A Legal Validation of a Formal Representation of GDPR Articles

Cesare Bartolini[1], Gabriele Lenzini[1], and Cristiana Santos[2]

[1] University of Luxembourg,
Interdisciplinary Centre for Security, Reliability and Trust (SnT) *
{cesare.bartolini, gabriele.lenzini}@uni.lu
[2] University of Minho, JusGov
cristiana.teixeirasantos@gmail.com

Abstract. It is possible to model the meaning of articles of the GDPR in logic formulæ and this enables a *semi-automatic reasoning* over the Regulation, e.g., to build an argument of compliance. However, any formal reasoning requires that the formulæ are validly expressing the legal meaning(s) of the articles, including potential disagreements between legal experts over their interpretation. The problem is that IT experts may anticipate some unofficial legal meaning, invalid under any interpretation, while verifying if this happens requires legal expertise. However, legal experts are unlikely familiar with the logic formalism and cannot give informed feedback without understanding the legal interpretation(s) that a formula embodies. On a previous work, we devised a methodology and a human-readable intermediate representation to help non-experts reading formulæ in Reified I/O logic (RIO), a formalism expressing GDPR provisions introduced to reason about data protection compliance. This paper validates the methodology and shows that is possible to retrieve feedback from legal experts about the validity the RIO representation of the Regulation. Precisely, we collect and evaluate the feedback on the RIO version of Art. 5.1a and Art. 7.1, and show how to elicit suggestions to improve the formalization thereof. What emerges is an agile process to support public trust in the formal framework and in its use.

Keywords: General Data Protection Regulation (GDPR), data protection, compliance, legal validation.

1 Introduction

The processing of personal data – and therefore data protection legislation – is an essential facet of a modern economy. Personal data is widely associated with a modern business model made of Internet-based services offered free of charge and whose revenues come from the collection, the processing and the use of personal data for advertising purposes, but it comes into play also with more

* Bartolini and Lenzini are supported by the FNR CORE project C16/IS/11333956 "DAPRECO: DAta Protection REgulation COmpliance".

traditional business models, such as the product market, which are evolving to e-commerce, or tailoring their offers to individual customers.

The legal landscape of the protection of personal data within and outside the European Union (EU) has been redesigned by the amplitude of the material and territorial scope of the General Data Protection Regulation (GDPR) [5,25,21], as had already happened, to some extent, with the previous Directive [9].

This new landscape, coupled with the heavy fines that supervisory authorities are entitled to issue in case of violation, calls for a need to ensure that data processing activities (and tools thereof) comply with the GDPR. Data controllers and processors could therefore take advantage from tools helping design and verify compliance, thus diminishing their risks of violating provisions and incurring into fines. Such tools could also help companies build, in an automated or computer-assisted way, their case in response to one-time casuistic decisions emanated by supervisory authorities and courts against them.

A critical facet for such automation is to be able to build executable rules for a computer-assisted assessing compliance. In previous research, the authors have proposed a complete model of the GDPR for legal reasoning and legal compliance [1,17,16,15]. This model comprises three components: the legal text in Akoma Ntoso format, an ontology of legal concepts concerning privacy and data protection, and a knowledge base of data protection rules in LegalRuleML format. This last component, called the Data Protection Regulation Compliance (DAPRECO) Knowledge Bas Knowledge Base, is the most critical: it contains the bulk of provisions written as logic rules that can be used e.g., to check whether certain practices (themselves also formalized) are aligned with the provisions. Consequently, the Knowledge Base needs to be adequately (i.e., legally) validated before it can perform in a real-world environment. This pragmatical strand is demanded, since "for developers, as contrasted to researchers, the issue is not whether the resulting rule base is complete or even accurate or self-modifying – but whether the rule base is sufficiently accurate to be useful" [3] when it is moved out from the research laboratory and into the marketplace [24].

However, as is widely acknowledged in literature [19,23,11], testing Legal Knowledge Based System (LKBS) is a difficult task. It is more difficult even than software testing in general because approaches reveal coder-dependency and it is complex to emulate the "art-of-the-experts" [4]. With ongoing maturity in the field of AI and Law and Legal Knowledge-Based Systems, the need for an easily accessible and interdisciplinary validation methodology comes into play [10].

The concept of validation refers to the determination of the correctness of the system with respect to user needs and requirements [23]. Legal validation is thus "needed to verify the correctness of the output of the system in relation to the knowledge of the legal domain it covers", "the guarantee of the one-to-one relation between analysis and representation" [12]. Such a method would assist legal professionals framing an evaluation of legal knowledge-based systems and help IT experts understanding the validation requirements of legal professionals [11].

