Making Business Processes Law Compliant

Sepideh Ghanavati[1], Daniel Amyot[1], Alberto Siena[2], Angelo Susi[2], and Anna Perini[2]

[1] School of Information Technology and Engineering (SITE)
University of Ottawa
800 King Edward Avenue, Ottawa, Canada
[2] Fondazione Bruno Kessler
FBK - Irst
Via Sommarive 18, 38050 Povo, Trento, Italy

Abstract. This paper introduces a problem of law compliance that arises during the requirements engineering (RE) phase of software systems. High-level law prescriptions often have a pervasive impact on business processes, the system they have to support, and consequently on the functionalities of the system itself. However, it is not easy to verify that business processes, which are very detailed and domain-dependent, actually comply with abstract, domain-independent legal prescriptions. We propose the use of RE languages combined in a framework to compare these two levels and make conclusions about compliance.

1 Introduction

Business processes compliance to laws has become a very important issue for most organizations and software developers. Violations to regulations can lead to great financial penalties and loss of organizational reputation. However, managing compliance can be very demanding and complicated. Legal prescriptions can be categorized in three types [1, 2]: constitutive laws provide a propositional definition of things being regulated; procedural laws consist in collections of propositions in natural language that describe the sequences of actions forming a procedure; and regulative (or requirements-level) laws consist in collections of propositions (permissions, obligations and prohibitions) in natural language that define the states of affairs (desired by the legislator). Regulative laws aim to cover a wide range of cases, and for this reason they cannot simply be applied, i.e., they need to be elaborated and often operationalized in order to be incorporated into business processes.

As a result, requirements for business processes have to be properly engineered with respect to the applicable laws. On the other hand, business processes contain the activities which exist for the purpose of compliance and activities which exist for performing the process and satisfying business objectives. Both types of activities need to be compliant with the law and it is important to verify the compliance of the latter kind with respect to the first. This is what we call compliance of business processes to legal prescriptions.

2 Background

Much research has been done on compliance assessment against legal documents. In requirements engineering (RE), four main approaches have been proposed. The first one concerns the analysis of legal text and extraction of legal requirements from the text. For instance, Breaux *et al.* [3] introduced a systematic approach to extract legal rights in terms of permissions, obligations and constraints from the text whereas Maxwell and Antón [4] use production rules to model regulations and extract legal elements in terms of eight Hohfeldian classes of legal rights. These production rules help query the regulation model, find instances of non-compliance, and derive new legal requirements.

The second type of contribution in RE deals with modeling legal documents with goal-oriented requirements engineering (GORE) techniques. These approaches are mainly based on common characteristics between regulations and requirements. For instance, Ghanavati *et al.* [5] developed a requirements management framework that integrates legal and organizational models with the same notation, namely the User requirements Notation (URN) standard [6], to establish compliance and manage change. This framework combines goal models (built with URN's Goal-oriented Requirement Language – GRL) and business process models (built with URN's Use Case Map scenario notation – UCM) and includes three layers (source documents, goal models and business process models) connected by a set of traceability links. This framework does not provide guidelines on how to extract legal elements and build these layers. Darimont and Lemoine [7] applied the KAOS methodology to model legal objectives extracted from legal documents. Rifaut and Dubois [8] developed a framework based on the *i** goal modeling notation [9] to capture legal requirements and analyze business process compliance with respect to related published regulations.

Another type of research deals with compliance of business processes with business contracts and laws. Governatori *et al.* [10] use a logic-based formalism (FCL) based on deontic logic to model business contracts. To ensure compliance, the authors first model business processes with BPMN, then transform them into a group of event patterns aligned with FCL, and finally compare them with the FCL models of the business contracts.

Finally, the last type of research focuses on formal modeling notations. In this area, Siena *et al.* [11] introduced a modeling framework called *Nòmos*, which adds the eight Hohfeldian classes of legal rights (i.e., duty, privileges, claim, no-claim, power, immunity, liability and disability) as extensions to *i**. The framework is comprised of a modeling language and a methodology. With the help of *Nòmos*, legal and goal elements are modeled with a common notation and it is possible to extract a set of law-compliant requirements. This work, however, does not take into consideration the effect of a law model on applicable business processes.

