





# Towards a Lawful Authorized Access: A Preliminary GDPR-based Authorized Access

Cesare Bartolini<sup>1</sup> <sup>a</sup>, Said Daoudagh<sup>2,3</sup> <sup>b</sup>, Gabriele Lenzini<sup>1</sup> <sup>c</sup> and Eda Marchetti<sup>2</sup> <sup>d</sup>

<sup>1</sup>Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg

<sup>2</sup>Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo", CNR,  
via G. Moruzzi 1, 56124, Pisa, Italy

<sup>3</sup>Computer Science Department, University of Pisa, Pisa, Italy

Keywords: Access Control Policy, GDPR.

Abstract: The General Data Protection Regulation (GDPR)'s sixth principle, *Integrity and Confidentiality*, dictates that personal data must be protected from unauthorised or unlawful processing. To this aim, we propose a systematic approach for authoring access control policies that are by-design aligned with the provisions of the GDPR. We exemplify it by considering realistic use cases.

## 1 INTRODUCTION

The new General Data Protection Regulation (GDPR) is changing how *Personal Data* should be processed. It states, in Art. 5.1(f), that “[data] should be processed in a manner that ensures appropriate security of the personal data [...] using appropriate technical or organisational measures (integrity and confidentiality)”.

Access Control (AC) systems can be such a measure. AC is a mechanism used to restrict access to data or systems according to 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). By implementing them, one can gain compliance to the principle of Integrity and Confidentiality, but when enriched with policies elicited from the GDPR's provisions, we believe, AC systems can realize a compliance by-design to the GDPR's provisions expressed in the policies.


According to the GDPR, resources are Personal Data while the Controller, the Processor, or the Data Subject are those requesting access to them. But, besides this simple mapping, it may be challenging for ACPs designers to *identify*, to *extract*, to *translate* and to *encode* the GDPR's provisions into enforceable


ACPs (Xiao et al., 2012). Provisions can be ambiguous and can include implicit information. They are also unstructured and therefore not straightforwardly expressible in a formal policy. This call for a systematic process, following which one can design ACPs properly linked to the GDPR. Failing this task may have serious consequences: not only the AC system enforcing them will leave unprotected personal data but, in the specific context of the GDPR, it will also become unlawful.


The risk can be mitigated by promoting the adoption of AC systems with policies which are systematically designed for expressing GDPR's provisions, and in this paper we make a step towards this goal.


Recent literature provides partial solutions to this problem. In (Fatema et al., 2016), for instance, the authors propose an approach to extract ACPs from the Data Protection Directive (Directive 95/46/EC), the document that before the GDPR was a reference point for the protection of personal data. In (Brossard et al., 2017) the authors discuss an approach for implementing Attribute-Based AC policies tailored to the protection of resources in an industrial setting; although the proposal is an example of systematic implementation of policies, it does not consider any legal framework.

Our proposal is to leverage those results by combining them and by providing a unified framework able to design ACPs in reference to the legal framework of the GDPR. In particular, inspired by the principle of *Data Protection by-design*, we discuss how to develop such ACPs by gathering access control AC

<sup>a</sup>  <https://orcid.org/0000-0002-6538-3466>

<sup>b</sup>  <https://orcid.org/0000-0002-3073-6217>

<sup>c</sup>  <https://orcid.org/0000-0001-8229-3270>

<sup>d</sup>  <https://orcid.org/0000-0003-4223-8036>

requirements from the GDPR.

**Outline.** We recall the GDPR and AC in section 2, where we also discuss the related work. In section 3 we describe a simple scenario used as reference in the remaining sections. In section 4 we describe our approach and in section 5 we apply it. In section 6 we conclude and point out the future work.

## 2 BACKGROUND

**GDPR Concepts.** The General Data Protection Regulation (GDPR)<sup>1</sup> has been conceived to strengthen the rights of natural persons over their own data and at the same time to make organizations accountable. The mandatory part of the GDPR contains 99 Articles. Art. 4 defines *Personal Data* as any information related to an identified or identifiable natural person, called the *Data Subject*. Art. 6 states that the *Purpose* of the *Processing* of personal data is determined by the *Controller*, and this “processing shall be lawful only if and to the extent that at least one of the” six legal bases “applies”. In particular, item 1(a) of the article, states that one of those legal bases is the *Consent* given by the data subject “to the processing of his or her personal data for one or more specific purposes”. Art. 7 introduces the duty to demonstrate the consent and the right to withdraw it.