As "algorithmic representations of law are typically very poor as regards their transparency", "one cannot begin to devise an algorithm to apply legal provisions without determining first its intended purpose and by whom it will be used" [22]. Therefore, validating a legal model requires that the formalization used is understandable, accessible. Consequently, the methodology should be driven by usability considerations in the adopted criteria, and validation tests (through user acceptance surveys or questionnaires) [23].

In the particular domain of modelling the GDPR, a considerable effort has been reserved to represent the Regulation's provision in a logic formalism, precisely the Reified Input/Output (RIO) logic [20]. As we will recall in Section 3, the logic formulæ refer to concepts that belong to a legal ontology for data protection, that is, the Privacy Ontology (PrOnto) ontology which is the result from an interdisciplinary effort meant to provide legal soundness. But of course referring to an ontology is not sufficient to ensure legal soundness in a reasoning process for many reasons, among which that the ontology has been devised for concepts relevant in data privacy but not for the specific context of the GDPR and thus new concepts may need to be expressed; besides, certain legal interpretation are anticipated e.g., in the choice of the formula's functions or when deciding that certain articles express an obligation or a permission. We will discuss further the critical points of a formalization exercise but, in short, it should be evident that formalizing articles in a logic formalism requires a legal supervision. Postponing any legal validation until the whole GDPR is translated into RIO formulæ, as it would happen if we were awaiting to have any output of the enabled logical reasoning, is a procedure prone to errors. Finding and removing the cause of some unsound conclusions would be also a very expensive step if left only at the end, quite likely inspiring distrust in the whole framework. A more *agile* process is advisable to verify for legal soundness, assisting who is responsible for the formalisation of the GDPR incrementally and concomitantly during the modelling work.

Pursuant to this, we discussed in [2] such an agile methodology, proposing also a solution for a further problem that arose in this case: how to let expert in law understand the logic formula, which are usually embedded in a machine readable but quite human incomprehensible LegalRuleML, in such a way to collect *informed* feedback from them about the legal soundness of the formalization. The solution is an intermediate representations, devised human-readable, of a RIO logic formalization of two GDPR articles. A usability experiment involving legal domain experts, consisting in assessing the readability and understandability of the human-readable representation compared with the original LegalRuleML version and with another control format, brought evidence that the former suits the purpose of being used for an interdisciplinary legal validation.

The customizable human-readable representation has been assessed as understandable, increasing our confidence on it being an eligible candidate to validate the formalized GDPR articles. In this work we proceed further and show that the methodology is effective in gathering feedback of legal experts on the legal validity of the representation of the GDPR articles, so as to provide quality assurance of our methodology as a whole.

2 Related work

Some discussion within the AI and Law community [23,11,10] – specifically amidst the Proceedings of the International Conference on Artificial Intelligence and Law works (ICAIL), and later through the Journal of Artificial Intelligence and Law contributions (JAIL), – concerned qualitative evaluation methodologies suitable for legal domain systems/techniques, and the best practices through which AI and Law researchers could frame the assessment of the performance of their works, both empirical and theoretical. For example, performance evaluation is emphasized and compared to known baselines and parameters, using publicly available datasets whenever possible [7,8].

A set of six categories was compiled to define the broad types of evaluation found therefrom. They include the following assessments: i. *Gold Data*: evaluation performed with respect to domain expert judgments (e.g., classification measurements or measures on accuracy, precision, recall, F-score, etc.); ii. *Statistical*: evaluation performed with respect to comparison functions (e.g., unsupervised learning: cluster internal-similarity, cosine similarity, etc.); iii. *Manual Assessment*: performance is measured by humans via inspection, assessment, review of output; iv. *Algorithmic*: assessment made in terms of performance of a system, such as a multi-agent system; v. *Operational-Usability*: assessment of a system's operational characteristics or usability aspects; vi. *Other*: those systems with distinct forms of evaluation not covered in the categories above (task-based, conversion-based, etc.). In our case, we combined the following types of evaluation: gold data (i.), manual assessment (iii.) and operational-usability (v.).

Some authors [10] developed the Context Criteria Contingency-guidelines Framework (CCCF) for evaluating LKBS. Besides considering evaluation context and goals, they also propose evaluative criteria and guidelines alike. In this framework, the quadrant criteria pertinent to the purposes of this paper are herewith mentioned. The *User Credibility* quadrant refers to credibility and acceptability of a system at the individual level. It comprises three main branches associated with *user satisfaction*, *utility* (usefulness or fitness for purpose) and *usability* (ease of use). The usability branch is further decomposed into branches associated with operability, understandability, learnability, accessibility, flexibility in use, and with other human factors and human computer interface issues. The *Verification and Validation* criteria quadrant refer to knowledge base validity, including knowledge representation and associated theories of jurisprudence, inferencing, and the provision of explanations.

