An Empirical Study on Socio-technical Modeling for Interdisciplinary Privacy Requirements

Claudia Negri-Ribalta, Rene Noel, Oscar Pastor, Camille Salinesi

An Empirical Study on Socio-technical Modeling for Interdisciplinary Privacy Requirements

Conference Paper · October 2023

DOI: 10.1007/978-3-031-46846-9_8

4 authors:

Claudia Negri-Ribalta
Université de Paris 1 Panthéon-Sorbonne
13 PUBLICATIONS **46** CITATIONS
SEE PROFILE

René Nöel
Universidad de Valparaíso (Chile)
59 PUBLICATIONS **231** CITATIONS
SEE PROFILE

Oscar Pastor
Universitat Politècnica de València
618 PUBLICATIONS **6,510** CITATIONS
SEE PROFILE

Camille Salinesi
Université de Paris 1 Panthéon-Sorbonne
278 PUBLICATIONS **3,006** CITATIONS
SEE PROFILE

An empirical study on socio-technical modeling for interdisciplinary privacy requirements *

Claudia Negri-Ribalta[1], Rene Noel[2,3], Oscar Pastor[3], and Camille Salinesi[4]

[1] SnT, University of Luxembourg, Luxembourg claudia.negriribalta@uni.lu
[2] Escuela de Ingenieria Civil Informatica, Universidad de Valparaiso, Chile
[3] VRAIN, Universidad Politécnica de Valencia, Spain
[4] CRI, Université Paris 1 Panthéon-Sorbonne, France

Abstract. Data protection regulations impose requirements on organizations that require interdisciplinary. Conceptual modeling of information systems, particularly goal modeling, has served to communicate with stakeholders of different backgrounds for software requirements analysis. An extension for a Socio-Technical Security (STS) modeling language was proposed to include data protection modeling concepts to help represent relevant issues of the European Union's General Data Protection Regulation. This article examines whether models designed with this extension serve as communication facilitators for privacy compliance and common ground across stakeholders. Through a series of 8 focus groups, with 21 subjects, we observed if professionals with different backgrounds (software developers, business analysts, and privacy experts) could detect discuss about the GDPR principles and identify privacy compliance "red flags" that we seeded in a use case. Using a qualitative approach to analyze the data, all the groups discussed the majority of the GDPR principles and identified more than 80% of the seeded red flags, with privacy experts identifying the most. This research provides preliminary results on using conceptual modeling as a communicator facilitator between stakeholders to contribute to a common ground between them.

Keywords: Privacy · Modeling Language · Compliance · Requirements

1 Introduction

Data protection laws seek to protect the fundamental human right of privacy [12], and against unfair practice [13]. Indeed, the GDPR[13] in Article 5 defines seven guiding principles that guide the regulation: (1) Lawfulness, fairness, and transparency; (2) Purpose limitation; (3) Data minimization; (4) Accuracy; (5) Storage limitation; (6) Integrity and confidentiality; (7) Accountability; setting a series of requirements that information systems (IS) must include in the software development lifecycle (SDLC)[13].

Compliance requirements must start from the early phases of the SDLC to avoid re-developing the IS [5]. These requirements are usually not included in the first

* This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 956562. Part of first (and corresponding) author work was done at Paris 1 as part of her PhD. thesis.

stages, particularly privacy requirements [6,5]. Furthermore, developers seem to have difficulties understanding regulatory privacy and data protection requirements[6,16]. This situation has led to a lack of "common ground" [16] - that is, establishing a shared understanding - over what data protection regulatory requirements are and how to satisfy them. Common ground is vital, as cross-functional teams that achieve it identify requirements from early phases, with fewer defects and reworkd in their IS [9].

For decades, conceptual models have enabled the communication of stakeholders with different backgrounds. Different established conceptual models have privacy extensions for goal [23], business process [1], and system modeling languages [2]. In particular, the Socio-Technical Security modeling language (STS-ml) [8] was designed to help analysts address security requirements at an early stage from a socio-technical point of view. However, empirical evidence on their facilitator role is an open challenge.

