Integrating Access Control and Business Process for GDPR Compliance: A Preliminary Study

Antonello Calabró[1], Said Daoudagh[12], and Eda Marchetti[1]

[1] Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"
Consiglio Nazionale delle Ricerche, Pisa, Italy
{firstname.lastname}@isti.cnr.it
[2] University of Pisa, Pisa, Italy
said.daoudagh@di.unipi.it

Abstract. Currently, the scientific communities and private companies are actively working to provide theoretical and practical solutions for enforcing the adoption of the General Data Protection Regulation (GDPR) and its compliance problem. In line with the principle of data protection by design, the paper proposes an approach for the automation and enforcement of GDPR requirements. The idea is to extend the currently adopted access control mechanisms so to leverage them to the enforcement of GDPR compliance during business activities of data management and analysis. From a practical point of view, this means to integrate into the existing business processes specific facilities for assisting in the design, development, maintenance, and verification of the GDPR requirements as well as to modify the language and architecture of the access control systems so as to let the management of GDPR principles and obligations. For this, the basic steps of the proposed approach are provided as well as an example used to clarify the integrated use of access control systems and business process models.

Keywords: Access Control, Business Process, GDPR Compliance

1 Introduction

General Data Protection Regulation[3], known as GDPR, is the new EU Data Protection Regulation that became enforceable on May 2018. The purpose of the GDPR is to harmonize the regulation of Data Protection across the EU member states and, at the same time, to enhance and to arise business opportunities within the Digital Single Market space. GDPR imposes several limitations of processing personal data and provides several provisions, defining responsibilities and fines in case of non-compliance.

[3] 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).

In general, implementing GDPR requirements and demonstrating a presumption of compliance, and therefore avoid the related penalties, is not a trivial problem. From a practical point of view, this issue can be reloaded as: making a given Data Management System (DMS) comply with the GDPR legal requirements, and providing the necessary information and evidences so that a supervisor authority could accept this as evidence of the compliance.

Currently, the scientific communities, as well as private companies, are actively working to provide theoretical and practical solutions for enforcing the adoption of the GDPR and its compliance problem. To facilitate this process and tackle the principle of *data protection by design*, contained in Article 25.1 of the Regulation, an important step is the automation the enforcement of GDPR requirements. From this the idea of this paper: improving the currently adopted security services and access control procedures so to leverage them to the enforcement of GDPR compliance during business activities of data management and analysis.

Indeed, the current trend of increasing automation and data exchange promoted by the Industry 4.0 is encouraging many industrial realities to the adoption of visual models, called Business Processes (BPs), to easily manage the assignment of tasks, the interactions between the different roles, and the changes in the organization or in the business activities [18]. Thus, in many enterprises, especially large ones, this means to integrate into their business processes specific facilities for authorization and access management so as to target GDPR needs.

From a practical point to view, there are several possible ways to model a BP; perhaps the most popular and widespread adopted is Business Process Model and Notation (BPMN) [32], which provides a visual representation supported by a formal XML specification. Since BPMN is an extensible standard, it is possible to empower it to express activities related to data protection [26, 41, 3]. The main benefits of BPMN commonly rely on the possibility of having a clear and standard notation for creating a description of processes (in terms of participants and activities) and develop executable frameworks for the overall management of the process itself. Directly integrating, through the usage of security services, the GDPR requirements into the business process execution represents a key aspect both for privacy management and assurance [41, 26].

Following this idea, the solution presented in this paper relies on two pillars: 1) exploit the BPMN models for assisting in the design, development, maintenance, and verification of a system in order to comply with the GDPR requirements, including the detection of possible violations, with the objective to minimize the risk of sanctions being issued by the supervisory authority; 2) leverage the authorization systems, and in particular the access control ones, to tackle the problem of the GDPR compliance.

Integrating in the BPMN the appropriate mechanisms for GDPR definition and compliance can provide a number of benefits: i) it can be used by controllers of personal data for having a clearer view of their duties with respect to data protection in the context of their business; ii) it can be used to check if the

BPMN is compliant with the requirements imposed by the GDPR; iii) it can automatically suggest and perform the mandatory activities and obligations to be met to achieve GDPR compliance; iv) it can be used to discover when specific GDPR obligations are not fulfilled at runtime; and finally, v) it can supply auditors and supervisory authorities with a complete view of the process and the procedures adopted for data protection.

