2, respectively. More precisely, we will show how CaPe² (industrial open-source product) and GENERALD (Gdpr-based ENforcement of perSonAL Data) framework (academic proposal) can collaborate and easily be integrated to achieve the GDPR compliance.

To better explain the use of CaPe and GENERALD framework, we consider the following application example sets into a wellness environment. Alice, a Data Subject, wants to use a smart wellness application to monitor her daily activities to achieve a predefined training objective. The application is provided by the myWellness company (Controller). To meet Alice's needs, myWellness has so far defined different purposes, each related to a specific data set of Personal Data. At the time of subscribing to the myWellness application, Alice provided her personal data (i.e., Age, Gender, and Blood Cholesterol) and gave her consent for one purpose (i.e., MyCholesterol). Additionally, Alice gave her consent to share her personal data with a third-party company named zzz-HealthOrg company. In turn, myWellness gave to Alice controller's contacts that include: piiController, orgName, address, e-mail, and phone number.

4.1 Consent Manager: CaPe at Glance

CaPe provides an ICT suite for a consent-based, user-centric personal data management. It follows MyData³ principles to exploit the potential of personal data, facilitates its control and new business opportunities in compliance with the GDPR. Thus, CaPe assures the following features: i) Consent authorizes Data Sources to provision data to Data Consumer and authorizes Data Requester to process that data; ii) Consent refers to a Data Usage Policy that can be linked to consent formalization; iii) Consent is given in a clear manner so as to let the data controller to demonstrate that a valid consent has been given; iv)

²<https://www.cape-suite.eu/>

³<https://mydata.org/>

Consent record clearly includes 1. Who consented; 2. When they consented; 3. What was consented; 4. How was consented; 5. Whether a consent withdrawn occurred.

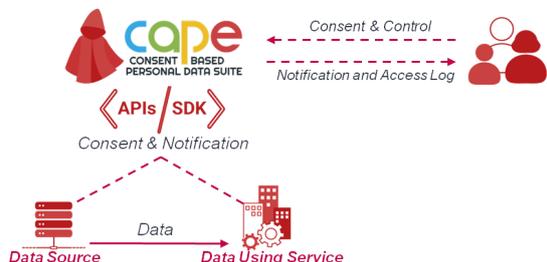


Figure 3: Overview of the CaPe Consent Manager.

Figure 3 shows an overview of the CaPe Consent Manager. As in the figure, the CaPe acts as an intermediary for the communication between data subjects and data controllers, supporting the generation and management of dynamic consents.

As shown in Figure 4, the CaPe provides also two specific dashboards (the Data Controller Dashboard and the User Self-Service Dashboard) for let the overall management of the personal data management. Additionally, through these interfaces, CaPe provides specific features to **grant and withdraw consent** to third parties for **access** to data about oneself.

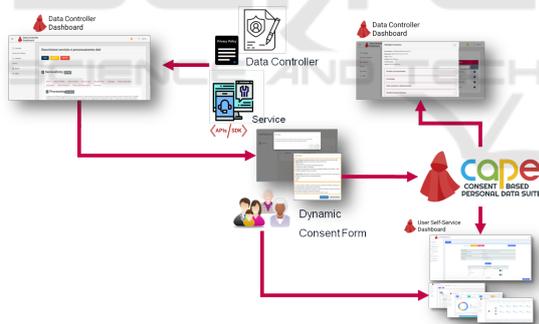


Figure 4: How CaPe Works.

A general CaPe use is provided in Figure 4. In the depicted scenario, through the *Data Controller Dashboard* an organization can model the legal basis for the processing of personal data: in a standardized manner; in accordance with the relevant information (i.e., purpose, processing, type of data and so on); and in line with the related privacy policy. According to the derived model, CaPe automatically generates the consent form that can be shown to the data subject. The two separated dashboards can let, on one side, the Data Controller to view and manage all the consents collected, on the other, the Data Subject, through the *User Self-Service Dashboard*, to check which data is

used, how and for what purpose and to manage the related consents.