In previous work, an extension for STS-ml [8] has been proposed for data protection [24] to allow stakeholders to specify, share and negotiate data protection requirements from an interdisciplinary perspective. In this research, we identify the extension of [24] as STAGE (Socio-Technical Analysis of GDPR rEquirements). We aim to provide empirical evidence on the usage of STAGE, more specifically:

RQ1 - How do the subjects interact to identify and discuss GDPR compliance risks exposed in STAGE's model?

RQ2 - What are the GDPR principles discussed? And how?

Through the qualitative analysis of 8 different focus groups, where 21 subject experts in their area participated, our results show that conceptual modeling — even with limited knowledge of data protection — allowed subjects to discuss and identify privacy risks and compliance, even when they had different mental models [16]. Subjects also resolved conceptual inconsistencies seeded in the model regarding data protection, even without prior knowledge and experience of goal modeling. Most groups discussed and related most GDPR principles in the proposed scenario. Our results show that conceptual modeling can help interdisciplinary teams discuss regulatory requirements among stakeholders with different mental models and limited previous knowledge, helping establish common ground and identifying requirements from early phases [9].

The paper is structured as follows: in Section 2 we introduce the background work, followed by the research method in Section 3. Section 4 shares the results and their discussion. Threats to validity and future work are discussed in Section 5, while Section 6 presents the related work. Section 7 concludes and presents future work.

2 Background

2.1 The Socio-Technical Security Modeling Language (STS-ml)

Socio-technical systems are those systems encompassed by stakeholders of different natures: humans, organizations, and technology [8]. Building on this paradigm, STS-ml seeks to support modeling the relationships and intentions of the different actors, with a particular emphasis on security requirements. STS-ml is a security goal and actor-oriented modeling, part of the i* paradigm [25] based on the work of [31]. Modeling languages based on i* allow actors to have goals (intentions, desired state of the world [8])

and own assets and resources [31]. Goal models also specify how actors can also interact with other actors and delegate primitives (such as goals) between them, establishing social relationships. The STS-ml follows this approach by integrating security concepts.

In the STS-ml, actors can be agents, humans, or socio-technical systems and have (multiple) roles [8]. Actors can delegate to each other to achieve their needs through *delegating* one or more *goals*, for which they need to *transmit* information in the form of *documents*. Such transmissions can have six security requirements: *non-repudiation, redundancy, non-delegation, trustworthiness, goal-availability,* and *authentication*. Actors' inner goals can be decomposed into sub-goals through *AND/OR relationships*, which are achieved through documents. Documents are composed of *information* that an actor owns. An actor who owns information and depends on other actors, *authorizes* other actors to perform certain operations on the information for one or more specific goals. The operations that an actor can authorize are *reading*, *modifying*, *transmitting*, or using the information to *produce* new information.

The STS-ml considers three views to represent the above concepts, with different objectives [8]. First, in the *social view*, the intentions and interactions of the stakeholders are modeled. It gives a system overview, with decomposition of goals and relationships between the different actors, goals, and documents. Documents are modeled, and their transmissions are specified, detailing the relevant security requirements. In the *information view*, documents are decomposed into the information they contain, as well as the actors that own the information. It allows the analyst to revise the hierarchy of the information. Finally, the *authorization view* represents the authorizations regarding information across the actors, aiming to represent the permissions and prohibitions on how to use the data, with an emphasis in *read, modify, produce, and transmit*.

2.2 GDPR Extensions for the Socio-Technical Security Modeling Language

The first STS-ml GDPR extension was first proposed by [26]. This proposal addressed specific aspects of the GDPR: identification of *personal data*, *employment relationships* between actors, and *legal basis* for data processing. However, this extension is insufficient to address issues regarding GDPR principles [24]. Hence, [24] proposes STAGE. STAGE works on top of [26] and uses legal reasoning on the effects of not addressing the GDPR principles. STAGE proposes a way to identify *special categories of personal data*, *asymmetrical relationships* between actors, identify actors which provide information about *minors*, define the *data retention time* for personal data, and whether an actor *belongs to the EU*. Through this 5 semantically charged attributes, the objective is to provide more rich data protection semantics to help stakeholders to discuss compliance while keeping the language clean and simple. The metamodel for the extended STS-ml highlighting the STAGE contributions is shown in Figure 1.