The GDPR sets other fundamental rights of the data subject, such as the *Right of access by data subject* (Art. 15) and the new *Right to data portability* (Art. 20), and several principles that the controller and processor shall abide. For a full reference, we remand the reader to original text of the Regulation.

**Access Control Context.** Among the AC models proposed in the literature, we refer to the Attribute-Based Access Control (ABAC) (Jin et al., 2012) which is currently one of the mostly adopted in industrial environment (Hu et al., 2019). The basic idea of ABAC is to use attributes of different entities to formulate access control decisions regarding a subject’s (e.g., user, process, or legal entity such as controller and data subject) access on an object (e.g., file, database or personal data) in a system. The authorization decisions are obtained by means of authorization policies specified using a policy specification language. ABAC policies are a set of rules defined based

<sup>1</sup>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).

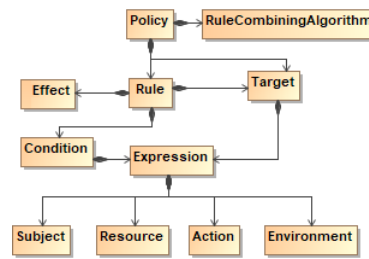


Figure 1: XACML Policy Data Model.

on the attributes of subjects, objects and operations as well as other attributes, such as contextual or environmental attributes.

The ABAC model is usually implemented using the eXtensible Access Control Markup Language (XACML) (OASIS, 2013), which is a *de facto* standardized specification language that defines ACPs and access control decision requests/responses in a XML format. A XACML policy defines the access control requirements of a protected system. An access request that aims at accessing a protected resource is first evaluated against the policy, after which the access is granted or denied. A *XACML Request* is composed of four main elements: 1. *Subject*, the entity requesting the access; 2. *Resource*, the requested object that is described in terms of attributes; 3. *Action*, the operation that the subject wants to perform; 4. *Environment*, the contextual information such as the request time and the location. By referring to the GDPR we assume that the *consent* is a contextual information. The core component of a *XACML Policy* is the *Rule*, which represents the basic enforceable element: it is composed of an *Effect* (Deny or Permit value); *Target* which defines the applicability of the rule, and *Condition* that represents a more complex boolean function. The effect of the rule is returned when the evaluation of a given request meets the constraints of its target and condition. The rules are organized in policy which contains a *Combining Algorithm*. The algorithm defines the way to obtain a single decision in case of two or more rules are evaluated true. Figure 1 reports the XACML policy data model.

**Legal Ontologies.** Designing ACPs in reference to the GDPR requires to refer, within a policy, to GDPR concepts and to relationships among them. It also demands for a consistent vocabulary along the whole lifecycle of the development of the ACPs. An help in this direction comes from semantic web technologies and in particular from the legal ontologies. Among the legal ontologies currently available, in this paper we refer to the Privacy Ontology (PrOnto) “that aims to provide a legal knowledge modelling of the privacy agents, data types, processing operations, rights and

obligations” (Palmirani et al., 2018).

**Related Work.** In literature there are several works that use access control as main means of protecting personal data. For example, authors in (Cerbo et al., 2018) report an initial proposal for an automatically enforceable policy language for access and usage control of personal information, aiming at transparent and accountable data usage. A formal definition of the consent is introduced in (Ulbricht and Pallas, 2018), where the authors defined a privacy preference language explicitly designed to fulfill consent-related requirements and to suit constrained execution environments. Only some proposals take as an explicit reference a determined data protection law. For instance, the HIPAA was considered as a case study in (Chowdhury et al., 2012) where the authors have evaluated whether the XACML standard is adequate to express the constraints imposed in HIPAA. A work closer to ours is reported in (Fatema et al., 2016). Here the authors examined the feasibility of translating the articles related to access control of the directive, and also provided an implementation. In the industrial environment, authors in (Brossard et al., 2017) proposed a systematic methodology for the implementation of ABAC solutions in real contexts.