The validation phase of legal modeling by domain legal experts – driven by operational usability assessments – is also mentioned in the methodologies referring to ontological expert knowledge evaluation. For example, the Methodology for Modeling Legal Ontologies (MeLOn) [14] offers evaluation parameters consisting in completeness, correctness, coherence of the conceptualization phase and artifact reusability. Usability concerns were considered in an experimental validation of a legal ontology by legal experts, the Ontology of Professional Judicial Knowledge (OPJK), described in [6]. This model was validated in a two-step process. First, the evaluators answered a questionnaire whereby they expressed their opinion on their level of agreement towards the ontology conceptualization and provided suggestions for the improvement thereof. Then an experimental validation based on a usability questionnaire followed, the System Usability Scale (SUS), tailored to evaluate the understandably and acceptance of the contents of the ontology. This evaluation questionnaire could offer rapid feedback and support towards the establishment of relevant agreement, shareability or quality of content measurements in expert-based ontology evaluation. An evaluation methodology based on Competency Questions (CQs) [18] was built to evaluate the transformation of legal knowledge from a semi-formal form (Semantics Of Business Vocabulary And Rules - Standard English (SBVR-SE)) [13] to a more structured formal representation (OWL 2), and to enable cooperation between legal expert and knowledge IT expert in charge of the modelling in logic formalism. Ontology quality criteria were accounted for.

Although the legal formal framework target of this work's analysis (i.e., the DAPRECO Knowledge Base) refers and is strictly bound to a legally validated ontology (i.e., the PrOnto) an argument for its legal validity cannot follow only from the validity of the ontology of reference. It requires a more comprehensive analysis and we believe that both qualitative evaluation methodologies and certain criteria from the CCCF are required. Ontologies are in fact about concepts, data, and entities and any validation strategy of them is inevitably about assessing the legal qualities of those objects. Formal models for legal compliance, such as the DAPRECO Knowledge Base, model also the logical and deontic structure of a legal text, its temporal aspects and, as when the formalism allows multiple conflicting interpretations, as the DAPRECO Knowledge Base does, it includes structural elements to allow defeasible reasoning. The validation assessment should take these elements into account.

Thus, the necessity of an integrated approach, which additionally should also acknowledge an operational-usability assessment, since the legal validity of the DAPRECO Knowledge Base logic formulæ have to be validated by people who are not experts in logic.

3 Background and Methods

This work leverages on our previous work [2] which discusses how to take the formalization of GDPR provisions expressed in RIO logic [20] and how to extract from them pieces of information that a legal expert will process of legal validity. This, in fact, means to answer a questionnaire whose questions are meant to provide feedback on specific quality linked to the legal validity, such as completeness, coherence, and conciseness (see later). We will refer to this synthetic digest of an otherwise specific logic formalism as *human-readable representation of a RIO formula.*

Empirical validation using tailored constructed questionnaire is a very useful quantitative indicator of user acceptance [26]. In this case, where users are lawyers, the questionnaire has been designed with the purpose of having legal feedback on the quality of the legal interpretation in the RIO formulæ. The questionnaire is build around six questions reported in Table 1.

Table 1. The questions used.

q_1	Does the deontic modality (obligation/permission/other) of the formula coincide with the modality of the GDPR articles?
q_2	Does the formula capture all the important legal concepts?
q_3	Does the formula capture all the important legal relations?
q_4	Is the interpretation given by the model correct?
q_5	Is the interpretation complete?
q_6	Is the interpretation to the point?

They are tailored to check for the following legal validation qualities: Accuracy (q_1); Completeness ($q_2 - q_4$); Consistency (q_5); and Conciseness (q_6).

We now give two examples of human-readable representations accompanying the questionnaire. Both examples will be referred later in this paper.

