A Hybrid Compliance Checking Approach: Law Meets Process Domain

Juanita Caballero-Villalobos[1]

[1]Technical University of Denmark, Richard Petersens Plads, 321, 2800 Kgs. Lyngby, DK

Abstract

Integrating compliance checking with business processes has become increasingly essential to ensure adherence to regulatory standards from both the process and legal domains. However, compliance officers and process modelers face significant challenges in eliciting regulatory requirements, integrating them into business process models, and understanding their outcomes. Therefore, this PhD aims to reconcile their needs while increasing transparency and understandability of the digitalization of regulatory requirements such as the General Data Protection Regulation (GDPR). The expected key contributions are: 1) Develop a formal framework to unify the terminology to extract and model compliance and normative feasibility of digitalization, 2) Provide formal methods and techniques to offer a global compliance perspective and increase the expressiveness of business process model languages to support normative requirements and their effects, 3) Develop understandable compliance checking outcomes.

Keywords

Compliance Checking, Conformance Checking, Requirements engineering, Declarative Languages, Visual Analytics

1. Introduction

Compliance checking allows organizations to review and analyze the levels of adherence to organizational processes and their outcomes with regulatory documents. This minimizes the risk of non-compliance, avoiding potential financial and trust-related losses. Typically, compliance checking involves the specification/extraction of engineering requirements, business process model design, definitions of compliance checks, choice of a compliance strategy[1] and the analysis of the outcomes [1]. Stakeholders from the legal and process domains are involved in each. Indeed, compliance officers and process modelers have different objectives that might cause conflicts and ambiguities. Traditionally, compliance-checking approaches have been developed to help process modelers [2, 3, 4] and treat the needs of compliance officers isolated. Therefore, offering a unified approach between the needs of compliance officers and process modelers could offer unexplored benefits in terms of transparency, understandability, and traceability of business process compliance.

From the compliance perspective, there are four key concepts: *regulatory requirements*, as external rules to comply with (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), and EU AI Act), *compliance requirements* [5], as the organizational objectives to ensure adherence to regulatory requirements (e.g., company policies, best practices, industry thresholds), *normative requirements* [6], as actionable events derived from regulatory requirements (e.g., a data collection form that displays the necessary information before the data is collected.) and *normative effects*[6], the impact of applying the law (e.g., obligations, prohibitions, permissions, compensations and violations). The legal jargon, process specifications, inherent complexity, and variability make it challenging to ensure compliance with business processes.

ICPM 2024 Doctoral Consortium, October 14–18, 2024, Kongens Lyngby
jcavi@dtu.dk (J. Caballero-Villalobos)
0000-0002-4915-0961 (J. Caballero-Villalobos)

[1]Compliance strategies might be included design-time controls, ensuring compliance by design from early stages; run-time, when processes are being executed; audits, post-mortem analysis of the logs; or hybrid approaches, which ensuring monitoring while offering significant flexibility to domain-specific applications, e.g., extensions of business process model languages with goal-oriented languages or embedding normative requirements into business language semantics

Compliance requirements have been extracted using conceptual models, taxonomies, and ontologies described in [1, 5]. However, these approaches mainly focus on representing hierarchical, dependency, temporal, and meronymic relationships without involving normative effects (e.g., obligations based on cross-references (e.g., recitals)) and do not provide a unified terminology to be used during the extraction and further formalization of the business process models. This results in misunderstandings and ambiguities when interpreting business compliance languages. Since there is no traceability of all the elements of the process that contribute to the interpretation and/or evaluation of the law in a given instance, the effectiveness of the compliance checking process is compromised. To address this, existing approaches have proposed enriching the business process language expressiveness [7, 8] by enforcing normative requirements into business process models, making the traceability from design to post-execution analysis. However, as complex regulatory requirements become embedded into business processes, model languages are highly demanding, given that compliance rules have high variability and unpredictability.