However all the available proposals either focus only some aspects of the GDPR or do not provide implementations or are not specific for legal requirements. Differently from these works, this paper aims at defining a systematic approach for gathering as many GDPR requirements as possible so to comply with the regulation, and consequently provide ACPs in line with the GDPR.

### 3 RUNNING EXAMPLE

In explaining our proposal, we refer to a simple scenario (see Figure 2). A customer *Alice* (the data subject) wants to purchase goods online from *ABC* (the controller), an e-commerce company which provides an online service for ordering and delivering goods. *ABC* follows two marketing strategies, both using customer personal data: (1) *Untargeted Marketing*: the customers’ E-mail is used to advertise novelties, such new services or special sales; (2) *Location-based Targeted Marketing* (or *Geomarketing*): a customers’ location is processed to customise the user experience of who is visiting the platform that provides the service.

After the GDPR entered into force, *ABC* wants to adopt an AC systems to be compliant to the GDPR obligations. Its main objectives are: (1) to regulate

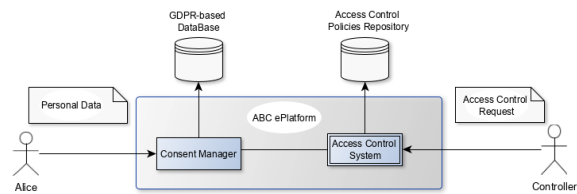


Figure 2: E-Commerce Scenario.

the access to personal data; (2) to guarantee that its processing is lawful; (3) to facilitate data subjects in exercising their rights.

## 4 THE PROPOSED APPROACH

Our approach has three phases: (1) *GDPR-based ACP Template Generation* (2) *Legal Use Cases Definition*; (3) *Access Control Policies Authoring*.

**Phase 1: GDPR-based ACP Template Generation.** The GDPR text is analysed in search for provisions that spot a relation with AC so as to derive a meta-model (i.e., ACP template) for each of them.

This phase is organized in ten activities (see Figure 3). The first six (from ① to ⑥) aim at selecting only the articles related to access control and discard all the remaining ones (activity ④). Subsequently, the selected articles are then distinguish between articles related to ACPs (activity ⑤) and the ones related to AC mechanism (activity ⑥). The former group is used for the definition of meaningful ACPs. The latter is used to gather legal requirements from the architectural point of view, and it is out of the scope of the current paper. Indeed, the collected functional and non-functional requirements will be used during the ACPs enforcement. During the activity ⑦ all and only the attributes relate to AC are identified. The selection of these attributes is driven by a conceptual model of the GDPR as they are represented in the PrOnto ontology. Thus, we restricted our study to the concepts described within PrOnto representation.

For aim of completeness, we report the following sentence, as a simple example, where the identified GDPR-based attributes are highlighted:

**Data Subject** can access his **Personal Data**.

The next activity (⑧) is then aimed to classify the identified attributes into the commonly-used entities (or categories) in AC, namely, *Subject*, *Resource*, *Action* and *Environment*. For instance, considering the above sentence, the identified attributes are classified as reported in the following:

**Data Subject**<sub>[Subject]</sub> can **access**<sub>[Action]</sub> his **Personal Data**<sub>[Resource]</sub>

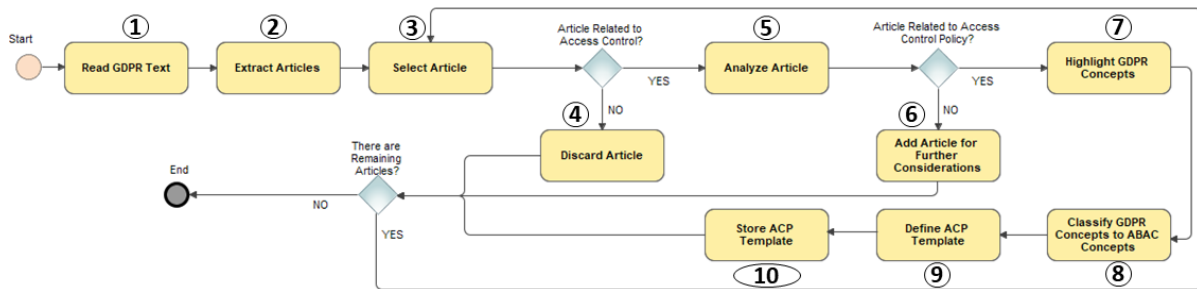


Figure 3: GDPR Articles Selection and Templates Generation Process.