3 Proposed Framework

Regulations have a more prescriptive nature than a detailed and operational one. In other words, regulations tell an organization to perform an activity at an

abstract level but they seldom tell how to achieve this activity specifically. On the other hand, business processes deal with very detailed activities. Hence, each high-level activity needs to be refined into detailed tasks and steps for business processes to perform correctly while remaining compliant with the normative propositions mentioned in the regulations. Therefore, even though regulation definitions may be very clear, an important challenge consists in bridging the gap between the abstract level prescriptions in the regulations and the concrete task level in the business processes. For example, Article 164.502 of the U.S. Health Insurance Portability and Accountability Act (HIPAA) states: *A covered entity (CE) is required to disclose protected health information (PHI): (i) To an individual, when requested under, and required by Sec. 164.524 or Sec. 164.528.* Such individual is usually a patient, and a CE can be en entity like a hospital. In this example, the abstract action is to disclose PHI to the individual, but it does not specify how or what process has to be followed to disclose this PHI. In order to reach the concrete task level, it is necessary to define the purpose of this disclosure based on the organizational and legal goals and refine them until we get sufficiently detailed tasks.

To perform such refinement in context, we propose a four-layer compliance framework. This framework takes advantage of both *Nòmos* and the requirements management framework developed by Ghanavati et al. by combining them into a single framework. The main contribution of this framework is that it provides templates for the business processes based on the Hohfeldian concepts of rights.

The first and topmost layer contains the source legal documents providing the prescriptive actions. The second layer consists of a formal *Nòmos* model of the law. This model captures the prescriptions found in the first layer using the Hohfeldian classes of legal rights. The elements of this layer are connected to their corresponding statements in the first layer. In *Nòmos*, the eight classes of rights are grouped into four categories: duty-claim, privilege-noclaim, power-liability, and immunity-disability. Each of these groups imposes a set of patterns on the business processes of the organization. For instance, if the *Nòmos* model contains an element of type duty-claim, then an activity that helps achieve this duty has to exist in the business process. In our example involving Article 164.502, the duty of the CE is to disclose PHI to individuals when it is requested. This duty has to be present in the business process as shown in the URN/UCM in Figure 1. The third layer is a strategic-legal goal model in URN/GRL. The main role of this layer is to analyze the *purpose* of normative elements in the *Nòmos* model and refine/decompose them until tasks are reached. In addition to the legal goals, the strategic goals of the organization and of other stakeholders are modeled and refined in this layer, to provide a more complete view of the context. This layer makes it possible to analyze the degree of compliance of business processes, to identify missing elements, and to document the rationale for the elements of the business processes. The fourth and bottom layer consists of the business process models in the URN/UCM notation. These models include the tasks found in the third layer and the other activities needed to perform the process.

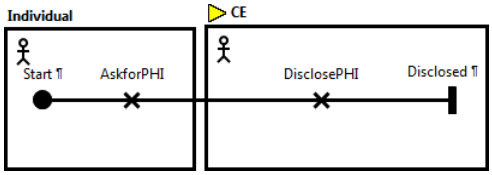

Fig. 1. Duty-Claim business process model.

The activities in the URN/UCM processes have links to their corresponding task in the URN/GRL strategic-legal goal model layer, hence documenting their rationale. Traceability links between each pair of adjacent layers help support impact and compliance analysis.

By defining *business process templates* for each class of legal right, it is possible to reason in operational terms about the constraints that laws impose on the business processes, but also about opportunities that laws offer (e.g., when being compliant becomes a competitive advantage). Such templates can be modeled with URN/UCM (see Figure 1), reusable in and verifiable against business processes in the fourth layer. Also, the strategic-legal goal model layer plays a crucial role in this framework. In addition to filling the gap between high-level legal models and low-level business process models, goal models can help identifying non-compliant instances. With the help of goal satisfaction algorithms inspired from URN's [6], it becomes possible to perform what-if analysis for non-compliant instances and to prioritize their resolution based on the organization's context. Goal models can also help analysts to understand how close or far the organization is from full compliance, and the cost of getting there.