Considering the application example mentioned at the beginning of this section, for confidential reasons we report in Figure 5 just an extract of the consent model derived by CaPe. As in the figure, the Consent is modeled as an entity having a unique ID identifying it and a status (Active, Non-Active).

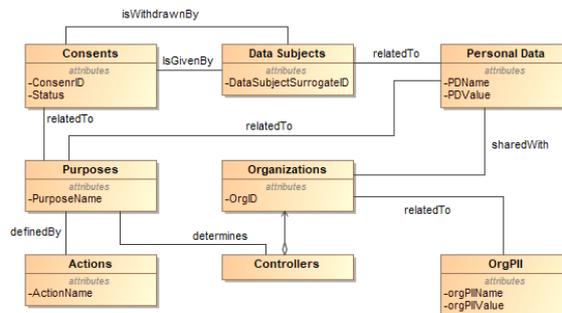


Figure 5: Extract of the CaPe Consent Model.

A *Data Subject* is identified by its ID, and it is related to a set of *Personal Data*, each represented by a name/value pair. The Data Subject can give a *Consent* for processing his/her for a specific *Purpose* defined by the *Controller*. Each Purpose has a name and it is implemented by means a set of *Actions*. During the given consent phase, the Data Subject can choose also to share his/her Personal Data with one or more *Organizations*, so as the controller can eventually achieve the defined purposes. As defined in Art. 7 of the GDPR, Data Subject can withdraw at any time the given consent. In the defined model, this is modeled as the *withdrawnBy* association between Data Subjects and Consent entities reported in Figure 5.

In the current implementation, CaPe encodes the instances of the defined model as Json files, and it then provides such a files to the GENERAL_D Framework for the aim of making the given consent directly enforceable by the Smart ICT Core System.

4.2 Access Control Manager: GENERAL_D Framework

GENERAL_D Framework instantiates the Access control Manager, and it is composed of four main components (see Figure 6): User Stories Manager; Json Manager; ACP Manager; and DBs Manager.

User Stories Manager. manages a Data Protection Backlog that contains GDPR-based User Stories (Bartolini et al., 2019b). In the considered implementation, these are specific ACP templates, each associated with specific GDPR's provision,

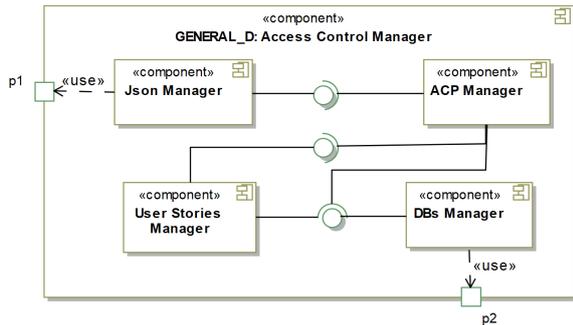


Figure 6: Overview of GENERAL_D Access Control Manager.

useful for automating the implementation of standardized access control policies in compliance with the regulation. In our case, the here considered User Stories are templates structured as abstract XACML policies, and they are stored in an internal database (not shown in Figure 6).

Json Manager. has the responsibility to interact directly with CaPe described in the previous section. It receives the consent in Json format, and it parses that consent so as to extract the relevant information for the ACPs generation purpose. Such information includes, among others, the *Consent ID* and the *Consent Usage Rules* that contain the defined purposes of processing, the allowed operations, and Personal Data provided by the Data Subject.

ACP Manger. is the core component of GENERAL_D framework. It has the responsibility of creating enforceable ACPs encoded in the XACML language. It interacts with: 1) Json Manager for retrieving the data to be processed (e.g., the Controller’s data, the defined purposes, the list of allowed third parties); 2) User Stories Manager for receiving the ACPs templates to be filled with those data. Therefore, ACP Manager combines the received data for deriving XACML policies, that it stores in the Access Control Policies repository.