3 Materials and Research Methods

3.1 Research Method

The main goal of the study is to explore how conceptual modeling helps professionals with different backgrounds establish common ground on data protection compliance

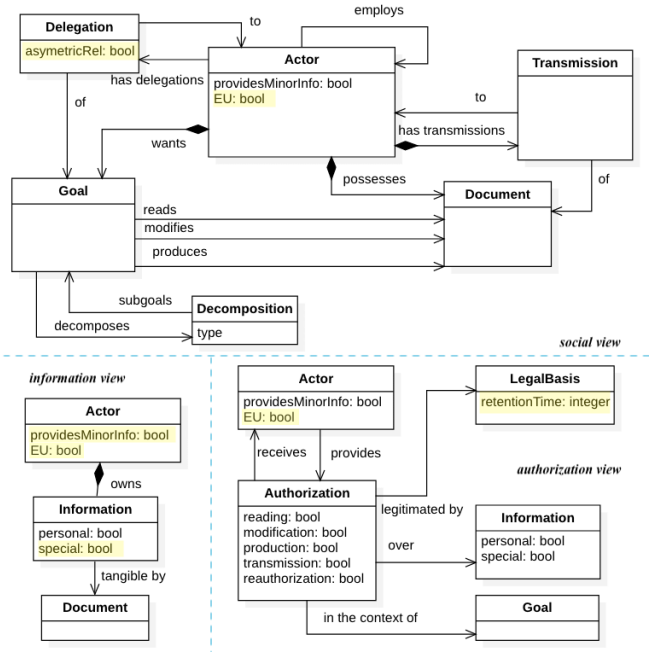

Fig. 1. Metamodel for the STS+GDPR modeling language extension, presented in [24]. This extension is called STAGE in this article.

analysis in the context of the early requirements stage of information systems development. As presented in Section 1, we focus on early stages of requirements engineering since it involves stakeholders from multiple areas, such as business analysts, data protection experts and software engineers [31], where the main conceptual modeling approach is goal oriented. Although different modeling frameworks have been proposed for to cover different requirement domains, we focus on the Socio-Technical Security method (STS) [8] and its extensions for GDPR compliance analysis [26,24].

The research questions of the study are:

RQ1 - How do the subjects interact to identify and discuss GDPR compliance risks exposed in STAGE's model?

RQ2 - What are the GDPR principles discussed? And how?

We address the research questions with a mixed methods approach as defined by Creswell, particularly a *concurrent embedded strategy* [7]. This approach is recommended to achieve a broader understanding of the phenomena under observation. One of the advantages of this strategy is that qualitative and quantitative data are collected simultaneously, allowing us to use the time of the professionals participating in the study better.

The data collection method is through a series of focus groups. The focus group's source data comes from the interaction of the participants in the activity [22]. Given that STAGE aims to facilitate stakeholders' communication of different backgrounds

to establish common ground over data protection requirements, a focus group is suitable to gather data on how STAGE is used for interaction [22]. Hence, for each focus group, we followed a triangulation approach, with subjects with different professional backgrounds and a moderator (that took a more or less structured approach guiding the discussion). Finally, [22] indicates that the number of focus groups necessary will depend on saturation levels, with a "rule of thumb" around four and six focus groups.

For analyzing the focus groups, we followed a deductive qualitative content analysis (CQDA) approach [11,17]. The idea of CQDA is to analyze data - verbal, written, audio, or in other forms - and classify the words into concepts or categories in a rather "flexible manner" [11,17]. The objective of content analysis is not just to "counting" words, but understanding and interpreting what is being said [17].

As content analysis deals with significant amounts of text and data, a coding process is done [11]. Consequently, codes and categories must be created for the coding process, which may be inductive or deductive, depending on the research objective [17,11]. As our research question is how STAGE can be used to discuss GDPR principles, our codes are defined on the seven GDPR principles [13]. This objective implies we followed a deductive approach, using previous theory or research [17]. Furthermore, in our coding process, we followed a manifest content analysis rather than a latent approach [11] (meaning non-verbal or underlying intentions of what was communicated).

