Impact of Legal Interpretation on Business Process Compliance

Sepideh Ghanavati∗ and Joris Hulstijn†
∗Luxembourg Institute of Science and Technology, Luxembourg,
Email: sepideh.ghanavati@list.lu
†Delft University of Technology, Netherlands
Email: j.hulstijn@tudelft.nl

Abstract—Regulations are often written as open norms. Thus, the development of systems that support compliance involves interpretation. Often, compliance officers consider several alternative solutions. Comparing the feasibility and deciding which alternative to select are important tasks. In this paper, we aim to show how analyzing the impact of several interpretation can be supported by requirements engineering tools, in particular, by LEGAL-URN. Two cases are used to illustrate the importance of interpretation and how LEGAL-URN facilitates it.

I. INTRODUCTION

Organizations need to ensure that they are compliant with a large number of relevant regulations. Therefore from the beginning, business processes and information systems must be developed in such a way that they are compliant and that they inspire compliant behavior. Laws and regulations tend to cover many aspects at once and thus, they are complex and relatively abstract. As Massey et al. [21] mention, just like other natural language documents, legal texts are ambiguous and sometimes they need interpretation. Often there are many legal sources, which may even conflict (EU directives; national legislation; sector specific implementation guidelines; professional standards, company policies). In addition, regulations generally do not propose implementation details [3]. They are meant to be generic and are formulated as open norms. It is the duty of the company to interpret the regulations and implement business processes and software applications. Regulators will then assess to what extend these implementations are compliant. Due to strategic objectives or the high cost of implementation, sometimes organizations decide to comply with the weakest interpretation and accept the consequences.

Furthermore, the cost of non-compliance can be very high. For example, in 2012, Google received a charge of 22.5 million USD as civil penalty [10] from the Federal Trade Commission (FTC). In France, Google got a fine of 150,000 EUR [22]. To avoid the high-level costs of non-compliance and to help organizations and software companies to document different legal interpretations (i.e. alternatives) and to help performing a trade-off analysis between organizational high-level goals and legal alternative requirements, we propose to exploit LEGAL-URN [12] [14] framework.

A recent interview with two compliance specialists1, confirmed that interpretation is their daily business. Projects to implement legal changes may take several years of debate and discussion with all the stakeholders involved, before reaching consensus. Often, several alternative interpretations are considered in parallel. Comparisons between alternatives are made based on various characteristics (legal aspects, costs, IT requirements, and alignment with business strategy).

Yet, according to these specialists, there are few tools and techniques to support this decision making process. Mostly, existing tools focus on business process management. They help to locate legal requirements in processes. But no tools support strategic decision making about compliance.

The remainder of the paper is structured as follows. Section II provides some background on legal interpretation. Section III presents our framework. Section IV describes two cases to illustrate the usefulness and adequacy of the approach. The paper ends with a discussion of the limitations of the research set-up and ideas for future research.

II. LEGAL INTERPRETATION

The implicit view in much research on compliance management and conformance testing [16], treats legal interpretation as a linear process. Typically, there is only one legal source, a text, which is considered to be decisive. This text translates into a set of legal requirements. Specifications of business processes and information systems are then tested against these requirements to determine conformance. Boella et al. [3] argue that this linear picture does not fit reality. In practice, there are many legal sources, of different status. Legal sources may conflict, and often also conflict with business objectives, to develop new products or reduce costs. As laws try to be generic, many clauses are deliberately written as open norms; they have to be made specific for each individual context. Therefore, often various alternative interpretations of the key concepts are being debated. Black [2] calls such debates regulatory conversations. For this reason, we focus on developing software to support human experts in making compliance related decisions: legal knowledge management.

There are essentially two steps involved: interpretation and implementation (Figure 1). That means that we need an intermediate level of representation of legal requirements, sometimes called prescriptions [3], in between the legal sources and

1A legal consultant for government parties in the Netherlands, and a security officer and compliance expert at a commercial bank.
the finalized process or system specifications. These representations can be in formal logic or semi-formal textual format. What is crucial is that the legal knowledge management tool will allow the compliance officer to perform several kinds of reasoning tasks: searching relevant prescriptions, mapping prescriptions to parts of the processes, comparing alternative solutions, determining properties of solutions like feasibility, costs and dependencies, tracking changes, etc. These tasks are essential to requirements engineering.