DBs Manager. offers databases supporting functionalities to the User Stories Manager and ACP Manger (e.g., create/modify/delete database, and insert/modify/delete specific entries in the available tables). In the considered implementation, DBs Manager relies on the MySQL Data Base Management System.

By referring to the Alice’s activities in the myWellness’ application scenario presented at the beginning of this section, and to CaPe’s consent model shown in Figure 5, the algorithm implemented by

GENERAL_D Framework, for deriving enforceable XACML policies, is reported in Algorithm 1.

From the behavioral point of view, the algorithm implements three scenarios:

1. Data Subject (Alice) gives his/her consent to Controller (myWellness company). In this case the XACML-based ACPs are generated from scratch and loaded into the database. These policies will be then made enforceable as soon as the Alice’s activities start, i.e., during the production phase.
2. Data Subject modifies his/her consent, e.g., Alice wants to modify her given consent so as to allow the management only to two of the three initially provided Personal Data. This involves the withdraw of the previously given consent and its substitution with a new one. In terms of the access control policies, this means to modify the related ACPs in DENY-ALL policies and create new ACPs for the modified consent. This behavior is in line with the accountability principle, because it lets the controller to demonstrate the compliance with the GDPR by showing the history of both the consent and the related ACPs modifications. Specifically, it refers to the transparency principle (Art. 5.1(a) “lawfulness, fairness and transparency”) and Art. 30 (“Records of processing activities”).
3. Data Subject (Alice) withdraws the given consent: i.e., prevent any access to Personal Data belonging the Data Subject. In terms of access control, this means to deny any access requests to those data. Practically, this can be enforced by the ACP Manager by setting the related ACPs to DENY-ALL.

From a procedural point, as shown in Algorithm 1, through the Json Manager component, GENERAL_D parses the Json file for retrieving the data of interest, i.e., Personal Data, Purposes and the third parties those data are shared with. Then, through the joint collaboration of ACP Manager and User Stories Manager, the ACPs templates can be instantiated for generating XACML-based policies that are compliant with the GDPR (GENERAL_D Framework’s outcomes).

In details, the Algorithm 1 (line 1) takes as input the consent represented in Json format (CJF), and it parses that file by obtaining its internal representation (CJFAsPOJO, line 4). Then, in case of active consent (Algorithm 1, line 6), the algorithm verifies whether the processed consent is a modification of an already given one. In case of modification, the related ACPs derived so far are modified to DENY-ALL policies (Algorithm 1, line 8). Consequently,

for each User Story and for each consent related to a specific purpose, an XACML policy is generated (Algorithm 1, line 11-16). In case of withdrawing the content, the received Json input contains the status *non-Active* (Algorithm 1, line 17), and in terms of AC, this means that no one is able to access Personal Data related Data Subject. This is reflected in denying all the incoming access requests, by triggering the default DENY-ALL policies modified in Algorithm 1, line 18.

```

Algorithm 1: GDPR-based ACP Derivation.
1: input: CJF                ▷ Consent as Json File
2: output: GAL             ▷ GDPR-based ACP List of XACML
   policies
3: GAL ← {}
4: CJFAsPOJO ← parse(CJF)
5: cID ← CJFAsPOJO.getCID()
6: if CJFAsPOJO.isActive() then
7:   if isAlreadyGiven(cID) then
8:     DenyAllPolicies(cID)
9:   end if
10:  USTL ← loadUserStoriesTempaltes()
11:  Foreach usti ∈ USTL do
12:    Foreach cj ∈ CJFAsPOJO do
13:      ACP ← CreateACPS(usti, cj, cID)
14:      GAL.add(ACP)
15:    end for
16:  end for
17: else if !CJFAsPOJO.isActive() then
18:   DenyAllPolicies(cID)
19: end if
20: return GAL
    
```

By referring to the previously presented Use Case scenario, and by applying Algorithm 1, we illustrate in Figure 7 one of the obtained ACPs in XACML-like format. This policy rules access to the Personal Data as defined in Art. 6.1(a), i.e., when the processing activity is lawful based on the consent given by the Data Subject. As in the figure, the allowed subjects, to access Alice’s Personal Data, are both myWellness (Controller) and zzz-HealthOrg (Third Party). This is expressed in the Target element of the XACML policy. As specified in the derived rule, the purpose of processing (i.e., MyCholesterol purpose) is achieved by allowing access to perform a specific set of Actions, i.e., AGGREGATE, COLLECT, DERIVE and QUERY.