The paper is organized as follows: 2 presents the background about the BP modeling, a brief summary of GDPR structure and content and the basic concepts of access control systems; 3 introduces the basic steps of the propose approach; an example in 4 shows how the proposed approach can be used; 5 provides a survey of existing literature concerning the integration GDPR principle into BP; finally, 6 gives a set of conclusions and the envisioned future work.

2 Background

The present work aims at use the authorization systems, and in particular the access control, into a business process so as to model and to provide a presumption of GDPR compliance. There are many possible ways in which the two might be integrated, depending on the specific purpose; however, all the proposals are based on three building blocks: 1) the model of the business process; 2) the representation of the GDPR; and 3) the access control mechanisms for the enforcement of GDPR requirements.
In the following basic concepts about these three topics are provided.

2.1 Business Processes

Business processes usually refer to any structured collection of related activities or tasks that are carried out to accomplish the intended objectives of an organization. The main focus is creating an abstract but meaningful representation of the real business domains and sharing a formalized definition, so as to improve expressiveness and to make easier the development of tools [23].

Usually, BPMN [32] is the formalism chosen to represent business models, which is the *de facto* standard for process modeling. It is indeed a rich and expressive language (but also a complex one) used for the tasks associated with process modeling [37].

In detail, a BPMN has four categories of graphical elements that can be used to build the diagrams:

1. *Flow Objects* are associated with the actions that can be performed in a business process and make up the behavior of the BP. They consist of Events, Activities, and Gateways;
2. *Connecting Objects* can be used to connect elements to each other in three different ways: Sequence Flows, Message Flows, and Associations;
3. *Swimlanes* give the capability of grouping the primary modeling elements. Swimlanes have two elements through which modelers can group other elements: Pools and Lanes;

4. *Artifacts* are used to provide additional information about the process that does not affect the flow.

In 2 and 5 examples of BPMN are provided.

2.2 General Data Protection Regulation

General Data Protection Regulation, known also as *GDPR*, is the new European Union Law (Regulation) for the protection of *personal data*. GDPR defines *personal data* as any information related to an identified or identifiable natural person called also *data subject*. This means that a data subject is a Natural Person (a living human being), whose data are managed by a *Data Controller*. The regulation became into effect on May 2018 and has replaced the previous Data Protection Directive conceived in 1995. The aim of the new regulation is to strengthen the rights of the individual over their own data and at the same time to make organizations more accountable w.r.t. the previous Directive. In addition, GDPR has also the objective to eliminate all the barriers for the services to be delivered in the European Union and, therefore, to enhance business opportunities within the Digital Single Market. GDPR contributes to the harmonization of the previous fragmented data protection laws across the EU, so to ensure equal protection of Human Rights of the European Citizens.

GDPR is divided into two parts: the first part is composed by 173 Recitals that explain the motivation of the regulation and the intended achievements; the second part is composed by 99 Articles that represent the code. The GDPR regulation is applied to the processing of personal data, whether it is automated (even partially) or not. The new EU regulation defines the following principles regarding data and processing:

- *Transparency*, i.e., data must be processed fairly, lawfully and transparently;
- *Purposes*, i.e., data should only be collected for determined, explicit and legitimate purposes, and should not be processed later for other purposes;
- *Minimization*, i.e.,the data processed must be relevant, adequate and limited to what is necessary in view of the purposes for which they are processed;
- *Accuracy*, i.e., the data processed must be accurate and up-to-date regularly;
- *Retention*, i.e., the data must be deleted after a limited period;
- *Subject explicit consent*, i.e.,the data may be collected and processed only if the data subject gives his explicit consent.

To introduce the GDPR requirements in software business process modeling, an important step is to provide mechanisms to extend the existing models so as to expressed in legal provisions. Among the currently available proposals, in this paper we refer to [25, 14, 27] that provide mechanisms for manage content-oriented pattern and customized process views.

2.3 Access Control Systems

Access control system is a way to ensure that access to assets is authorized and restricted based on business and security requirements (ISO/IEC 27000,

2018[4]). *Access Control* ensures that only the intended people can access security-classified data and that these intended users are only given the level of access required to accomplish their tasks. It is also considered as a fundamental building block for secure information sharing [5]. Several access control models have been proposed, including models taking into account time, location, and situation [10, 24] and models specific for privacy-sensitive data [28].