In ABAC terms **Data Subject** is classified as a *Subject*, **access** is classified into the *Action* category, and finally **Personal Data** is classified as a *Resource* category.

Finally, the last two activities ((9) and (10)) involve the definition of GDPR-based ACP templates, where the natural language statements are transformed in a machine-readable representation and the relations between attributes identified.

Considering the previous example, we need to clarify the meaning of **his** and to define possible relations between the attributes *Data Subject* and *Personal Data*. Article 4(1) can be used for the purpose. Specifically, it states that: ‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, [...]; this means that the Personal Data have the property of identifying a particular Data Subject. We can express this property as:

$$\text{DataSubject} = \text{PersonalData.Owner}$$

Consequently, a possible GDPR-based ACP template related the aforementioned sentence could be:

$$((\text{Subject} = \text{Data Subject}) \wedge (\text{Resource} = \text{Personal Data}) \wedge (\text{Action} = \text{access}) \wedge (\text{Data Subject} = \text{PersonalData.Owner})) \implies (\text{Authorization} = \text{Permit})$$

**Phase 2: Use Cases Definition and ABAC Attributes Selections.** Depending on the peculiarities of the specific application scenarios and the selected GDPR articles, the use cases are defined, customized and better specified for each user of the system, e.g., Data Subject or Controller to gather AC requirements in terms of concrete attributes. The second phase is then made up of two main steps.

**Step 1. Legal Use Case Definition** which includes the development of ACPs able to guarantee by design some of the Data Subject’s rights, such as the right

of access of personal data (Article 15) and the right to data portability (Article 20). This is in line with the Article 12.2, which is worded as follows: “The controller shall facilitate the exercise of data subject rights under Articles 15 to 22. [...]”. Indeed, on the basis of the template developed in the first phase (section 4), the controller can automatically, easily and promptly setting up customized ACPs as soon as the consent is obtained from a data subject and in line with the GDPR provisions. This allows the controller to act *without hindrance* and *without undue delay* (pursuant to Article 20) to wishes of the data subject to exercise his/her rights. As a consequence, the data subject can exercise his/her rights as soon as the ACPs become enforceable from the access control system, i.e., when the policies are deployed in the ACPs repository.

To better explain the proposed methodology, we consider the running example from section 3. We suppose that Alice, at registration time within the ePlatform, provided the ABC company her name, her E-mail address, and the name of the city where she has the permanent address. We also assume that, at a later moment, Alice wanted to know which data she gave to the ABC Company during the registration, so as to exercise her right of access pursuant to Article 15.1.

Consequently, ABC defined the following authorization requirement:

**ABC Req:** Alice can read her name, E-mail, and her permanent city.

Of course, without the appropriate access control mechanisms, the specified authorization requirement could hardly be enforced. For this, the next activity.

**Step 2. AC Attribute Identification and Classification** We identify AC attributes directly from the *Legal Use Case* and . for each of them: (1) the specific category is defined. This includes categories of data subjects, e.g., customer or employee and categories of personal data, e.g., biodata, financial data, health data or biometric data and so on; (2) the proper classification is identified. This include to classify the attributes according to the commonly used enti-



ties (or categories) of AC specification, i.e., Subject, Resource, Action and Environment.

By referring to the requirement **ABC Req**, the identified attributes are highlighted as follows:

**ABC Req:** Alice can read her name, E-mail, and her permanent city.

A possible classification of those attributes is then reported in Table 1, where (1) column *Identified Attribute* contains the identified attributes; (2) column *Attribute Category* shows a possible classification of those attributes into a specific category<sup>2</sup>; (3) while column *AC Category* illustrates the classification attributed into the commonly used entities in AC.