Many tools and techniques exist to support legal requirements engineering, see [28], [6], [25]. However, none have explicitly taken alternative interpretations into account. How easily can existing techniques be adapted to support interpretation and comparisons?

An important topic in Requirements Engineering is traceability [27]. It is often hard to trace individual design decisions to the legal or business objectives that give rise to them. By capturing the properties of alternative interpretations, early on in the process, and track their development until finally one gets selected, traceability should be improved.

Improving traceability of decisions should also improve accountability [4]. Typically, auditors on behalf of the regulator demand to know how compliance officers respond to certain legal issues. In particular, when organizations choose to deviate from the expected, they need to have a motivation (comply or explain). Tracing the pros and cons of several alternatives, and motivating the final choice will help convince regulators that the organization is ‘in control’.

III. LEGAL COMPLIANCE TRADE-OFF ANALYSIS

A. LEGAL-URN FRAMEWORK OVERVIEW

The LEGAL-URN framework [12] is a goal-oriented compliance framework based on the User Requirements Notation (URN) Language [20] which combines Goal-oriented Requirements Language (GRL) and Use Case Maps (UCM). The LEGAL-URN framework includes four layers of legal and organizational models: official source documents, Hohfeldian models which are based on Hohfeldian classes of rights [17], goal models (GRL and Legal-GRL) and business process models (UCM and Legal-UCM). Each element of LEGAL-URN is linked to each other via a set of traceability links.

In the Legal-GRL layer, different elements of the legal statements are mapped to GRL elements. Each legal statement can have one actor (the subject) and one modal verb (modality), one to many clauses (verb and action), 0 to many crossreference, 0 to many precondition and 0 to many exception. Modalities are of type of permission and obligation. Thus in Legal-GRL, goals and softgoals can be Permission or Obligation goals/softgoals.

Organizational GRL captures the high-level goals of the organizations as softgoal and goals and the alternatives to achieve these goals via tasks. GRL softgoals such as costs, time, scalability, confidentiality, etc, are type of goals that are abstract and they cannot be achieved fully. Tasks (or alternative solutions) in both GRL and Legal-GRL models are used to realize (legal) goals and softgoals. These tasks are linked to the goals and softgoals of both models via decomposition, contribution or correlation links.

More detail of LEGAL-URN is described in [14]. LEGAL-URN also has the capability to compare multiple regulations [15] and analyze the degree of compliance [13].

B. COMPLIANCE ANALYSIS WITH LEGAL-URN

In LEGAL-URN, compliance analysis occurs at the level of goals (i.e. Legal-GRL and GRL level). To analyze the compliance of organization to regulations, first we create Legal-GRL and organizational GRL models and establish the traceability links between them. We exploit the GRL evaluation algorithm described in [1]. The analysis can be done quantitatively, qualitatively or with the mixture of both.

Compliance analysis starts by first giving a base value (quantitative or qualitative) to the lowest level intentional elements in our model. The satisfaction values are propagated to the higher levels goals and softgoals in organizational via the links between its intentional elements. The satisfaction values are also propagated to the Legal-GRL model via traceability links. After identifying the non-compliance instances, it is also possible to find out which business processes need to be fixed via responsibility links between GRL and UCM models. Based on the type of algorithm chosen, the result of the analysis can be qualitative (with the qualitative degrees of satisfaction: denied, weakly denied, weakly satisfied, satisfied, conflict, unknown, none) or quantitative (with quantitative degrees of satisfaction ranging from −100 to 100).

C. LEGAL INTERPRETATION ANALYSIS WITH LEGAL-URN

As mentioned earlier, legal statements are subjected to interpretation. The interpretations may be updated during time based on the case laws or new information. We capture the interpretation as “alternative” solutions (i.e. tasks) in LEGAL-URN. Each of these interpretations can have different impact on the high-level goals of both models. We model the different impacts via qualitative or quantitative contribution values.