An*access control mechanism* is defined as an access control system that provides a decision to an authorization request, typically based on predefined policies. Access control mechanisms are embedded in many different systems, ranging from operating systems to database management systems, and standards have been proposed [16]. Among them, here we refer to the Attribute-based Access Control (ABAC) model [16], which relies on the eXtensible Access Control Markup Language (XACML) [30] for specifying and enforcing *Access Control Policies*.

An *access control policy* is a specific statement of what is and is not allowed. Briefly, an XACML policy has a tree structure whose main elements are: PolicySet, Policy, Rule, Target and Condition. The PolicySet includes one or more policies. A Policy contains a Target and one or more rules. The Target specifies a set of constraints on attributes of a given request. The Rule specifies a Target and a Condition containing one or more boolean functions. If the Condition is evaluated to true, then the Rule's Effect (a value of Permit or Deny) is returned, otherwise a NotApplicable decision is formulated (Indeterminate is returned in case of errors). The PolicyCombiningAlgorithm and the RuleCombiningAlgorithm define how to combine the results from multiple policies and rules respectively in to derive a single access result. The anatomy of an access control policy and an access control request is sketched in Figure 1(a). While an example of an XACML policy is provided in Figure 6.

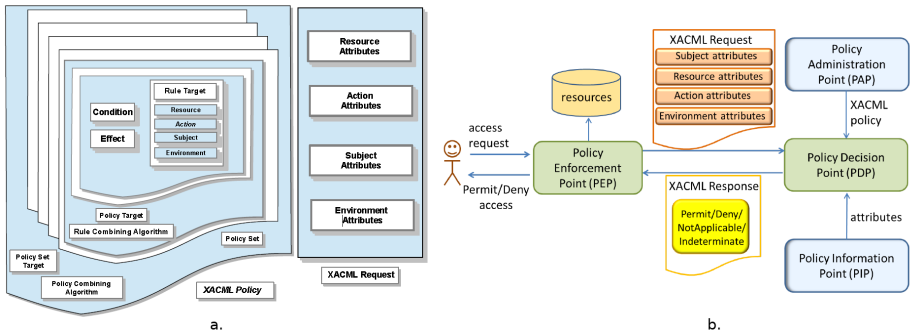

Fig. 1. a. XACML Policy and XACML Request - b. Access Control System Architecture

[4] https://www.iso.org/standard/73906.html

Concerning the architecture, the main components of an XACML-based access control system are shown in Figure 1(b). In particular, the Policy Administration Point (PAP) is the system entity in charge of managing the policies; the Policy Enforcement Point (PEP), usually embedded into an application system, receives the access request in its native format from the requester, constructs an XACML request and sends it to the Policy Decision Point (PDP); the Policy Information Point (PIP) provides the PDP with the values of subject, resource, action and environment attributes; the PDP evaluates the policy against the request and returns the response, including the authorization decision to the PEP.

3 Approach

There are different proposals addressing specific data protection principles by leveraging authorization systems (see for instance [33, 36]). However, currently only few are targeting the GDPR compliance problem and proposing access control systems as a key solution [4]. Indeed, as they are, the current access control mechanisms and techniques are not able to either satisfy the GDPR requirements or be easily integrated into the business process steps.

The proposal of this paper is to move a step ahead and provides a comprehensive methodology that combines, merges and integrates the access control system into the BP so as to address different aspects of the GDPR compliance problem. For aim of simplicity, here we restrict ourselves to the GDPR provisions directly related to access control mechanisms.

On the bases of the methodology presented in [7], the approach adopted in this paper, for integrating the access control systems into the business process activities, consists in the following steps:

Define the use case: i.e., analyze the business process activities, often expressed through an existing BPMN so as to establish a common basis to discuss with different stakeholders. The purpose here is to leverage the business process to be compliant with the GDPR implementation challenges.

Gather authorization requirements: i.e., gather all the authorization requirements and the sources they come from. In this case, authorization requirements will be expressed in terms of statements or natural language authorization policies. Additionally, business requirements (e.g. working hours) and security best practices (e.g. encrypting data) will be defined.