After the design phase, model-checking techniques are applied to verify that the model represents the extracted requirements; industries must define their compliance strategy, mechanisms, and measures to ensure compliance. One of the techniques that have been used to assure adherence to regulations is conformance checking [2], which usually provides support to binary compliance decision Yes/No, but does not offer a global perspective (e.g., answering questions, How far are they from achieving their goals? How satisfied/fulfilled are they with their goal?) and computation of the normative effects (e.g., the impact of compensations, punishments, or implications of cross-reference statements). Furthermore, the outcomes provided by some of the compliance-checking techniques (e.g., conformance checking, process discovery, logic-based properties verification) have not received extensive attention within the research community to date [9]. On the one hand, compliance officers have been encouraged to interpret the outcomes with external tools like Disco[2] and to make their own compliance reports. On the other hand, process modelers have traditionally visualized 2D process representations, which often struggle in analyzing complex relations, dynamic constraints, and event dependencies, generating that messages are misunderstood in comparison to semantic models [10, 11].

Our motivation comes from the challenges identified in digitalizing compliance and normative requirements and their effects. We envision a unified approach supporting the compliance checking process for legal and process domains. This project considers the following research questions (RQ):

- RQ.1: How can compliance officers and process modelers be supported to elicit and categorize compliance and normative requirements and their effects from the regulations?
- RQ.2: How can process modelers be supported in integrating compliance and normative requirements and their effects into business process models?
- RQ.3: How can compliance officers and process modelers be supported in understanding the outcomes of compliance-checking?

2. A Hybrid Approach to Compliance Checking: The Case of GDPR

This research has as a main objective to increase the transparency[3] and understandability[4] of compliance checking, by providing a framework of specification, modeling, verification and visualization of business processes compliance. As running examples (GDR RunE), we will use some of the articles in Chapter 3.[5] of the General Data Protection Regulation, Rights of the Data Subject. At a minimum, we anticipate the framework encompassing the methods and tools described below. As we are in an early stage of the research, some limitations of the methods and discussion of the results are not currently considered.

[2]https://fluxicon.com/disco/

[3]Ability to represent and infer relevant inherent information and behaviors in the compliance-checking decision-making process that are not currently captured by business process model language expressiveness.

[4]Facilitate the interpretation of the compliance-checking outcomes, making it reliable for analysis in different levels of abstraction and easy to integrate with the systems of the organization.

[5]https://gdpr-info.eu/chapter-3/

2.1. RQ.1 Norms extraction and elicitation

To support the formalization and extraction of feasible[6] normative and compliance requirements, we will develop a conceptual model for integrating and aligning run-time compliance checks within compliance processes. The main outcome will be a conceptual model to categorize, identify, and align compliance and normative requirements of a GDR RunE.

Completed and current work: We mapped the compliance and normative requirements of articles 13, 14, 32, and 5 of GDPR to evaluate the feasibility of automation of these requirements. Later, we discussed our results with compliance officers and refined our models and interpretation of inherent ambiguities. As a result, we propose a first mapping of substantive and procedural elements of the article and their corresponding normative and compliance requirements. Some of them are feasible to map as workflow and temporal constraints. Meanwhile, legal dependencies, normative effects, and annotations to avoid ambiguous interpretation are not explicit in most business process models, making its traceability difficult. Currently, we are working on validating and adjusting our definitions with lawyers.

Next Steps: We will establish the deontic effects (antecedent-consequence, classes, and relationships) of cross-reference elements (e.g., recitals, internal reference to another provision of the regulation). Then, we will align legal jargon with formalization terms and categories by providing a unified representation of the feasible normative and compliance requirements for later formalization. Automating the requirements extraction with techniques such as natural language processing is not currently considered at this stage.

2.2. RQ.2 Integrating rules with processes

To model compliance processes, mainly imperative business process model languages have been used [4]. Nevertheless, the dynamic nature and context-dependency of domains such as health care and law may be especially suited for declarative techniques [3]. As part of our initial approach, we chose Dynamic Condition Response (DCR) Graphs as a declarative language for modeling compliance processes. We aim to integrate the compliance and normative requirements identified by the foresaw framework into a business process model language. We will adopt a compliance strategy hybrid [1] integrating elements of design-time, run-time, and goal-oriented languages. The primary outcomes will be focused on the formal extension of **GoalsDCR** ; we will introduce the monitoring semantics of the integration of compliance requirements into DCR semantics and an algorithm to evaluate after the execution of an event *How far is the organization from meeting a compliance goal?*. Later, we will develop a second version of Goals+RegDCR, the formalization of compliance and normative requirements, that is adaptable to both compliance by design and run-time execution. We expected to develop an algorithm to compute the normative effects (e.g., compensation, punishments) in the cross-reference relationships and the global compliance checking.