Table 1: Attribute Classification Example.

Identified Attribute	Attribute Category	AC Category
Alice	Customer	Subject
read		Action
name	Biodata	Resource
E-mail	Contact data	Resource
permanent city	Location data	Resource

**Phase 3: Authoring and Assessing the GDPR-based ACPs** The first two phases provide the necessary building blocks for authoring and assessing concrete, meaningful and enforceable ACPs. This phase is composed of three steps: (1) *Attribute Matching*; (2) *Authoring the GDPR-based ABAC Policy*; and (3) *Assessing the GDPR-based ABAC Policy*.

**Step 1: Attributes Matching.** The GDPR-based attributes identified in **Phase 1** are connected and instantiated with the concrete ABAC attributes identified in **Phase 2**. The process we adopted for this aim is illustrated in Figure 4. Therefore, by referring to the requirement **ABC Req**, *Alice* is classified as *Data Subject*; the *read* action is connected to the *access* one; and finally, *Name*, *E-mail* and *Permanent City* attributes match *Personal Data* one.

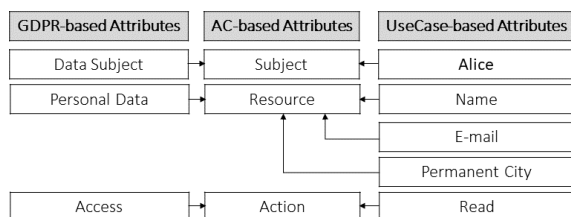


Figure 4: Attributes Matching Example.

**Step 2. Authoring the GDPR-based ABAC Policy** The concrete and enforceable ACPs are obtained by performing two activities: (1) instantiate the ACP

<sup>2</sup>Note that classification refers only to the personal data and not to the processing operations such as *read* action.

templates (see **Phase 1**) with actual attributes gathered from the legal use cases, as in **Phase 2** and (2) translate the resulting policies in a given formalism or language<sup>3</sup>.

Consequently, by referring to the classification of the attributes of **ABC Req** defined in **Phase 2** and to the policy defined during the *Authoring Access Control Templates* activity of **Phase 1**, a possible abstract ACP looks like the following:

$$\begin{aligned}
 & (\text{Subject} = \text{Alice}) \wedge (((\text{Resource} = \text{Name}) \wedge \\
 & (\text{Subject} = \text{Name.owner})) \vee ((\text{Resource} = \text{E-mail}) \wedge (\text{Subject} = \text{E-mail.owner})) \vee ((\text{Resource} = \text{PermanentCity}) \wedge (\text{Subject} = \text{PermanentCity.owner}))) \wedge (\text{Action} = \text{read}) \implies \\
 & (\text{Authorization} = \text{Permit})
 \end{aligned}$$

The second activity involves the translation of the abstract ACP into a reference formalism or language. In this paper we refer to the widely used XACML standard (OASIS, 2013) to express the GDPR-based ABAC policies; but, one can choose any other implementation of ABAC model. An example of a concrete XACML policy is provided in section 5.

**Step 3: Assessing the GDPR-based ABAC Policy** The last step is in charge of checking whether the authored GDPR-based policies conform with intended access rights, i.e., it verifies the correctness of the authored policies. In literature different proposals target the problem of policy assessment and are generally divided into: model-based testing (Xu et al., 2015), combinatorial based (Bertolino et al., 2013). We refer to the literature for more details.

## 5 APPLICATION EXAMPLE

In this section we illustrate the application of our approach to the GDPR. To this regard, we first selected the articles related to AC and then we provided a ACP model for each of them (**Phase 1** of the approach). This allows the controller, or his/her delegate (e.g., an internal security administrator), to write ACPs in line with the GDPR according to the principle of data protection by design and by default. Consequently, the usage scenario and required attributes have been defined (**Phase 2**.) Finally, the ACP templates have been instantiated so as to obtain enforceable ACPs (**Phase 3**).