Identify required attributes: i.e., identify the BP model activities that can be affected by GDPR requirements. These will be extended/substituded with sub-processes compliant with the GDPR specifications so as to enforce the GDPR provisions and make easier requirement reviews. To make easier this step, a pre-defined set of sub-processes will be provided. Depending on the different (industrial) environments, the set will include specific activities necessary to allow the integration with access control systems.

Author the authorization policies: i.e., to transform the natural language statements into machine-interpretable statements, so as to eliminate any

ambiguity introduced by natural language. Thus, a list of XACML policies encoding the GDPR principle will be specified and the order in which those policies will be evaluated defined.

Test the policies: i.e., to ensure that the implemented XACML policy meets the GDPR requirements. For this, state-of-the-art testing techniques will be used or adapted according to specific exigencies.

Deploy the architecture: i.e., the definition on the contact point with existing systems (PEP). A specific PEP will be defined for each application that interacts with the authorization system. From the architectural point of view, the XACML reference architecture, depicted in Figure 1(b), can be easily integrated within existing Identity and Access Management (IAM) solutions. A common threat affecting the traditional IAMs is that they are mainly based on RBAC model where the user's access rights are directly assigned to the user by means of roles and permissions. RBAC model also provides coarse-grain access control, allowing security managers to implement broad changes. Differently, ABAC model adopts a more fine-grain access control, allowing to make authorization decisions that consider specific or even complex conditions. More precisely, by adopting ABAC model and in particular its XACML standard implementation, user's access rights are the result of a runtime authorization request evaluated against a set of policies [7]. The result of the evaluation of the authorization request is performed by the PDP in collaboration with different components that must be integrated and carefully tested.

Deploy the policies: i.e., deploying the authored XACML policies according to the selected (production) environment.

Run access reviews: an access review consists of an analysis of the policies against a set of attributes to determine what these attributes grant.

In the next section more details about the proposed approach will be provided through a simplified running example.

4 Application Example

In this section, we illustrate the proposed approach through a simple example relative to a standard process for service provisions by a specialist/professional. Thus, the use case considered is represented in Figure 2, where the basic activities have been shown by means of a generic Business Process Model (BPM).

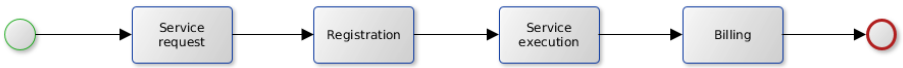

Fig. 2. Generic business process

As in the figure, the BPM has four main phases (activities):

- *Service request*, in which the *Customer* and professional (*Seller*) establish the first contact and agree about the provisioning of a service;
- *Registration*, in which, for starting the collaboration, the *Seller* collects the *Customer* data (if he/she has not been already registered for the same service);
- *Service execution*, during this activity the requested service is provided;
- *Billing*, in which the collaboration ends with the production of an invoice.

As described in Section 3, during the `Gathered authorization requirements` step, the GDPR requirements relative to the activities of the BP are explicitly listed. It is part of this stage the identification of the data types affected by privacy constraints, the primary purpose of data collection as well as the optional purposes that could involve the data management. Additionally, the activities related to collecting, reading, storing, transmitting, or deleting personal data that have to be compliant with the definition provided in GDPR Article 4(2) are also identified. In Figure 3(a) the simplified version of the consent request form is provided. As in the figure optional purposes can be also included, such as the usage of the customer's e-mail of physical address for sending: i) un-target news or advertisements (Newsletters); ii) specific target marketing based on the customer's history (Target Marketing).

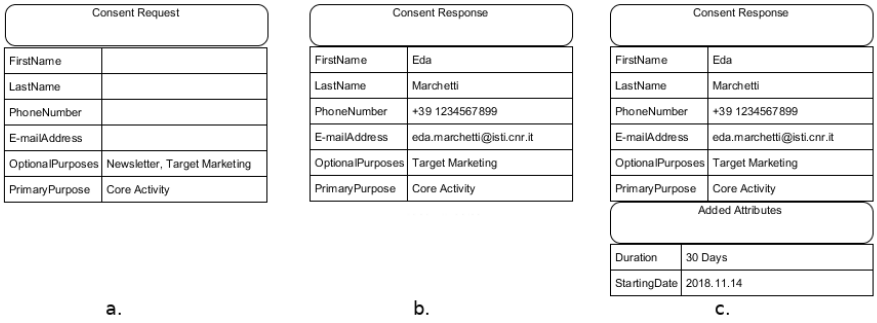

Fig. 3. a. Form request - b. Form response - c. Form response enriched

Afterward, during the `Identify required attributes` step, the activities affected by GDPR provisions are highlighted in the BP model. These will be substituted or extended by specific activities or sub-processes to guarantee the GDPR compliance. In the considered example, only the *Registration* activity has been highlighted as critical from the GDPR point of view (see Figure 4), and therefore, improved with a set of compliant GDPR sub-tasks as shown in 5.