To analyze the different interpretation and their impact on high level legal and organizational goal, we start by selecting an alternative/interpretation and assigning a satisfaction value to it. Based on the links between the alternative solution (i.e.
task) and the higher level goals and softgoals in both models, the satisfaction values of each of the goals and softgoals are calculated automatically. We repeat the same process for all of the alternative solutions and compare the satisfaction values of organizational and legal goals for all of the alternatives.

With this approach, organizations can decide to choose the alternative that best satisfies their own goals and legal goals. In this approach, however, the interpretations are not captured automatically. It is due to human judgment to interpret and disambiguate the law. The benefit of this approach over the paper-based decisions is that organizations can compare the impact of multiple alternatives on the organizational goals at the same time and before making any decision.

IV. CASE STUDIES

We now illustrate the use of LEGAL-URN in making a choice between legal interpretations via two case studies. Concepts that are modeled are shown in this font.

A. Case 1: XBRL Assurance

XBRL is a standard representation format for exchanging financial information [7]. The standard concerns the syntax of messages, which are called XBRL instances. The semantics of all kinds of concepts used for reporting is provided by an officially maintained taxonomy. In the Netherlands, XBRL is being adopted as part of a program called Standard Business Reporting (SBR) [18]. The program is coordinated by Logius, a government agency. Businesses and their representatives use the same representation format and taxonomy to construct messages to different stakeholders. Stakeholders are the Tax Administration (corporate tax declarations), Bureau of Statistics (quarterly reporting) and the Chamber of Commerce, which offers a portal for filing an electronic version of the annual financial accounts. The point of annual financial statements is that they are audited by an accountant. The accountant provides assurance over the statements made by management, about the results of the company. By law, from 2015, annual financial statements need to be filed in XBRL, through the SBR portal. That means, that both the financial statements and the accountants opinion need to be coded in XBRL. The required taxonomy extension and architecture for doing so need to conform to legal requirements, as laid down in the Civil Code of Annual Financial Statements (Civil Code, Book 2, title 9).

In 2013, a project team led by the association of chartered accountants (NBA) developed a reference framework to allow providing assurance over XBRL instances. This ‘assurance taxonomy’ was presented for review in autumn 2013 [23]. Strictly speaking, it is an extension of the SBR taxonomy, that deals with meta-data concerning financial reporting, reliability, and assurance provisioning. Agreements were made about security measures to ensure both confidentiality and integrity of the data encoded in XBRL instances.

Subsequently, a prototype was developed by Logius with the initial tests scheduled in 2014. Since the time schedule was very tight, one of the goals was Implementation in

Limited Time. As it can be expected, at the beginning of 2014 many development issues were still open. Here, we discuss one particular issue: the instance architecture. How should assurance be encoded in an XBRL instance, about another XBRL instance, in a reliable way?

According to the initial requirements of the project, the architecture contained five XBRL instances (Figure 2). The company prepares a financial report (1). The manager needs to sign; the signature is coded as a separate XBRL instance that refers to the first one using a unique hash code (2). The accountant prepares an assurance report (3), which refers to the statement, again using a hash code. The accountant uses a professional PKI certificate to sign the assurance report (4). All of this is filed as one package at the Chamber of Commerce portal (5).

This process, however, creates a conflict. The fact that five separate instances are needed, makes the XBRL filings very large, and would make filing on a large scale impossible, given reasonable assumptions about bandwidth and storage space.

Logius, as the project leader, was under time pressure to create a working solution within the available infrastructure. Moreover, they did not want to burden the Chamber of Commerce with a portal overload. NBA did not want to change the framework since they had backing of many other stakeholders and their reference framework was generic. To them, it is crucial that both the manager and the accountant can sign their statements, and that are linked. They did not realize that this architecture is expensive in terms of storage space, as they never considered feasibility, and did not regard signatures as separate messages.