Example 1. We refer to Article 7.1 of the GDPR, which reads:

> "*Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data*"

Without entering into any detail on its modeling (the reader can refer to [20] for it), RIO formula expressing this provision is the following:

$$
\begin{aligned}
&(\,[\,(\mathsf{RexistAtTime}\ a_1\ t_1) \wedge (\mathsf{and}\ a_1\ e_p\ e_{hc}\ e_{au}\ e_{dp}) \wedge (\mathsf{DataSubject}\ w) \wedge \\
&\quad (\mathsf{PersonalData}\ z\ w) \wedge (\mathsf{Controller}\ y\ z) \wedge (\mathsf{Processor}\ x) \wedge (\mathsf{nominates}'\ e_{dp}\ y\ x) \wedge \\
&\quad (\mathsf{PersonalDataProcessing}'\ e_p\ x\ z) \wedge (\mathsf{Purpose}\ e_{pu}) \wedge (\mathsf{isBasedOn}\ e_p\ e_{pu}) \wedge \\
&\quad (\mathsf{Consent}\ c) \wedge (\mathsf{GiveConsent}'\ e_{hc}\ w\ c) \wedge (\mathsf{AuthorizedBy}'\ e_{au}\ e_{pu}\ c)\,] \rightarrow \\
&\quad [\,(\mathsf{RexistAtTime}\ e_a\ t_1) \wedge (\mathsf{AbleTo}'\ e_a\ y\ e_d) \wedge (\mathsf{Demonstrate}'\ e_d\ y\ e_{hc})\,]\,) \in O
\end{aligned} \tag{1}
$$

Names like nominates and PersonalData are either chosen by the IT expert in charge of the modelling in logic formalism or are taken from the PrOnto [17,16,15]. PrOnto is one of the three essential components along with the Akoma Ntoso representation of the legal text and the formulæ in RIO logic. When connected together the three components form the complete model of the GDPR. The formula expresses an obligation, and that is what the O at the rightmost end Equation (1) is supposed to mean. Equation (1) is not however what a user would see. Stored to be machine-readable, the formula is written in its LegalRuleML version. An excerpt of this version is given below.

Listing 1. LegalRuleML representation of formula 1 (snippet).

```
<ruleml:Rule closure=”universal”>
```

```
    <ruleml:if>
      <ruleml:Exists>
        <ruleml:And>
          <ruleml:Atom>
            <ruleml:Rel iri=”rioOnto:RexistAtTime” />
            <ruleml:Var keyref=”:a1” />
            <ruleml:Var key=”:t1”>t1</ruleml:Var>
          </ruleml:Atom>
          ...
          <ruleml:Atom>
            <ruleml:Rel iri=”prOnto:DataSubject” />
            <ruleml:Var keyref=”:w” />
          </ruleml:Atom>
          ...
        </ruleml:And>
      </ruleml:Exists>
    </ruleml:if>
    <ruleml:then>
      <ruleml:Exists>
        <ruleml:And>
          <ruleml:Atom>
            <ruleml:Rel iri=”rioOnto:RexistAtTime” />
            <ruleml:Var keyref=”:ea” />
            <ruleml:Var keyref=”:t1” />
          </ruleml:Atom>
          ...
        </ruleml:And>
      </ruleml:Exists>
    </ruleml:then>
  </ruleml:Rule>
```

In [1], we described a parser that reads LegalRuleML and returns an itemized structured representation of the formula whose intended meaning has not been changed and is preserved in the translation. This version renders a cleaner version without all those XML based tags which are quite hard to process by a human reader. Applied to the LegalRuleML of (1), it results in the following text:

IF, in at least a situation,

- At time $:t_1$, the following situation exists:
  - (All of the following $(:a_1)$)
    1. **Processor** $(:x)$ does **PersonalDataProcessing** $(:e_p)$ of **PersonalData** $(:z)$
    2. **DataSubject** $(:w)$ performs a **GiveConsent** $(:e_{hc})$ action on **Consent** $(:c)$
    3. **Purpose** $(:e_{pu})$ is **AuthorizedBy** $(:e_{au})$ **Consent** $(:c)$
    4. **Controller** $(:y)$ **nominates** $(:e_{dp})$ **Processor** $(:x)$
  - **PersonalData** $(:z)$ is relating to **DataSubject** $(:w)$
  - The **Controller** $(:y)$ is controlling **PersonalData** $(:z)$
  - **PersonalDataProcessing** $(:e_p)$ **isBasedOn Purpose** $(:e_{pu})$

THEN it must happen that, in at least a situation,

- At time $:t_1$, **Controller** $(:y)$ is **Obliged** to **AbleTo** $(:e_a)$
  - **Controller** $(:y)$ **Demonstrate** $(:e_d)$ **GiveConsent** $(:e_{hc})$

The words capitalized and in bold are concepts from the PrOnto ontology. The words in bold non-capitalized are relations introduced by the IT expert. Although this format still requires some mental effort to be read, it is at least human-processable;

The *human-readable* representation is built from the output of the parser through a manual post-processing. That of Article 7.1 is shown in Table 2.

Table 2. Human-readable representation of the RIO formulæ expressing Article 7.1.