In particular, Figure 5 details the new sub-process provided. Here, the *Customer* has been identified with the data subject and the *Seller* with the data controller.

In this sub-process, the *Seller* checks if the *Customer* has already provided consent to the required service. If not, the *Seller* prepares the *Consent request*

Fig. 4. Enhanced Business Process Model

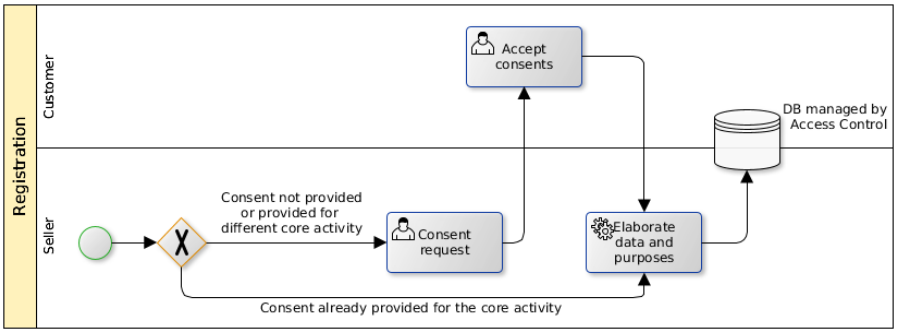

Fig. 5. Registration sub-process

according to the form shown in Figure 3(a) and sends it to the *Customer*. This last fills the form with required data (see Figure 3(b)) and sends it back to the *Seller*.

According to the approach proposed in 3, the task `Elaborate data and purposes`, in Figure 5, implements the steps from `Author the authorization policy` to `Deploy the policy`. It is in charge of converting the information collected into `XACML` policies/attributes encoding the GDPR principles and, setting up the access control mechanism in order to rule the data access though a common database.Figure 3(c) shows an abstraction of attribute considered for policy specification. As in the figure, two additional attributes (Duration and StartingDate) are included in order to satisfy Article 17 of GDPR.

Without going deeply into technical details, in order to integrate the GDPR principles and articles in the authorization systems different steps are necessary:

- *Formally express articles of the GDPR by means of formulas*: for this we rely on the Reified Input/Output (RIO) logic [38], which is a deontic logic suitable approach to express legal concepts recently embedded in the LegalRuleML [31].
- *Provide a formal extension of the XACML* language to explicitly manage GDPR principles of *consent* and *purpose limitation*. Management of obligations require specific solution, because they cannot be directly expressed as XACML rule. Indeed, XACML include the concept obligations, but with a different meaning of that associated to the GDPR: XACML obligations are treated mainly as black boxes, without specifying what an obligation should include and how it should be handled.

- *Transform the RIO/LegalRuleML rules into access control rules and policies* by using the extended XACML language. This will provide a set of predefined policy forms to be instantiated on demand according to different specific constraints. In particular, we considered the RIO/LegalRuleML rules that express provisions about the access, collection, blocking or transfer of personal data. A common terminology of actions (like read, write, update, delete) is adopted and refined using both the English version of the GDPR and, the guidelines provided by the European Data Protection Board and the previous Article 29 Working Party. Consequently, a set of notions (consent, purpose, data subject, controller, processor) are classified as building block of ABAC policies and translated into XACML meta policies.
- *Extend the existing access control architecture* with suitable mechanisms to assure a high presumption of compliance. This includes tools for authoring and enforcement of GDPR-based policies, and tools for collecting and managing information for compliance and audit purposes.

According to the `Test the policy` step, before deploy the XACML policy on the access control system, an accurate testing activity is also performed so as to avoid possible security or privacy flaws.

Figure 6 shows an extract of the policy derived using the data of Figure 3(c). The extended access control architecture will use the policy for ruling the access to the database so as to guarantee the online GDPR compliance.