<sup>3</sup>The approach aims at providing a generic ACP i.e., an independent representation from any formalism. This helps one to author ACPs in different languages that refer to different formalisms such as ABAC and Role-Based Access Control (RBAC). For aim of clarity, here, we illustrate how to encode actual ACPs by referring the ABAC model and its implementation XACML.

**Phase 1.** From a procedural point of view, we firstly parsed the text of the GDPR (*Read GDPR Text* activity) and we selected only 99 articles<sup>4</sup>(*Extract Articles*). For each selected article (*Select Article*), we evaluated its adherence to the concept of access control: not pertinent the articles have been consequently discarded (*Discard Article*). The remaining ones have been further analyzed (*Analyze Article*) to assess whether they could be related either to ACP concepts or the AC mechanisms (*Add Article for Further Considerations*). As final results, among the 99 selected articles, only forty-one have been considered as related to access control. Specifically: three of them were concerning only AC mechanisms; eight were referring only ACPs, and thirty articles related to both ACPs and AC mechanisms. Consequently, only thirty-eight articles have been used to derive GDPR-based ACP templates.

As an example, in the remaining of the section we illustrate the proposed approach only for one of the final selected articles, which is related to the management of both the purpose and the consent given by the data subject.

### 5.1 Lawfulness of Processing

For providing a lawful authorized access of personal data by the controller the first step is to guarantee that all the accesses authorized by the AC system (or processing activities in general) are based on lawful basis. To this purpose, the Article 6 lists as first basis the Consent: this is the most general concepts and the most critical for a legal point of view<sup>5</sup>. Specifically, during the *Highlight GDPR Concepts* activity (see Figure 3), we refer to the sub-paragraph of the Article 6.1(a) which words:

Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given **consent** to the **processing** of his or her **personal data** for one or more specific **purposes**;

Consequently, by referring to the PrOnto ontology we identified the following four GDPR concepts, as highlighted before: (1) consent, (2) processing, (3) personal data, and (4) purposes.

During the activity *Classify GDPR Concepts into ABAC*, we classified personal data as *Resource* and processing as *Action*. Concerning the purposes attribute, we distinguished the purpose for which the

<sup>4</sup>In this proposal we focused on the articles that are mandatory.

<sup>5</sup>For more details we refer to the *Guidelines on consent under Regulation 2016/679* of the Article 29 Working Party (WP29).

personal data is collected and the purpose for which the data is requested or accessed. For this, we referred to the XACML Privacy Policy Profile (OASIS, 2015) provided by the XACML standard. This specification describes a profile of XACML for expressing privacy policies and defines two attributes and one rule: (1) the **resource:purpose** attribute “indicates the purpose for which the data resource was collected”. (2) the **action:purpose** attribute “indicates the purpose for which access to the data resource is requested”; while, (3) the defined rule “stipulates that access shall be denied unless the purpose for which access is requested matches [...] the purpose for which the data resource was collected”.

Therefore, since the purposes listed in Article 6 refers to the purposes for which the personal data was collected, we classified the identified attribute as *Resource*, and more precisely as an attribute of personal data.

The same strategy has been adopted for the consent as well, i.e., we defined the consent as a special attribute of the specific purpose for the personal data is collected. In case of personal data, we considered the consent as a **BOOLEAN** contextual attribute. This allows the controller to manage also the right of the data subject “to withdraw his or her consent at any time” pursuant the Article 7 (*Conditions for consent*). As a consequence the consent attribute has been classified as Environment attribute with the following result:

[...] (a) the data subject has given **consent**<sub>[Environment]</sub> to the **processing**<sub>[Action]</sub> of his or her **personal data**<sub>[Resource]</sub> for one or more specific **purposes**<sub>[Resource]</sub>.

During *GDPR-based ACP Template* activity, the following ACP template associated the Article 6.1(a) has been derived:

$$((\text{Resource} = \text{PersonalData}) \wedge (\text{Action} = \text{processing}) \wedge (\text{Action.purpose} = \text{PersonalData.purpose}) \wedge (\text{PersonalData.purpose.consent} = \text{YES})) \implies (\text{Authorization} = \text{Permit})$$

Table 2: Legal Use Case: Attribute Classification.