5 CONCLUSIONS

Smart ICT Systems are gaining a certain amount of attention in the last years. They provide means for developing Smart Services in different domains such as Smart-Cities, Education, and Healthcare environ-

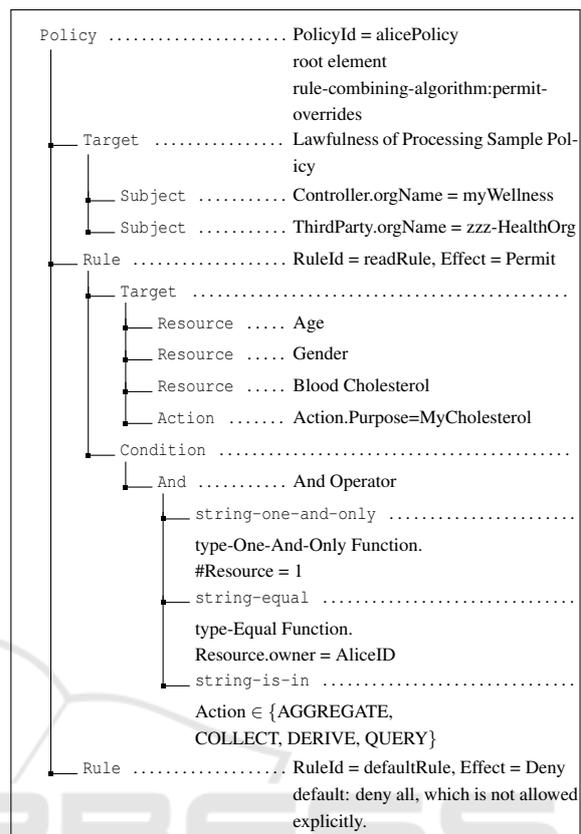


Figure 7: An XACML-like Policy authorizing Lawfulness of processing of Personal Data based of the Consent Given by the Data Subject (Art. 6.1(a)).

ments, to cite a few. However, with the entering into the force of the EU data protection regulation, i.e., the GDPR, proposed solutions for Smart ICT Systems lack appropriate supports to aid Controllers in developing Smart Services. More precisely, the proposed solutions are not Privacy-By-Design conceived, i.e., the implemented services are not compliant with the GDPR from the early stage of their design. To overcome these difficulties, we have conceived a possible generic architecture that can be customized with real artifacts to accomplish the GDPR compliance. We have also provided a proof-of-concept consisting of the integration of two new tools coming from the industrial and academic sectors: CaPe and GENERAL_D Framework. This integration has demonstrated the applicability and flexibility of our Privacy-By-Design solution for Smart ICT Systems.

For future work, we are planning to validate our approach by considering a Smart-Cities environment. In particular, the integration will be validated in the currently available and emerging Smart-Cities platforms, such as the ones based on the market-ready open-source software FIWARE platform.

ACKNOWLEDGEMENTS

This work is partially supported by CyberSec4Europe H2020 Grant Agreement No. 830929.