Focus groups were recorded and transcribed with the subjects' consent. In addition, live annotation and modifications of the STAGE diagrams were produced for data gathering and transparency purposes. As previously mentioned, the codes used are based on the different GDPR principles. Figure 2 is an example of how different verbatims were coded as the first GDPR principle.

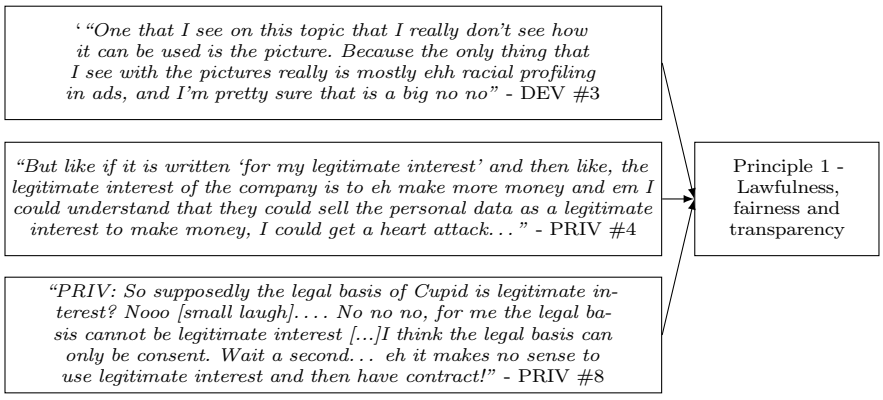

Fig. 2. Example of the content analysis procedure.

On the other hand, to complement the qualitative approach, we provide descriptive statistical analysis of the results to better characterize and support the discussion of the qualitative findings. The quantitative approach is used for describing the effectiveness of each focus group in terms of the number compliance risks identified. For

this, we noted down the background of the subject who identified the risk. Similarly, we measured how many of the GDPR principles were addressed during the analysis and by who, to provide further transparency of our qualitative approach.

3.2 Planning

Focus group details. Following Basili's template [4] the study's goal is *analyzing* IS stakeholders with different technical backgrounds, *for the purpose of* exploring how they interact and collaborate concerning the identification and discussion of GDPR compliance risks, *from the point of view of* data protection *in the context of* a meeting for reading socio-technical conceptual models of an IS.

We gathered volunteers online to form focus groups using purposive sampling. We published a survey online in different social media and selected the participants based on the characteristics we sought (expertise in development, business analysis, and data protection laws) [3]. As the objective is to analyze the interaction between subjects who have specific characteristics (context) with the usage of STAGE (artifacts), and if it can be used as an artifact to discuss privacy compliance requirements (effects), non-random sampling techniques can be used [29]. The aim is not to analyze causal mechanisms. The subjects are tagged according to their background as software developers (DEV), business analysts (BUS) and Privacy Experts (PRI), aiming for a three-people triangulation focus group.

Scenario and red flags. The participants are exposed to a real-life inspired case presenting the intention of a software-as-a-service company (named Cupid) of adding new features to its dating app for divorced adults with children. The new features are aimed to gather more data about their user base to provide better results and a targeted marketing campaign[5]. The scenario is introduced by a textual description, and further exposed through the social, information, and authorization view models using STAGE. The models describe the scenario, but they have been designed with seeded GDPR compliance risks (identified as "Red Flags") which should be identified and resolved using the STAGE model (check Table 1). We aimed to assess whether the participants could reason about the model to identify compliance issues (e.g. data for unlimited time), or inconsistencies in the model (e.g. unauthorized transferring rights).

Problem Red Flags (PRF) were introduced based on each new attribute of STAGE, plus re-using data for other purposes. PRF are GDPR compliance risks associated with the domain logic correctly modeled in the three views rather than issues with the models. On the other hand, Model Red Flags (MRFs) are semantic ambiguities caused by not using or misusing STAGE constructs; either not all attributes are identified, actors have rights that are not authorized, or the goals are not well specified, among others[6]. They were not systematically seeded. . Table 1 gives details on each red flag.