Under the time pressure, Logius convinced the other stakeholders to settle for a compromise: three XBRL instances. They argued that the manager’s signature is redundant, as the manager is typically also mentioned in the financial report, as its author. They also argued that linking the assurance report with the financial report does not need to be done in XBRL itself. This can be done by encrypting the outer XML message, in which the XBRL is embedded, using the XAdES standard. This process of linking and storing was termed ‘certified archiving’ (Dutch: zekerstellen) [24].

Although this outcome is probably the only feasible one, given the described circumstance, one could argue that the compromise architecture is not compliant: it does not respect
the clause that the manager should sign the annual statements (Civil Code 2-210). Furthermore, the point of XBRL is to be a standard; the XBRL Assurance reference architecture was adopted as an official extension of the taxonomy. This should ensure compatibility with other developments, like XBRL-based reporting under MIFID regulations. This work-around already creates an exception to the standard.

To help Logius with understanding the impact of their choices on their own goals and the legal objectives, we modeled the two alternatives, i.e. 3 XBRL Instances and 5 XBRL Instances with LEGAL-URN. As it is shown in Figure 3, alternative 1 (5 XBRL Instances) has negative impact on Logius’ softgoals. Minimize Cost, Limited Storage, Limited Time and Limited Bandwidth are shown as “Red” which means that their satisfaction values are “denied”. However, this alternative is the one in compliant with XBRL assurance. That is, it is fully satisfying the law (All legal softgoals are in “Green”). On the other hand, alternative 2, 3 XBRL insurance has positive impact (“Light Green”) on Logius softgoals except Minimize cost (which is neutral). However, this alternative is not fully compliant with XBRL assurance. In this case, Logius has to decide whether to violate some of the legal aspects but provide a feasible solution and accept consequence or being fully compliant but delaying the project.

B. Case 2: Right to be Forgotten

In 2012 the European Commission proposed a major reform of the European Union (EU) legal framework on the protection of personal data. The various data protection acts of the member states, now based on Directive 1995/46/EC, will be harmonized in a single EU regulation [8]. Part of the regulation is the so-called ‘Right to be Forgotten’ (Article 17): “Any person should have the right to have personal data concerning them rectified and a ‘right to be forgotten’ where the retention of such data is not in compliance with this Regulation. In particular, data subjects should have the right that their personal data are erased and no longer processed, where the data are no longer necessary in relation to the purposes for which the data are collected or otherwise processed, where data subjects have withdrawn their consent for processing or where they object to the processing of personal data concerning them or where the processing of their personal data otherwise does not comply with this Regulation.” [8].

The right to be forgotten attracted a lot of attention and debate, when a Spanish citizen started a lawsuit to have links to his personal data removed by search engines, such as Google. In response, the EU Court of Justice issued a ruling which addresses in particular on-line search engines [9]. The ruling states that individuals have the right – under certain conditions – to ask search engines to remove links to their personal information. This applies where the information is inaccurate, inadequate, irrelevant or excessive for the purpose for which the data is being collected or processed. To avoid a possible conflict with the ‘freedom of expression’, the EU Court of Justice confirms that “the right to get your data erased is not absolute and has clear limits. The request for erasure has to be assessed on a case-by-case basis. It only applies where personal data storage is no longer necessary or is irrelevant for the original purposes of the processing for which the data was collected. Removing irrelevant and outdated links is not tantamount to deleting content [9]”

The ‘right to be forgotten’ is subject to interpretation. To implement this principle, Google and other search engines have to decide on what is outdated, irrelevant or unnecessary. Also, in the case of removal, they have to decide whether to inform the source of the removed data. Furthermore, it is unclear whether the law is applicable to all instances of the search engine (such as Google.com) or just to the local search engine of the citizen (Google.fr for French citizens). Since summer 2014, Google has provided a form for EU citizens to request de-listing. Until January 2015, Google has evaluated more than 202,000 requests asking for more than 733,000 URLs to be removed, according to its Transparency Report (http://www.google.com/transparencyreport/removals/). It has only agreed to a minority of requests, removing just under 238,000 URLs from search results so far. In their interpretation, Google limits the application scope to EU. If an EU citizen asks for removal of their personal data from the Google, the data is only removed from the local Google search engine (e.g. Google.fr) in Europe and not globally.