Identified Attribute	Attribute Category	AC Category
<i>Req 1</i>		
ABC company	Controller	Subject
Alice	Customer	Subject
send		Action
E-mail	Contact data	Resource
Consent		Environment
untarget marketing	purpose	Resource

**Phase 2.** A possible **Legal Use Case** aligned with Article 6.1(a) concerns the registration phase within the ePlatform and the actions required by the controller to obtain the explicit consent from its customers. More precisely, by referring the scenario in section 3, to use the online service provided by the ABC company, Alice needs to create an account within the ePlatform (see Figure 2), and submits a set of personal data, i.e., Name, Surname, E-mail Address, Home Address, the Gender, and Birthdate. Afterwards *Consent Manager* asks Alice her consent for processing some of her personal data for the purposes defined by Controller, i.e., Untarget and Location-based target marketing. Consequently, Alice for each requested consent gives or denies her consent. In particular, we consider the specific situation in which she gives only the explicit consent of processing her E-mail Address for Untarget Marketing purpose, and withhold her consent for Geomarketing purpose. Finally, the Consent Manager stores and sends the collected information to the AC System for authoring an ACP related to Alice. A possible authorization requirement related to Alice’s consent is:

**Req 1: ABC company** (Controller) can **send** communications only for **untarget marketing purpose** using the **E-mail** of Alice, because of the **consent** given.

The next activity is the **Access Control Attribute Identification and Classification** where the attributes based on the above requirements are identified, and reported in the first column of Table 2. The table depicts the classification of the identified attributes into a commonly used access control categories as well.

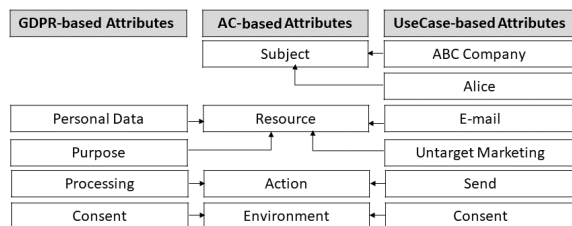


Figure 5: Article 6.1(a): Attributes Matching.

**Phase 3** Due to space limitation, in the following we report only the result of the **Attribute Matching** (see Figure 5) and **authoring policy** activities, considering **Req 1** (see Figure 6).

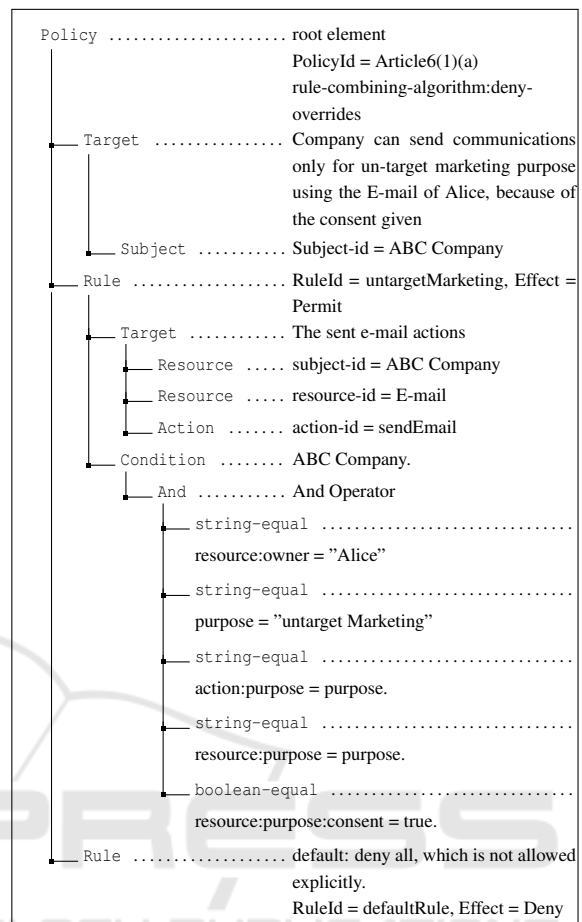


Figure 6: A Possible XACML Policy for Article 6.1(a).