We presented the subjects with different models to address the research questions. The moderator told them that these models had red flags they needed to identify,

[5] The complete exercise is available here: `https://doi.org/10.5281/zenodo.7729512`.

[6] Due to space issues, the models are available online`https://doi.org/10.5281/zenodo.7729512`

from a data protection and modeling perspective. Thus, we asked them if they could see any issues. The moderator would re-guide the discussion into data protection requirements if it strayed too far from this aspect. Once the subjects discussed the compliance and modeling issues and agreed on these, we added annotations for each agreement in the STAGE diagrams and marked it as established common ground.

Focus groups stages. The overall design of the focus group considered five stages:

Stage 1 — Subjects Selection: We gathered the participants based on an online form, as already discussed, for focus groups of 45 minutes. Given that we were missing people with privacy backgrounds, we contacted some experts that we knew from the domain. The focus groups were done between a business analyst, a developer, and a privacy expert, for triangulation.

Stage 2 — Initial Survey and Method Training: We sent via e-mail an initial survey form to collect informed consent and demographics that may affect conceptual model understandability. We also provided a handout on the STS-ml language, presenting the three views. The handout covers a subset of the original STS-ml language constructs and all the STAGE constructs[7].

Stage 3 — Focus Group Execution: The main task of the focus group is to analyze an STAGE model to identify the red flags. The case describes a scenario where *Cupid*, a fictional dating app company focused on divorced people, wants to better characterize its users to implement targeted advertisement, as in described Section 3.2.

The execution of the focus group starts by presenting a short text describing the problem context, which does not reveal the potential issues, e.g., it does not detail that the data processor is non-eu. Then, the social, information, and authorization views are presented sequentially. The views were seeded with two types of red flags: Problem Red Flags (PRF) and Model Red Flags (MRF), which are explained in detail in Table 1 and in Section 3.2. The results of the identification of the MRF and PRF are presented in Table 4 and the percentage of how many red flags and how they were identified in Table 3. The materials of the focus group are available online[8].

Stage 4 — Final Survey: After the task, subjects were asked to fill out a survey on their perception of the usefulness, utility, and intention to use the method, according to the understandability framework of [10] and the questionnaire of [21].

To answer the research questions, we examined the video recordings and transcription of each focus group, the modifications done to the models, and the data about which participants identified the red flags and the GDPR principles during the sessions. Regarding the identification of red flags, we recorded who identified which red flag when a participant:

- Individually identified a red flag, marked as an "I";
- Collaboratively identified a red flag (i.e., the red flag was identified in an interaction between two or more participants) marked as an "IA";
- Agreed to a red flag identified by another participant marked as an "A"; and
- Did not agree to a red flag identified by another participant as a "D".

[7] On an anecdotal note, some subjects said at the end of the activity that they had not read the handout and were a little lost at the beginning of the activity.

[8] `https://doi.org/10.5281/zenodo.7729512`

View	Red Flag
Social	PRF1 - Non EU: Data from EU data subjects is transferred to a (fictional) Non EU data processor (NexCloud Co.).
Social	PRF2 - Asymmetric relationship: One of the data subjects (Employee) is in an asymmetric relationship with the data controller (Cupid).
Social	MRF1 - Ambiguous goals: The data controller collects data with a second purpose that is ambiguously modeled ("better know users").
Information	PRF3 - Minor Information: The data controller is requesting information to the data subject that might be from other data subjects which are minors ("data subject's children data").
Information	MRF2 - Special Category: Some data that could be special category of personal information (Pictures) is not labelled using the STAGE construct (S-P).
Information	MRF3 - Ambiguous information modeling: information about the data subject's children is ambiguously modeled ("children information").
Authorization	PRF4 - Using other goals: The data controller is transferring data to the data processor for a purpose that is not delegated by the data subject ("better know users").
Authorization	MRF4 - Transmission not Allowed: The data controller is transmitting data to the data processor even though the transmission is not allowed.
Authorization	PRF5 - Arguable Legal Basis: The data controller is using an arguable legal basis (Legitimate Interest) to collect data that should be authorized through consent.
Authorization	PRF6 - Unlimited Retention time: the data controller requires storing data for unlimited time.
Authorization	PRF7 - Using ambiguous goal for auth: The data controller is transmitting information using an ambiguously defined goal ("better know users")

Table 1. Red flags seeded in the focus group problem.