The debate also centers on a conflict between the right of the individual to be forgotten and the right of other citizens to have access to information. Search engines like Google provide public infrastructure for democracies. Suppose that the major of a town was found guilty of bribery. That information is relevant to the inhabitants of the town, and should remain accessible. By contrast, suppose a student has ‘drunken pictures’ on social media. After the graduation, she wants to remove these pictures, but as copies have been made, this proves impossible. A person should have control over the data that is made available about him or her. Because of these tensions, the ruling states that decisions is made on a case-to-case basis. When assessing the circumstances, European Data Protection Authorities consider the interest of the public in having access to the information. If the interest of the public overrides the rights of the data subject, de-listing is not appropriate.

Google has to anticipate on these decisions. It is important to get it right; non-compliance can be expensive [10], [22]. So many other parties are following the Google case. Clearly, this is an example of what Julia Black [2] calls a regulatory debate, which helps shape the borderline of acceptable behaviors. To illustrate the usefulness of LEGAL-URN for modeling such debates, in Figure 4 we capture the issues that play role, and how they are related to the main objectives of the ruling.

In this figure, We only look at two alternatives of Removing Links to PI Locally or Removing Links to PI Globally. As it is shown, both of these options have negative impact on Comply with Freedom of Expression. Removing Links to PI Globally is worse with respect to Transparency but it is doing better (i.e. “Green” versus “Light Green”) with regards
to their own goals, Comply with Right to be Forgotten and Avoid Penalty. However, this option results in conflict for Google. In addition, Removing Links to PI Globally satisfies the legal obligation goal, Remove Links to Personal Information better than Removing Links to PI Locally. In this case, Google has to decide between being fully compliant with the law but having conflict in their own goals or being semi-compliant but satisfying their own goals partially as well.

C. Evaluation

Once alternatives have been discussed, they need to be stored for later reference. Compliance officers maintain repositories of the various alternative interpretations, the legal sources that motivate them, the legal objectives covered, and properties on the basis of which they can be compared. To maintain the repository and managing the change, URN models can be exported to the IBM DOORS tool [19]. Such tool has the capability to store the previous decisions with their evaluations and compare the changes in future.

V. DISCUSSION

In this paper, we investigate the usefulness of existing requirements engineering tools and techniques, in particular LEGAL-URN, for handling alternative legal interpretations.

We used LEGAL-URN framework, since the framework already has methods for creating goal models for law and analysis of compliance with the law. Adding different interpretation to the framework can help in the ambiguous situations that one may encounter in modeling legal goals. In this case, it is possible to perform the analysis with respect to the organizational high-level goals instead of the original compliance analysis of LEGAL-URN.

The case studies in this paper illustrated simple cases where the organization has to decide between only two alternatives. This process can be trivial and traditional paper-based approaches can be as effective. However, LEGAL-URN framework together with its tool support, jUCMNav, provides capability to model one or more than one regulation and analyze compliance with more than one regulation at the same time [15]. By adding alternative interpretation to LEGAL-URN framework, we allow users to not only check their compliance to multiple regulations but also analyzing the impact of their legal decisions on their high-level goals.

VI. CONCLUSION

In this preliminary work, we illustrate that with the help of Legal-GRL and GRL layer of LEGAL-URN, an organization can capture different alternative interpretations of legal clauses and help to choose an alternative which satisfies the main objectives of the organization while not violating the law. In addition, explicitly capturing interpretations improves traceability, and can be used as a proof of compliance to the regulator, as it brings about discussions about best practices. Thus it enhances accountability.

In future, we would like to expand our work with a more elaborate case study and analyze the validity of this preliminary work in more detail. We would also like to capture the different positions of stakeholders in a debate. This would make it possible to integrate with an argumentation framework [26], [5].
ACKNOWLEDGMENT

Sepideh Ghanavati is supported by AFR - PDR grant #5810263, Luxembourg.

REFERENCES