`Policy`	root element rule-combining-algorithm:first-applicable permit-overrides
`Target`	Sample Policy rules the access to the attributes of the *Customer*.
`AnyOf`	Or Operator
`AllOf`	resource-attributes = {Eda, Marchetti, +39 1234567899, eda.marchetti@isti.cnr.it}
`Rule`	RuleId = rule1, Effect = Permit
`Target`	The *Seller* can perform any action for the *Core Activity* and / or *Target Marketing* purposes within 30 days starting from the *StartingDate*.
`AnyOf`	Or Operator
`AllOf`	PrimaryPurpose = Core Activity
`AllOf`	OptionalPurpose = Target Marketing
`Condition`	30 ≤ CurrentDate - StartingDate
`Rule`	default: deny all, which is not allowed explicitly. RuleId = rule2, Effect = Deny

Fig. 6. An XACML policy using the data of Figure 3(c).

5 Related Works

Due to the complexity and the importance of the GDPR application, in recent years a lot of attention has been devoted to the clarification of data protection principles, policies and regulations [22]. At the same time, many supporting tools and applications have been developed to assist users in producing reports on GDPR compliance [17].

Notwithstanding these important contributions, the integration of data protection rules into the commonly-used business processes is still an emerging challenge. In literature, a lot of attention has been devoted either to include generic privacy aspects into the adopted business process [29, 8, 39, 12] or to assess of privacy and security analyses in all stages of system development [1, 6, 40, 19] or to verify the GDPR provisions [4, 20, 13].

This highlights the need of a standard methodology to perform an assessment of IT systems concerning privacy and security aspects especially targeting the GDPR requirements. In line with this field, the proposal of this paper attempts to make easier the assessment of GDPR requirements, by explicitly integrating specified access control systems into the commonly adopted business process. In particular, the presented approach aims to integrate and extend the available proposals promoting business processes and access control systems as a key solution for privacy issues [21, 35, 2, 4].

For this purpose, an extension of the XACML reference architecture is promoted. In literature, there are several proposals aiming to satisfy the GDPR requirements through improvement of the reference XACML architecture. The main proposals are: [11] which focuses on authorization decision depending on the context as well as on the user's access privileges; [15] and [9] where authors designed a system that ensured the enforcement of multiple privacy policies within an organisation and throughout a distributed system; [34] which proposes a proof-of-concept implementation for the IoT environment where the security between the XACML reference architecture components was addressed; [34] where the proposed architecture is an integration oriented proposal aimed to make XACML easier to use by other systems. Differently from the provided solutions, our idea is to decouple the authorization functionalities from the business logic. This let to adapt and extend the XACML reference architecture with new features without modifying the business logic of the applications that use and consume Personal Data. Separation of concern from the architectural point of view should help one to propose scalable, manageable and extendible authorization solutions.

6 Conclusions

Since the GDPR was about to be finalized, theoretical research and industry have started addressing the issue of compliance with the new Regulation. The idea of having integrated solutions that supports compliance throughout the various stages of the software development life cycle of data processing applications is in

itself very simple, but its realization is far from that. This paper moved a step ahead in the direction of *protection by design* by improving the currently adopted security services and access control procedures. The target was to leverage them to the enforcement of GDPR requirements across the business activities related to data management and analysis.

From a technical point of view, the BPMN was selected as the target model to integrate in the business process the access control mechanism. Indeed BPMN is a simple yet effective means of modelling a flow of activities (both man-made and automated). Of course different modeling languages could have been considered. However, the proposal of this paper aimed to focus on the underlying idea than on the technical implementation details.

To exemplify the proposal presented herein, the basic steps of a feasible approach are provided. Moreover, an application example has been used to clarify the adoption of access control systems for protection of personal data during the BPMN modeling and execution.

As a future work, we plan to prototype the proposed approach including the features for: extending the BPMN, highlighting inconsistencies, and enforcing the GDPR concepts into the access control systems.