The record is presented in Table 4. Based on the record, we defined the metrics, detailed in table 3. Figure 3 is an example on how we recorded a red flag as collaboratively identified (IA), individual identified (I), and agreed (A) for PRF and MRF.

- Group Effectiveness (GE): the percentage of identified red flags of the total number of seeded red flags.
- Group Collaboration (GC): the percentage of red flags identified jointly by two or more participants from the total number of seeded red flags.
- Contribution (C): The percentage of red flags identified by a participant from the total identified by the group, whether they were agreed upon or not by the rest.
- Agreement (A): The percentage of red flags to which the participant agrees were identified by another participant (s) from the group's identified red flags.
- Disagreement (D): The percentage of red flags identified by a participant to which the rest does not agree from the total of red flags identified by the group.

3.3 Conducting

The focus groups were conducted through the Zoom platform between October 2022 and February 2023. We organized 8 focus groups — achieving high levels of saturation

"**DEV:** Two things, the first, is eh on the information that the customer gives Cupid... the T is not marked there. But then I understand that they give it with the authorized goal, with is the potential dating partner met, they then just use it for something else.... (... PRI presented connected issues) **DEV:** That it is... it is like it is violating the agreement because as I say, I give you data for this and then you use it for what you want. And I didn't authorize you for what you are doing with the data originally.
Moderator: A little bit of what PRI#4 was saying about the authorization?
PRI: Ah yes, I didn't see that what DEV#4 was saying, it makes sense... [...] well what do you do with those profiles?"

Fig. 3. Quote translated from Spanish on Group #4 agreement and identification on PRF4 and MRF4 . PRF7 was only identified by DEV#4 but not agreed upon by the others.

[22] — where none of the subjects was familiar with the dating app scenario — meaning, none of them had or was working in a company with such a business model. Each focus group lasted 45 - 70 minutes, depending on the subject's interest [9].

We gathered a total number of 21 participants, which is a similar number of participants as other studies [27,20]. Participants' ages ranged from 28 to 46, all of them professionals with at least four years of experience in information system projects, as business analyst (BUS), developers (DEV) or privacy experts (PRI). Their experience working with GDPR ranged from zero to more than ten years. Participants were classified according to their professional background into three categories. Eight participants were classified as DEV, though their current professional roles were varied (software architects, software development researchers, and actual developers). Seven participants were classified as PRI, having current professional roles such as Data Protection Officers (DPO) and/or privacy researchers. Six participants were classified as BUS accordingly to their current professional roles.

In groups 1 and 5, the BUS did not attend the activity. In group 7, the PRI did not attend. In group 2, the BUS participated in the surveys but did not speak during the activity, although requested, so we do not include the its results. In group 8, the DEV would only wonder why we did not use UML and did not discuss data protection.

To control if the subjects knew about modeling languages and data protection, we asked for these issues. Table 2 shows how nine subjects knew about modeling, four answering UML. Regarding data protection, we asked to identify the definition of personal data through multiple questions and list out the principles of the GDPR. All PRI subjects identified the principles, but the other subjects did not. Everybody gave the correct answer regarding personal data, except two BUS.

During the focus groups, we modified live the different model views by writing the identified red flags to ensure the agreement and shared understanding of all the participants. Hence, one of the authors acted as moderator, which took a structured approach and guided the discussion into data protection requirements, and wrote down in red in the models the agreed-upon red flags, desired modifications, and interesting questions brought up by the subjects. These modifications are published online [10].