Completed and current work: We modeled the GDPR articles explored in RQ.1 in Dynamic Condition Response Graphs 2D Simulator[7] as an initial approach to evaluate the capacity to represent compliance, normative requirements from regulations, and their effects. The preliminary results indicate that a global compliance perspective and some normative requirements and their effects are currently not supported by the semantics, which makes its traceability difficult. To tackle that, we formalized compliance requirements as goals based on intentional elements of i* framework (e.g., goals, links). To do so, we identified the compliance requirements of article 13. of GDPR, "Information to be provided where personal data are collected from the data subject," and mapped them into intentional elements[8]

[6] A normative or compliance requirement that can be automatically or semi-automatically enforced or monitored by a compliance strategy without human judgment. We infer that a feasible requirement must be precise, measurable, and automatable (e.g., provision of information to data subjects during data collection).

[7] https://www.dcrgraphs.net/

[8] As an example, we define a top-goal of transparency. This ensures that one knows how one's data is collected, utilized, and managed. This main goal could be decomposed into sub-goals, such as ensuring transparency in data collection, accountability in data handling, a legal basis for data processing, compliance with cross-references, and so forth. The relationships between

For our extension, a **goal** represents the rationale and motivations underlying complying with a business compliance requirement, the "why." It can be decomposed into relevant domain-specific sub-goals. The fulfillment satisfaction of the goals is defined as executing a subset of normative requirements. The latter represents what the law should do, the "how." We modeled it using the dynamic condition response graphs semantics elements[9]. As a result, we differentiate goals from the events given their objectives, decomposition, and strengths[10]. Currently, we are focusing on formalizing our previous definitions, encoding the goals into BNF notation, and performing formal evaluations of the expressiveness of DCR semantics [12] based on its capacity to represent the requirements extracted.

Next Steps: We will integrate the goals into the DCR semantics by developing a feasibility check function to determine whether a goal is achievable and assess the current marking (trace) and the latest event executed. Then, we will introduce an algorithm based on the evaluation measures proposed in the compliance Requirements Framework to compute the satisfaction degree (compliance goal fulfillment) of high-level intentional elements. This will support the non-binary (Yes/No) decision-making process, measuring the extent to which the method is compliant based on the compliance checks defined in the previous phase. Later, we will extend our last semantics, incorporating normative requirements using regular grammar, and we will develop an algorithm to compute the effects of the normative requirements (e.g., compensation). Both extensions will validated as described in [13], mapping it to a Büchi automaton; we will use model-checking tools to prove the safety and liveness properties and the correctness of both extensions. Moreover, we will validate our approach to ensure compliance with an article on GDPR as a running example, using conformance checking as a primary technique.

2.3. RQ.3 Understandability and Generalisability

Consequently, after validating our formal approaches, we would like to offer understandable outcomes for users in the legal and process domains. We infer that graphical representations that refer a modelling pattern make easier to understand the process, dependencies and their relationships. However, we need to determine i) what are the key elements that play a differential role in the interpretation and understandability of compliance checking outcomes, and ii) what type of representations are considered helpful for the end users. The primary outcome of this phase will be to explore, create, or extend 2D and 3D artifacts to simulate the process and show the outcomes of the process understandably.

Completed and current work: We extended the 3D DCR Simulator [11] with some of the features that we infer increase the understandability of compliance checking outcomes. By including real-time logs annotations with integrations to real-time analysis using SQL Queries in Unity Cloud and integration of post-mortem analysis with process mining tools such as Disco. The tool contributes to two use cases in compliance checking: **elicitation and discovery of process variants** using unrestricted process models and **simulations of process models**. Currently, we are working to extend the support of these immersive representations.

Next Steps: We will conduct empirical studies with end users of the compliance checking process from both legal and process domains to determine the elements and environments (e.g., 2D, 3D) that make relevant, useful, and understandable the process outcomes. As an initial approach, we will extend the 2D DCR Simulator (e.g., adding new SVG visualizations to reflect the semantics extensions proposed in the previous phase) and 3D DCR Simulator (e.g., adding computer aid design models to tailored

these goals could be expressed with intentional relationships and goal dependency.