## 6 CONCLUSION AND FUTURE WORK

This paper presented a systematic approach to gather access control requirements from the GDPR. This approach is the first step towards a formal definition of an access control solution based on the GDPR.

Although grounded in a domain-related implementation (i.e., compliance to the GDPR), the approach yields a more general spectrum, since it can be applied to different data protection regulations and more in general to any legal text that implicitly contains, or suggests, data protection requirements. To the best of the authors’ knowledge, the novelty of the paper is the systematic approach to join and improve the current academic proposals for the extraction of legal by-design ACPs from the data protection regulation with the approaches currently used in industrial environment for implementing ABAC.

As future work, we are planning to consider the

GDPR requirements referring access control mechanisms, i.e., from the architectural point of view. The analysis will investigate functional and non-functional requirements so to assess the adequacy of the current reference architecture (e.g., XACML) and to provide possible extensions to align the access control mechanisms to the GDPR principles.

We also intend to investigate thoroughly on the expressiveness and adequacy of policy languages of current access control models, such as ABAC and RBAC, to eventually make legally sufficient access control systems. This research may either bring evidence that current model are adequate for the task or lead to formal extensions of the ABAC and RBAC core models.

## REFERENCES

- Bertolino, A., Daoudagh, S., Lonetti, F., Marchetti, E., and Schilders, L. (2013). Automated testing of extensible access control markup language-based access control systems. *IET Software*, 7(4):203–212.
- Brossard, D., Gebel, G., and Berg, M. (2017). A systematic approach to implementing abac. In *Proceedings of the 2Nd ACM Workshop on Attribute-Based Access Control*, ABAC '17, pages 53–59, New York, NY, USA. ACM.
- Cerbo, F. D., Martinelli, F., Matteucci, I., and Mori, P. (2018). Towards a declarative approach to stateful and stateless usage control for data protection. In *WEBIST*, pages 308–315. SciTePress.
- 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.
- Fatema, K., Debruyne, C., Lewis, D., OSullivan, D., Morrison, J. P., and Mazed, A. (2016). A semi-automated methodology for extracting access control rules from the european data protection directive. In *2016 IEEE Security and Privacy Workshops (SPW)*, pages 25–32.
- Hu, C. T., Ferraiolo, D. F., Kuhn, D. R., Schnitzer, A., Sandlin, K., Miller, R., and Scarfone, K. (2019). Guide to attribute based access control (abac) definition and considerations [includes updates as of 02-25-2019]. Technical report.
- Jin, X., Krishnan, R., and Sandhu, R. (2012). A unified attribute-based access control model covering dac, mac and rbac. In *Data and Applications Security and Privacy XXVI*, pages 41–55, Berlin, Heidelberg. Springer Berlin Heidelberg.
- 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>.
- OASIS (2015). XACML v3.0 Privacy Policy Profile Version 1.0. <http://docs.oasis-open.org/xacml/3.0/privacypv1.0/xacml-3.0-privacy-v1.0.html>.
- 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: The Thirty-first Annual Conference, Groningen, The Netherlands, 12-14 December 2018.*, pages 91–100.
- Sandhu, R. S. and Samarati, P. (1994). Access control: principle and practice. *IEEE Communications Magazine*, 32(9):40–48.
- Ulbricht, M. and Pallas, F. Yappl - A lightweight privacy preference language for legally sufficient and automated consent provision in iot scenarios. In *DPM 2018 and CBT 2018 - ESORICS 2018 International Workshops, Barcelona, Spain, September 6-7, 2018*.
- Xiao, X., Paradkar, A., Thummalapenta, S., and Xie, T. (2012). Automated extraction of security policies from natural-language software documents. In *Proceedings of the ACM SIGSOFT FSE '12*, FSE '12, pages 12:1–12:11, New York, NY, USA. ACM.
- Xu, D., Kent, M., Thomas, L., Mouelhi, T., and Le Traon, Y. (2015). Automated model-based testing of role-based access control using predicate/transition nets. *IEEE Transactions on Computers*, 64(9):2490–2505.