[9] Some subjects contacted us even after the focus groups to continue discussing STAGE
[10] `https://doi.org/10.5281/zenodo.7729512`

4 Results and Discussion

Question/Answer	Yes	No	I don't know
Do you know modeling? Which?	9	8	3
Are you familiar with goal modeling?	2	13	5
Are you familiar with STS-ml?	1	12	7

Table 2. Modeling knowledge answers

The focus group results are summarized in Table 4. At a high level, we have identified that STAGE allowed the different subjects to identify most of the privacy risks in the model, discuss the GDPR principles, and agree on them. Furthermore, the subjects were able to reason about these topics, even with little domain or modeling knowledge.

4.1 RQ1 - How do the subjects interact to identify and discuss GDPR compliance risks exposed in STAGE's model?

Qualitative Analysis. To answer RQ1, we performed a content analysis of the focus group. We defined "interactions" as the statements made by the participants aiming to achieve common ground on what are the red flags. We found three ways of interactions which we named as "identification" (statements made by a subject to explicit a red flag, without further interaction of other participants), "identification and agreement", made by two or more subjects that collaboratively identified a red flag, and "agreement", statements, made by participants that just agreed to a red flag identified by another participant without providing further comments. The results are summarized in Table 3, based on what was presented in Section 3. The data is presented and discussed according to the subjects' backgrounds: Privacy experts (PRI), software developers (DEV), and business analysts (BUS). Based on these results, next we comment on group effectiveness, group collaboration, problem and model red flags, and on interdisciplinary aspects of the results.

Group Effectiveness. As an overview, all groups found at least 50% of the implanted red flags, and six of them at least 80% of the red flags, as seen in Tables 3 and 4. Although the sample size is not statistically significant, as this is an exploratory study [24], specific trends can be noticed and analyzed without statistically significant samples [29], as discussed in Section 3. Thus, these preliminary results suggest that STAGE was effective in helping subjects identify and discussing GDPR compliance risks and requirements.

In all groups, PRI subjects identified most of the PRF, except in group 4, where the DEV identified most red flags, and group 7, where the PRI subject did not arrive, as seen in table 4 [11]. In group 7, where the PRI subject was missing, the group struggled to find some red flags and even questioned if certain elements were part of the GDPR. However, they asked the moderator questions about data protection. This questions appears as both BUS and DEV of group 7 do not possess much knowledge of the GDPR, as screened in the domain knowledge questionnaire.

[11] DEV of group 4 contributed significantly more than others, as it has a sound knowledge of goal modeling and could be treated as an atypical case.

Group	GE	GC	Role	C	A	D
1	82%	22%	DEV	30%	40%	10%
			PRI	50%	20%	10%
			BUS	-	-	-
2	55%	17%	DEV	17%	50%	0%
			PRI	67%	33%	17%
			BUS	-	-	-
3	100%	45%	DEV	9%	55%	0%
			PRI	18%	36%	0%
			BUS	27%	55%	0%
4	100%	18%	DEV	55%	27%	18%
			PRI	18%	45%	0%
			BUS	9%	55%	9%
5	91%	30%	DEV	20%	50%	10%
			PRI	50%	0%	0%
			BUS	-	-	-
6	100%	73%	DEV	9%	9%	0 %
			PRI	9%	0 %	9%
			BUS	18%	0%	9%
7	64%	14%	DEV	43%	0%	29%
			PRI	-	-	-
			BUS	29%	0%	29%
8	100%	55%	DEV	0%	0%	0%
			PRI	45%	0%	0%
			BUS	0%	0%	27%

Table 3. Results for red flag identification metrics per group and subject background, as defined in section 3.2.

Given that, in most cases, the PRI subject identified most of the PRF and led the discussion, we believe this situation supports the idea that PRI subjects could understand and reason about privacy risks using STAGE's model. None of the PRI and BUS subjects had prior knowledge about conceptual modeling, but PRI subjects outperformed DEV subjects in identifying the problem red flags. In fact, for the PRI subject of group 8, the difference between agent and role was evident. In group 4, there was an exception: the DEV participant outperformed PRI and BUS. This could be explained because the DEV has previous knowledge in conceptual modeling, which has been identified in previous works on business process modeling as positively affecting model understandability [10].