Premise	Where processing is based on consent,
Conclusion	the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
Modality	Obligation
Ontological Concepts	Where [Processing] is based on [Consent], the [Controller] shall be [Able to] [Demonstrate] that the [Data subject] [Has consented = GiveConsent] to [Processing] of his or her [Personal data]
Other Ontological Concepts	[Purpose]; [Processor]; [IsAuthorizedBy]; [Nominates]; [IsBasedOn]; [BeAbleTo]
Context	There is a processing, which has a purpose authorized by a consent given by a data subject, and that is what a processor, whom a controller controlling the personal data nominates, does on personal data of the data of the data subject.
Overall Meaning	**Whenever** there is a processing, which has a purpose authorized by a consent given by a data subject, and that is what a processor, whom a controller controlling the personal data nominates, does on personal data of the data of the data subject **then** the controller is **obliged** to able to demonstrate that "data subject gave consent".

Example 2. We refer to Article 5.1(a) of the GDPR, which is worded as follows:

> "*Personal data shall be a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');*"

The output of the re-interpretation of the RIO formula (here omitted for reasons of space), transform the LegalRuleML as follows:

IF, in at least a situation,

- At time :t_1, the following situation exists:
  - (All of the following (:a_1))
    1. The **PersonalDataProcessing** (:e_p) is performed by **Processor** (:x) over the **PersonalData** (:z)
    2. **Controller** (:y) **nominates** (:edp) **Processor** (:x)
  - **PersonalData** (:z) is relating to **DataSubject** (:w)
  - The **Controller** (:y) is controlling **PersonalData** (:z)

THEN it must happen that, in at least a situation,

- At, time $t2$, **Controller** (:y) is **Obliged to**
  - (All the following (:$a2$))
    1. Controller (:y) Implement (:ei) Measure (:em)
    2. The fact **Measure** (:em) is the cause of the fact **lawfulness** (:el)
    3. The fact **Measure** (:em) is the cause of the fact **fairness** (:ef)
    4. The fact **Measure** (:em) is the cause of the fact **transparency** (:et)
    5. **Controller** (:y) **Describe** (:ed) **Implement** (:ei)
  - **Thing** (:t1) is greater than, or at least equal to, **Thing** (:t2)
  - **PersonalDataProcessing** (:ep) respects the principle of **lawfulness** (:el)
  - **PersonalDataProcessing**(:ep) respects the principle of **fairness** (:ef)
  - **PersonalDataProcessing** (:ep) respects the principle of **transparency** (:et)
  - Task **PersonalDataProcessing** (:ep) is **RelatedTo DataSubject** (:w)

The output of the hand-made processing is shown in Table 3.

Table 3. Human-readable representation of the RIO formulæ expressing Article 5.1(a).

Premise	-
Conclusion	Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');
Modality	Obligation
Ontological Concepts	[Personal data] shall be [Processed] lawfully, fairly and in a transparent manner [InRelationTo] the [Data subject] ('[Lawfulness], [Fairness] and [Transparency]');
Other Ontological Concepts	[Processor]; [Measure]; [Nominates]; [IsBasedOn]; [Implement]; [Describe]
Context	There is a processing done by a processor on personal data of the data subject, and a controller, which is who controls the personal data; he nominates the processor. The controller describes (how) he implements a measure.
Overall Meaning	**Whenever** there is a processing done by a processor on personal data of the data subject, and a controller, which is who controls the personal data and who nominates the processor. **Then** before that moment **must be** that the controller describes (how) he implements a measure that is what causes lawfulness, fairness and transparency of the data processing related to the data subject.

4 Validation and Discussion

Can a legal validator reading the human-readable representation give useful feedback to the modeller? Answering this question is the goal of this paper. Rephrased, the goal is to show that the "Validation" phase of the methodology presented in [1] (see Figure 1) is effective, i.e., helpful feedback can be collected for the IT expert formalizing the GDPR with RIO logic.

The starting point is the human-readable representation of Articles 5.1(a) and 7.1 of the GDPR. The "Check" action (see Figure 1) has been implemented by gathering a set of four validators, all jurists knowledgeable of data protection law, and by asking them to answer questions $q_1 - q_6$ in Table 1.

Evaluators were told to compare the meaning of the formulæ, as expressed in the human-readable representation of the RIO logic, with the legal interpretation that them legal experts would give to the original articles in the GDPR.

We also asked them a few questions meant to reveal how much understandable for them is the human-readable format, before they start using it. General understandability of the format has been discussed elsewhere [1], but here the assessment is meant as a trust measure over the expert's answers. However, all our evaluators confirmed they have found the human-readable format understandable. From those trusted answers, we therefore compile a few recommendations. This is the "Generate Feedback" step in Figure 1.