References

1. Amir Shayan Ahmadian, Daniel Strüber, Volker Riediger, and Jan Jürjens. Supporting privacy impact assessment by model-based privacy analysis. In *Proceedings of the The 33rd ACM/SIGAPP Symposium On Applied Computing (SAC)*. ACM, April 2018.
2. Khalid Alissa, Jason Reid, Ed Dawson, and Farzad Salim. Bp-xacml: An authorisation policy language for business processes. In *Information Security and Privacy: 20th Australasian Conference, ACISP 2015, Proceedings [Lecture Notes in Computer Science, Volume 9144]*, pages 307–325. Springer, 2015.
3. Cesare Bartolini, Antonello Calabró, and Eda Marchetti. Integrating gdpr in business process modeling. In *Technical Report*, 2018.
4. David Basin, Søren Debois, and Thomas Hildebrandt. On purpose and by necessity. In *Proceedings of the Twenty-Second International Conference on Financial Cryptography and Data Security (FC)*, February 2018.
5. Elisa Bertino, Gabriel Ghinita, and Ashish Kamra. Access control for databases: Concepts and systems. *Foundations and Trends in Databases*, 3(12):1–148, 2011.
6. Felix Bieker, Nicholas Martin, Michael Friedewald, and Marit Hansen. Data protection impact assessment. In *Privacy and Identity Management*, volume 526 of *IFIP Advances in Information and Communication Technology*, pages 207–220. Springer, 2018.
7. David Brossard, Gerry Gebel, and Mark Berg. 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, 2017. ACM.
8. Erik Buchmann and Jürgen Anke. Privacy patterns in business processes. In *Proceedings of the 47. Jahrestagung der Gesellschaft für Informatik (INFORMATIK)*, pages 793–798. Gesellschaft für Informatik, September 2017.

9. David W Chadwick and Kaniz Fatema. An advanced policy based authorisation infrastructure. In *Proceedings of the 5th ACM workshop on Digital identity management*, pages 81–84. ACM, 2009.
10. Maria Luisa Damiani, Elisa Bertino, Barbara Catania, and Paolo Perlasca. GEO-RBAC: A spatially aware RBAC. *ACM Trans. Inf. Syst. Secur.*, 10(1):2, 2007.
11. Maryam Davari and Elisa Bertino. Reactive access control systems. In *Proceedings of the 23Nd ACM on Symposium on Access Control Models and Technologies*, SACMAT '18, pages 205–207, New York, NY, USA, 2018. ACM.
12. Vasiliki Diamantopoulou, Nikolaos Argyropoulos, Christos Kalloniatis, and Stefanos Gritzalis. Supporting the design of privacy-aware business processes via privacy process patterns. In *Proceedings of the 11th International Conference on Research Challenges in Information Science (RCIS)*. IEEE, May 2017.
13. Bob Duncan. Can EU general data protection regulation compliance be achieved when using cloud computing? In *Proceedings of the Ninth International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING)*, pages 1–6. IARIA, February 2018.
14. Rik Eshuis and Paul W. P. J. Grefen. Constructing customized process views. *Data Knowl. Eng.*, 64(2):419–438, 2008.
15. Kaniz Fatema, David W. Chadwick, and Stijn Lievens. A multi-privacy policy enforcement system. In *Privacy and Identity Management for Life*, 2011.
16. David F. Ferraiolo, Ramaswamy Chandramouli, Rick Kuhn, and Vincent C. Hu. Extensible access control markup language (XACML) and next generation access control (NGAC). In *Proceedings of the 2016 ACM International Workshop on Attribute Based Access Control, ABAC@CODASPY 2016, New Orleans, Louisiana, USA, March 11, 2016*, pages 13–24. ACM, 2016.
17. Pietro Ferrara and Fausto Spoto. Static analysis for GDPR compliance. In *Proceedings of the Second Italian Conference on Cyber Security (ITASEC)*, February 2018.
18. Elena Fleacă, Bogdan Fleacă, and Sanda Maiduc. Process modeling as key technique for embedding the practices of business process management in organization. In *International Conference on Exploring Services Science*, pages 89–99. Springer, 2016.
19. António Gonçalves, Anacleto Correia, and Luis Cavique. Data protection risk modeling into business process analysis. In *Computational Science and Its Applications ICCSA 2017*, volume 10404 of *Lecture Notes in Computer Science*, pages 667–676. Springer, 2017.
20. Duarte Gonçalves-Ferreira, Mariana Leite, Cátia Santos-Pereira, Manuel E. Correia, Luis Antunes, and Ricardo Cruz-Correia. HS.Register. In *Building Continents of Knowledge in Oceans of Data*, volume 247 of *Studies in Health Technology and Informatics*, pages 81–85. IOS Press, 2018.
21. Emil Heuck, Thomas T Hildebrandt, Rasmus Kiærulff Lerche, Morten Marquard, Håkon Normann, Rasmus Iven Strømsted, and Barbara Weber. Digitalising the general data protection regulation with dynamic condition response graphs. In *Proceedings of the 15th International Conference on Business Process Management (BPM)*, pages 124–134, September 2017.
22. IT Governance Privacy Team. *EU General Data Protection Regulation (GDPR).* IT Governance Publishing, second edition, 2017.
23. John Jeston and Johan Nelis. *Business Process Management.* Routledge, 3rd edition, 2014.
24. A. S. M. Kayes, Jun Han, and Alan W. Colman. An ontological framework for situation-aware access control of software services. *Inf. Syst.*, 53:253–277, 2015.