REFERENCES

- Åkerlund, A. and Große, C. (2020). Integration of data envelopment analysis in business process models: A novel approach to measure information security. In *ICISSP*, pages 281–288.
- Barsocchi, P., Calabrò, A., Ferro, E., Gennaro, C., Marchetti, E., and Vairo, C. (2018). Boosting a low-cost smart home environment with usage and access control rules. *Sensors*, 18(6):1886.
- Bartolini, C., Calabrò, A., and Marchetti, E. (2019a). Enhancing business process modelling with data protection compliance: An ontology-based proposal. In *Proceedings of the 5th International Conference on Information Systems Security and Privacy, ICISSP 2019, Prague, Czech Republic, February 23-25, 2019*, pages 421–428.
- Bartolini, C., Daoudagh, S., Lenzini, G., and Marchetti, E. (2019b). Gdpr-based user stories in the access control perspective. In Piattini, M., da Cunha, P. R., de Guzmán, I. G. R., and Pérez-Castillo, R., editors, *Quality of Information and Communications Technology - 12th International Conference, QUATIC 2019, Ciudad Real, Spain, September 11-13, 2019, Proceedings*, volume 1010 of *Communications in Computer and Information Science*, pages 3–17. Springer.
- Bartolini, C., Daoudagh, S., Lenzini, G., and Marchetti, E. (2019c). Towards a lawful authorized access: A preliminary gdpr-based authorized access. In van Sinderen, M. and Maciaszek, L. A., editors, *Proceedings of the 14th International Conference on Software Technologies, ICSoft 2019, Prague, Czech Republic, July 26-28, 2019*, pages 331–338. SciTePress.
- 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*.
- Calabrò, A., Marchetti, E., Moroni, D., and Pieri, G. (2019). A dynamic and scalable solution for improving daily life safety. In *Proceedings of the 2nd International Conference on Applications of Intelligent Systems*, pages 1–6.
- Carauta Ribeiro, R. and Dias Canedo, E. (2020). Using mcdm for selecting criteria of lgpd compliant personal data security. In *The 21st Annual International Conference on Digital Government Research, dg.o '20*, page 175–184, New York, NY, USA. Association for Computing Machinery.
- Dernaika, F., Cuppens-Boulaïhia, 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.
- 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.
- Greaves, B., Coetzee, M., and Leung, W. S. (2018). Access control requirements for physical spaces protected by virtual perimeters. In Furnell, S., Mouratidis, H., and Pernul, G., editors, *Trust, Privacy and Security in Digital Business*, pages 182–197, Cham. Springer International Publishing.
- Haofeng, J. and Xiaorui, G. (2019). Wi-fi secure access control system based on geo-fence. In *2019 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–6.
- Jensen, C. D., Geneser, K., and Willemoes-Wissing, I. C. (2013). Sensor enhanced access control: Extending traditional access control models with context-awareness. In Fernández-Gago, C., Martinelli, F., Pearson, S., and Agudo, I., editors, *Trust Management VII*, pages 177–192, Berlin, Heidelberg. Springer Berlin Heidelberg.
- Krenn S. et al. (2020). Deliverable D3.2: Cross Sectoral Cybersecurity Building Blocks. https://cybersec4europe.eu/wp-content/uploads/2020/06/D3.2-Cross_sectoral_cybersecurity-building-blocks-v2.0.pdf.
- Neuhüttler, J., Fischer, R., Ganz, W., and Urmetzer, F. (2020). Perceived quality of artificial intelligence in smart service systems: A structured approach. In Shepperd, M., Brito e Abreu, F., Rodrigues da Silva, A., and Pérez-Castillo, R., editors, *Quality of Information and Communications Technology*, pages 3–16, Cham. Springer International Publishing.
- OASIS (2013). eXtensible Access Control Markup Language (XACML) Version 3.0. <http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html>.
- Samir Labib, N., Liu, C., Esmaeilzadeh Dilmaghani, S., Brust, M., Danoy, G., and Bouvry, P. (2018). White paper: Data protection and privacy in smart ict-scientific research and technical standardization. Technical report, ILNAS.
- Sforzin A. et al. (2020). Deliverable D3.11: Definition of Privacy by Design and Privacy Preserving Enablers. <https://cybersec4europe.eu/publications/deliverables/>.
- Sokolovska, A. and Kocarev, L. (2018). Integrating technical and legal concepts of privacy. *IEEE Access*, 6:26543–26557.