Questions $q_1 - q_6$ (see Table 1) are yes/no questions, but in the questionnaire we additionally invited our checkers to motivate their answers and to pinpoint further whatever observation they valued meaningful. We collected eight documents with such written answers and comments which we reviewed and summarized. The following table resumes the findings, wherein we report the comments whenever the answer to the question was 'no', indicating that someone found some pertinent issue.

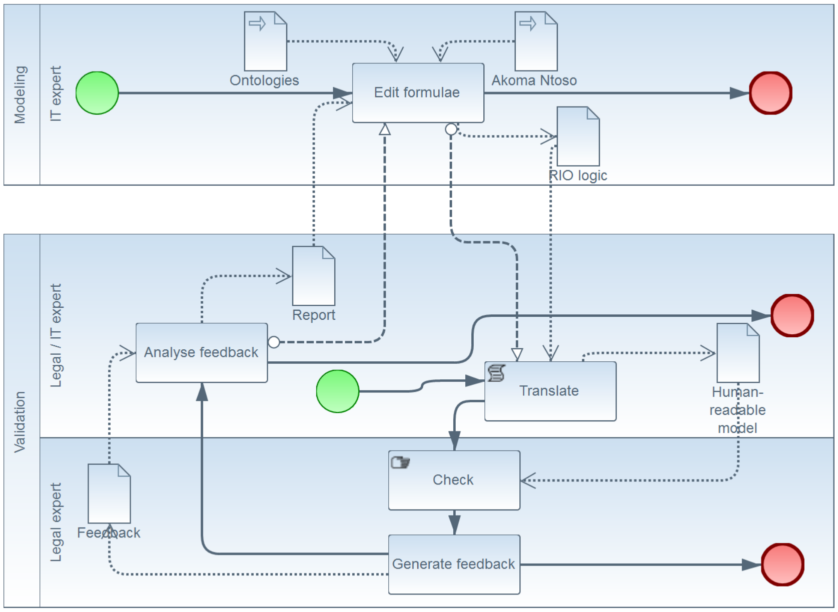


Fig. 1. Methodology (from [1]).

Table 4 shows that legal experts were able to give feedback on all the factors about the quality of the legal interpretation in the logic formalization of the articles. Even if the input to provide to the IT expert is not yet straightforward, a few highlights clearly emerge.

For instance, all experts easily understood and confirmed the deontic modality and agreed on the formulas be capturing all the legal concepts and relations (see Table 5). But is from the analysis conferred to the provided comments that we are able offer a broader spectrum, for they refer to the above surveyed criteria and also to other (non-surveyed) related criteria. Comments – in Completeness like “it was complex to capture the legal concepts within the structure of the formula”; comments in Consistency like “It refers to the implementation and description of a measure that it is hard to understand; “It is redundant and restates concepts already present at previous articles”, and comments in Conciseness like “’Obliged to be able to’ sounds weirds” – clearly indicate uneasiness about the way in which the formula have been structured; such comments may lead to a better formalization, for instance, stating certain contextual facts as a common premise valid for all the GDPR’s articles without repeating them each time in each article.

One evaluator, in particular, has mentioned “Interchanged roles for the controller and the processor” in Consistency. Even if that is stated in the Context of the human-readable table, the evaluator was probably induced in error/confused by the excess of information provided. Further analysis is of course required. Ex-

Table 4. human-readable representation of the RIO formulæ expressing Article 7.1.

	Art 5.1a	Art. 7.1
Accuracy	✓	✓
Completeness	It was complex to capture the legal concepts within the structure of the formula; It is missing the obligation: “the processing must be fair, lawful, transparent”	It was complex to capture the legal concepts within the structure of the formula;
Consistency	Interchanged roles for the controller and the processor; The interpretation is complex. It refers to the implementation and description of a measure that it is hard to understand; I can read/understand the model, but I think it does not faithful to the article’s meaning;	The reference to consent should be enhanced, namely regarding the requirements concerning the burden of the proof; “Shall” is not captured;
Conciseness	The formula mentions ”implement” ”describe” not expressed in the article; ”implement measure” is not expressed in the article; “Obliged to be able” sounds weird;	It is redundant and restates concepts already present at previous articles;