4 Discussion and Future work

This framework aims to help organization provide law-compliant business processes. The proposed four layers support the transition from very abstract legal prescriptions to concrete business activities while promoting and documenting compliance. Modeling mistakes or wrong decisions are however always possible, so how to ensure that the developed models match the legal prescriptions remain an important problem. The traceability links between the different layers of the framework help document the rationale and enable completeness and consistency analysis, but they do not eliminate the need for human intervention. Nevertheless, these traceability links help maintaining compliance as laws and business processes evolve.

Our framework builds on previous work done by Siena [11, 12] and Ghanavati [5]. So far, we have worked with several HIPAA articles, modeled them with *Nòmos* and UCM/GRL, and built URN/UCM templates for the business processes based on the groups of legal rights discussed earlier. However, it is necessary to extend the case study to all sections of HIPAA so that we can pro-

vide a more complete set of guidelines for this particular law. This will also help answer the following questions in the future:

- What is the legal scope that needs to be covered for each business process?
- How to deal with the parts of the business process that are not directly extracted from the law? How to ensure those parts will not contradict legal prescriptions?
- How to produce process templates that are truly reusable and verifiable?
- How to scale this approach to more than one law, especially when conflicting?

References

1. C. Biagioli, D. Grossi, *Formal Aspects of Legislative Meta-Drafting*, 2008 conference on Legal Knowledge and Information Systems, Netherlands, pp. 192–201, 2008.
2. G. Boella and L. van der Torre, *Substantive and Procedural Norms in Normative Multiagent Systems*, Journal of Applied Logic, pp. 152–171, 2008.
3. T.D. Breaux, M.V. Vail, A.I. Antón, *Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations*, 14th IEEE Int. Requirements Engineering Conf. (RE'06), IEEE CS, pp.49–58, 2006.
4. J.C. Maxwell, A.I. Antón, *Developing Production Rule Models to Aid in Acquiring Requirements from Legal Texts*, 17th IEEE Intl. Requirements Engineering Conf. (RE'09), IEEE CS, pp. 101–110, 2009.
5. S. Ghanavati, D. Amyot, L. Peyton, *Towards a Framework for Tracking Legal Compliance in Healthcare*, 19th Int. Conf. on Advanced Information Systems Engineering (CAiSE'07), LNCS 4495, Springer, pp. 218–232, 2007.
6. ITU-T, *Recommendation Z.151 (11/08): User Requirements Notation (URN) – Language Definition*, Geneva, Switzerland, 2008.
7. R. Darimont, M. Lemoine, *Goal-oriented analysis of regulations*, Int. Workshop on Regulations Modelling and their Verification & Validation (REMO'06:), Luxemburg, pp. 838–844, 2006.
8. A. Rifaut, E. Dubois, *Using Goal-Oriented Requirements Engineering for Improving the Quality of ISO/IEC 15504 based Compliance Assessment Frameworks*, 16th IEEE Int. Requirements Engineering Conf. (RE'08), IEEE CS, pp. 33–42, 2008.
9. E. Yu, *Modelling Strategic Relationships for Process Reengineering*, Ph.D. dissertation, University of Toronto, Canada, 1996.
10. G. Governatori, Z. Milosevic, S. Sadiq, *Compliance checking between business processes and business contracts*, Proc. of 10th IEEE Conference on Enterprise Distributed Object Computing (EDOC'06), IEEE CS, pp. 16–20, Oct 2006.
11. A. Siena, J. Mylopoulos, A. Perini, A. Susi. *Designing Law-Compliant Software Requirements*, 28th Int. Conf. on Conceptual Modeling (ER'09), LNCS 5829, Springer, pp. 472–486, 2009.
12. A. Siena, J. Mylopoulos, A. Perini, A. Susi. *Towards a Framework for Law-Compliant Software Requirements*, ICSE Companion 2009, NIER track, IEEE, pp. 251–254, 2009.