[9] Taking the sub-goal "ensuring accountability in data handling". We define at least the normative requirements of tracking all interactions with personal data, granting data subjects access to their data upon request, and timely notifying authorities and data subjects of any personal data breaches. We used the DCR semantics to represent the specific, measurable GDPR events and their inherent relationships.

[10] While goals focus on a high level of compliance-checking, the DCR events focus on workflow controls. Moreover, the first one allows one to decompose compliance requirements into measurable sub-goals, while the DCR elements representing normative requirements, including events, are modeled as normative triggers. Finally, goals bring a global compliance perspective that is useful for strategic planning. Meanwhile, DCR elements (including events) effectively ensure operational compliance.

[11] https://bit.ly/sourcecode3DCRBeta

domain-specific representations) by mapping the requirements extracted in the empirical studies. Then, we will conduct a second phase of empirical studies to compare the cognitive load between both representations and validate the effectiveness of our developments.

3. Acknowledgments

I thank my PhD supervisors, Hugo-Andrés López-Acosta and Andrea Burattin, and DICE members Olga Kokoulina and Alexandra Andhov for their guidance and support. This work is supported by the research grant “Center for Digital ComplianceE (DICE)” (VIL57420) from VILLUM FONDEN. Moreover, it is part of a EuroTech Alliance project entitled "Explainable Compliant Process-driven Platforms", a joint work with the Technical University of Eindhoven.

References

[1] M. Hashmi, G. Governatori, H.-P. Lam, M. T. Wynn, Are we done with business process compliance: state of the art and challenges ahead, Knowledge and Information Systems (2018).

[2] F. Caron, J. Vanthienen, B. Baesens, Comprehensive rule-based compliance checking and risk management with process mining, Decision Support Systems (2013).

[3] M. Elhagaly, K. Drvoderić, R. G. Kippers, F. A. Bukhsh, Evolution of compliance checking in process mining discipline, in: 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), 2019, pp. 1–6.

[4] F. Klessascheck, T. Knoche, L. Pufahl, Reviewing conformance checking uses for run-time regulatory compliance, in: Enterprise, Business-Process and Information Systems Modeling, Springer Nature Switzerland, 2024, pp. 100–113.

[5] A. M. Mustapha, O. T. Arogundade, S. Misra, R. Damasevicius, R. Maskeliunas, A systematic literature review on compliance requirements management of business processes, International Journal of System Assurance Engineering and Management 11 (2020) 561–576.

[6] M. Hashmi, G. Governatori, M. T. Wynn, Normative requirements for business process compliance, in: Service Research and Innovation, Springer International Publishing, 2014, pp. 100–116.

[7] A. Elgammal, O. Turetken, W.-J. van den Heuvel, M. Papazoglou, Formalizing and applying compliance patterns for business process compliance, Software & Systems Modeling (2016).

[8] A. Zasada, M. Hashmi, M. Fellmann, D. Knuplesch, Evaluation of compliance rule languages for modelling regulatory compliance requirements, Software 2 (2023) 71–120.

[9] J.-R. Rehse, L. Pufahl, M. Grohs, L.-M. Klein, Process mining meets visual analytics: The case of conformance checking, in: Proceedings of the 2023 ACM Symposium on Applied Computing (SAC), ACM, 2023, pp. 5452–5461.

[10] K. Figl, C. Di Ciccio, H. A. Reijers, Do declarative process models help to reduce cognitive biases related to business rules?, in: International Conference on Conceptual Modeling, Springer, 2020, pp. 119–133.

[11] S. Jensen, H.-A. López-Acosta, Towards immersive environments for declarative process models, in: Proceedings of The 22nd International Conference on Business Process Management 2024, 2024, pp. 214–231.

[12] S. Debois, T. T. Hildebrandt, T. Slaats, Replication, refinement & reachability: complexity in dynamic condition-response graphs, Acta Informatica 55 (2018) 489–520.

[13] T. T. Hildebrandt, R. R. Mukkamala, Declarative event-based workflow as distributed dynamic condition response graphs, in: Declarative Event-Based Workflow as Distributed Dynamic Condition Response Graphs, 2010, pp. 59–73.