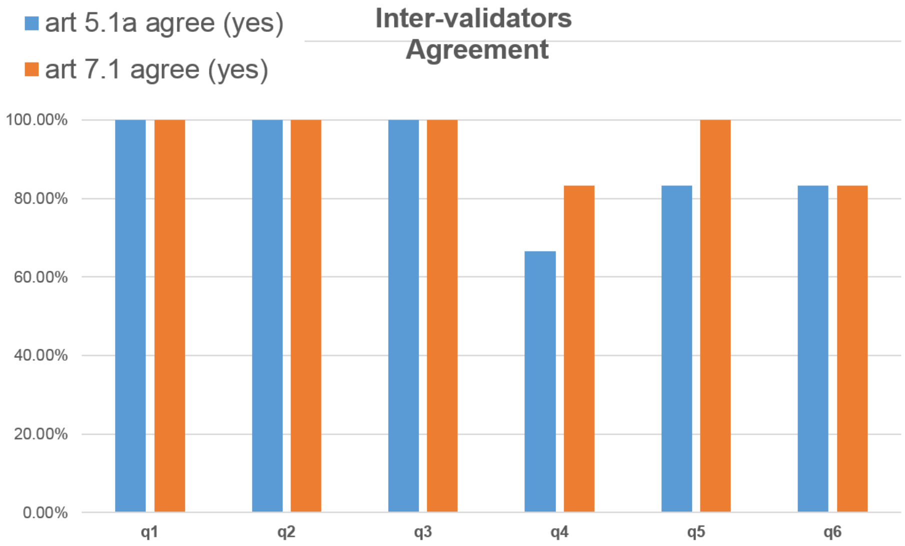
tracting from the non-structured comments valid input for the IT expert has to be left as future work, as we comment in the following section.

5 Conclusions and future work

This paper leverages a methodology that advocates an interdisciplinary validation of a representation of the GDPR articles in a logic formalism (i.e., RIO logic) to pursue quality, accountability, and transparency within. One important output of the methodology is the production of feedback derived from the involvement of legal experts, while assessing the quality of the legal interpretation that IT experts may instill in the formalization of the GDPR. This work has gathered evidence that such step is feasible. As a proof-of-concept, a small number of legal experts has been asked to answer six questions with the purpose of collecting comments about how two logic formulæ, modelling Articles 5.1a and 7.1 of the GDPR, are complete, accurate, concise, and consistent in reflecting the legal meaning of the articles. Several comments have been collected. Although a thorough analysis thereof requires more time – an involvement of a larger group of expert checkers is also advisable– we were able to identify a few issues of relevance using which the IT expert can review the formalization work.

Several challenges await us in the near future. We need to improve scalability in producing a human-readable representation of the RIO formulæ: it is currently done manually, starting from the pre-processed version. This is already more readable than the original LegalRuleML version and give us confidence that the work to produce a natural language analysis break-up table can be automatized. This step done, a forth bringing process will consist in streamlining the validation of the RIO formalization of the GDPR as a whole. This likely requires to set up

Table 5. Inter-validators agreement on answering 'yes' to the questions



an application where the work of the IT expert can be suitably translated in to the human-readable format and offered for on-line checking to a group of legal testers, which may also vary, providing feedback that the IT expert can take into consideration until a good quality of legal interpretation is assessed for the formulæ.

Concomitantly, there is a need to define together with the legal experts a more complete set of qualities and possibly a few metrics, which we can quantify and define criteria on the legal quality of the formalization. In Section 2 we pointed out possible metrics, and in this paper we have assessed a few (completeness, consistency, conciseness in Section 4), but a wide and systematic investigation of the state-of-the-art in this topic has not been done yet. The quadrant criteria presented in [10] also merits attention. This may lead to a revision of the current human-readable model.

References

1. Bartolini, C., Giurgiu, A., Lenzini, G., Robaldo, L.: Towards legal compliance by correlating standards and laws with a semi-automated methodology. In: BNAIC 2016: Modern Trends in Artificial Intelligence, Communications in Computer and Information Science, vol. 765, pp. 47–62. Springer International Publishing (2017)
2. Bartolini, C., Lenzini, G., Santos, C.: An interdisciplinary methodology to validate formal representations of legal text applied to the GDPR. In: Proceedings of the Twelfth International Workshop on Juris-informatics (JURISIN) (November 2018)