25. Agnes Koschmider and Hajo A. Reijers. Improving the process of process modelling by the use of domain process patterns. *Enterprise IS*, 9(1):29–57, 2015.
26. Wadha Labda, Nikolay Mehandjiev, and Pedro Sampaio. Modeling of privacy-aware business processes in BPMN to protect personal data. In *Symposium on Applied Computing, SAC 2014, Gyeongju, Republic of Korea - March 24 - 28, 2014*, pages 1399–1405, 2014.
27. T. H. H. Nguyen, T. P. Hong, and N. Le Thanh. An ontological approach for organizing a knowledge base to share and reuse business workflow templates. In *2017 Seventh International Conference on Information Science and Technology (ICIST)*, pages 271–277, April 2017.
28. Qun Ni, Elisa Bertino, Jorge Lobo, Carolyn Brodie, Clare-Marie Karat, John Karat, and Alberto Trombetta. Privacy-aware role-based access control. *ACM Trans. Inf. Syst. Secur.*, 13(3):24:1–24:31, 2010.
29. Nicolás Notario, Eleonora Ciceri, Alberto Crespo, Eduardo González Real, Ilio Catallo, and Sauro Vicini. Orchestrating privacy enhancing technologies and services with BPM tools. In *Proceedings of the 12th International Conference on Availability, Reliability and Security (ARES)*. ACM, August–September 2017.
30. OASIS. 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, January 2013.
31. OASIS. LegalRuleML TC. https://www.oasis-open.org/committees/legalruleml, 2013.
32. Object Management Group. Business process model and notation, January 2011.
33. Harshvardhan J. Pandit, Kaniz Fatema, Declan O'Sullivan, and Dave Lewis. Gdprtext - gdpr as a linked data resource. In *The Semantic Web*, pages 481–495, Cham, 2018. Springer International Publishing.
34. Óscar Mortágua Pereira, Vedran Semenski, Diogo Domingues Regateiro, and Rui L. Aguiar. The XACML standard - addressing architectural and security aspects. In *IoTBDS*, pages 189–197. SciTePress, 2017.
35. Qusai Ramadan, Mattia Salnitriy, Daniel Strüber, Jan Jürjens, and Paolo Giorgini. From secure business process modeling to design-level security verification. In *Proceedings of the ACM/IEEE 20th International Conference on Model Driven Engineering Languages and Systems (MODELS)*, pages 123–133. IEEE, September 2017.
36. Silvio Ranise and Hari Siswantoro. Automated legal compliance checking by security policy analysis. In *Computer Safety, Reliability, and Security*, 2017.
37. Jan Recker. Opportunities and constraints. *Business Process Management Journal*, 16(1):181–201, 2010.
38. L. Robaldo and X. Sun. Reified input/output logic: Combining input/output logic and reification to represent norms coming from existing legislation. In *The Journal of Logic and Computation*, 2017.
39. Ana Sokolovska and Ljupco Kocarev. Integrating technical and legal concepts of privacy. *IEEE Access*, 6:26543–26557, May 2018.
40. Uros Stevanovic, David Groep, Ian Neilson, Stefan Paetow, and Wolfgang Pempe. Data protection impact assessment-an initial guide for communities, April 2018.
41. Sören Witt, Sven Feja, Andreas Speck, and Christian Prietz. Integrated privacy modeling and validation for business process models. In *Proceedings of the 2012 Joint EDBT/ICDT Workshops, Berlin, Germany, March 30, 2012*, pages 196–205, 2012.