3. Berman, D.H.: Developer's choice in the legal domain. In: Proc. of the Third Int. Conf. on Artificial Intelligence and Law (ICAIL). ACM (June 1991)
4. Boella, G., Humphreys, L., Muthuri, R., Rossi, P., van der Torre L. W. N.: A Critical Analysis of Legal Requirements Engineering from the Perspective of Legal Practice. In: IEEE 7th Int. Work. on Requirements Engineering and Law (RELAW). pp. 14–21. IEEE (2014)
5. Buttarelli, G.: The EU GDPR as a clarion call for a new global digital gold standard. International Data Privacy Law 6(2), 77–78 (May 2016)
6. Casellas, N.: Ontology evaluation through usability measures. In: On the Move to Meaningful Internet Systems: OTM 2009 Workshops, Lecture Notes in Computer Science, vol. 5872, pp. 594–603. Springer (2009)
7. Conrad, J.G., Zeleznikow, J.: The significance of evaluation in AI and law. In: Proceedings of the Fourteenth International Conference on Artificial Intelligence and Law (ICAIL). pp. 186–191. ACM (June 2013)
8. Conrad, J.G., Zeleznikow, J.: The role of evaluation in AI and law. In: Proceedings of the Fifteenth International Conference on Artificial Intelligence and Law (ICAIL). pp. 181–186. ACM (June 2015)
9. Greenleaf, G.: The influence of european data privacy standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law 2(2), 68–92 (May 2012)
10. Hall, M.J.J., Hall, R., Zeleznikow, J.: A process for evaluating legal knowledge-based systems based upon the Context Criteria Contingency-guidelines Framework. In: Proceedings of the Ninth international conference on Artificial intelligence and law (ICAIL). pp. 274–283. ACM (June 2003)
11. Hall, M.J.J., Zeleznikow, J.: Acknowledging insufficiency in the evaluation of legal knowledge-based systems. In: Proceedings of the Eighth International Conference on Artificial Intelligence and Law (ICAIL). pp. 147–156. ACM (May 2001)
12. Koers, A.W.: Knowledge based systems in law. Kluwer Law and Taxation Publishers, 1 edn. (1989)
13. Lévy, F., Nazarenko, A.: Formalization of natural language regulations through SBVR structured english. In: Morgenstern, L., Stefaneas, P., Lévy, F., Wyner, A., Paschke, A. (eds.) Theory, Practice, and Applications of Rules on the Web, Lecture Notes in Computer Science, vol. 8035, pp. 19–33. Springer (2013)
14. Mockus, M., Palmirani, M.: Legal ontology for open government data mashups. In: Parycek, P., Edelmann, N. (eds.) Proceedings of the 7^{th} International Conference for E-Democracy and Open Government (CeDEM). pp. 113–124. IEEE Computer Society (May 2017)
15. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: Legal ontology for modelling GDPR concepts and norms. In: Proceedings of the 31^{st} International Conference on Legal Knowledge and Information Systems (JURIX) (December 2018), forthcoming
16. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: PrOnto: Privacy ontology for legal compliance. In: Proceedings of the 18^{th} European Conference on Digital Government (ECDG) (October 2018), upcoming.
17. Palmirani, M., Martoni, M., Rossi, A., Bartolini, C., Robaldo, L.: PrOnto: Privacy ontology for legal reasoning. In: Kö, A., Francesconi, E. (eds.) Electronic Government and the Information Systems Perspective, Information Systems and Applications, incl. Internet/Web, and HCI, vol. 11032, pp. 139–152. Springer (2018)
18. Ramakrishna, S., Górski, Ł., Paschke, A.: A dialogue between a lawyer and computer scientist. Applied Artificial Intelligence 30(3), 216–232 (2016)

19. Reich, Y.: Measuring the value of knowledge. International Journal of Human-Computer Studies 42(1), 3–30 (January 1995)
20. Robaldo, L., Sun, X.: Reified Input/Output logic: Combining Input/Output logic and reification to represent norms coming from existing legislation. Journal of Logic and Computation 27(8), 2471–2503 (December 2017)
21. Scott, M., Cerulus, L.: Europe's new data protection rules export privacy standards worldwide (February 2018)
22. Sergot, M.: The representation of law in computer programs. In: Bench-Capon, T. (ed.) Knowledge-Based Systems and Legal Applications, The A.P.I.C. Series, vol. 36, chap. 1, pp. 3–67. Academic Press (1991)
23. Stranieri, A., Zeleznikow, J.: The evaluation of legal knowledge based systems. In: Proceedings of the Seventh International Conference on Artificial Intelligence and Law (ICAIL). pp. 18–24. ACM (June 1999)
24. Susskind, R.E.: Expert Systems in Law. Out of the Research Laboratory and in the Marketplace. In: Proc. of ICAIL-1987, Boston, MA, 1987. pp. 1–8. ACM (1987)
25. Ustaran, E.: The true global effect of the GDPR (May 2018)
26. Zeleznikow, J.: The split-up project. Law, Probability and Risk 3(2), 147–168 (June 2004)