Group Collaboration. On another topic, Table 3 shows that groups—specifically groups 2, 6, and 8—that have high group collaboration (GC as seen in Section 3.2) have also identified 100% of the red flags (GE, group efficiency, revise Table 3). In particular, this refers were efficient in collaboration when identifying red flags, having GC indicators of 45% or higher. This indicates that STAGE seems to help with group collaboration and communication on GDPR requirements discussion.

However, other groups that do not have high GC (such as group 4) also recognized 100% of the red flags. Even so, as previously explained, group 4 DEV had an exceptionally high understanding of modeling, which could help explain why this group, with such a low level of GC, could recognize all the red flags. In addition, group 5 had a GC of 30% and identified 91% of the red flags. Future research could compare statistically how the different groups behave over these indicators.

Problem and Model Red Flags. In most cases, all the subjects agreed to the red flags identified by others, as seen in Table 3. Since PRI identified most of the problem red flags (PRF), DEV and BUS agreed. Indeed, once the PRF were identified and explained by a PRI, the rest of the participants would add more details and arguments as to why such a element was a risk. A possible explanation could be due to a "maturation", this is, subjects improve their performance during the study because they learned something [29]. This guides us to think that using STAGE could also help BUSs and DEVs learn about privacy when reviewing models with a PRI.

Focus group	Individual	Identification Problem Red Flag							Identification Model Red Flag				Discussion of GDPR principles							Understandability		
		F1	F2	F3	F4	F5	F6	F7	F1	F2	F3	F4	1	2	3	4	5	6	7	PEU	PU	IU
	PRI	IA	IA	IA	A	IA	IA		I	IA		A		✓	✓		✓		✓	15	30	7
1	DEV	A	A	IA	IA	A	IA	I		A		IA	✓		✓		✓	✓		14	33	5
	BUS*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	PRI	A	IA			IA	IA			IA	I		✓	✓	✓		✓		✓	23	32	7
2	DEV	IA	A			A	A			IA			✓	✓	✓		✓	✓	✓	21	31	9
	BUS†	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	PRI	IA	IA	A	A	IA	IA	IA	A	IA	A	IA	✓	✓	✓		✓	✓	✓	21	31	9
3	DEV	IA	IA	A	A	A	IA	A	A	A	A	IA	✓	✓	✓	✓	✓	✓	✓	24	25	7
	BUS	IA	A	IA	IA	A	A	IA	IA	A	IA	A	✓	✓				✓	✓	25	34	7
	PRI	IA	A	IA	A	IA	A			A		A	✓	✓	✓	✓		✓	✓	21	24	7
4	DEV	A	IA	A	IA	A	IA	I		IA	I	IA	✓	✓	✓		✓	✓	✓	23	32	9
	BUS	A	A	IA	A	A	A		I	A		IA	✓		✓				✓	23	35	8
	PRI		IA		IA	IA	IA	IA	IA	IA	IA		✓	✓	✓		✓		✓	19	27	6
5	DEV		A	IA	A	A	IA	IA	A	IA	A	I	✓		✓		✓	✓	✓	23	33	9
	BUS*	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	PRI	IA	IA		IA	IA	IA	IA	I	IA			✓	✓	✓		✓	✓	✓	15	28	6
6	DEV	IA		IA	IA	IA	IA	IA		A	I		✓	✓			✓		✓	22	31	5
	BUS	A	IA	IA	IA	IA	IA	A		IA		I	✓	✓	✓		✓	✓		n/a	n/a	n/a
	PRI*	-	-	-		-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
7	DEV	IA	A				IA		I	A		I			✓			✓		n/a	n/a	n/a
	BUS	A	IA		I		IA			IA				✓	✓		✓	✓		18	24	6
	PRI	I	IA	IA	IA	I	IA	IA	IA	IA	I	IA	✓	✓	✓		✓	✓	✓	n/a	n/a	n/a
8	DEV																			13	27	5
	BUS	A	IA	IA	A		IA	A	IA	IA		IA	✓	✓	✓		✓	✓	✓	15	18	2
	PRI																			20	30,29	7
Avrg.	DEV																			19	28,67	7
	BUS																			20,25	27,75	5,75

Table 4. Table representing the identified red flags in the model, the GDPR principles discussed and the understandabilities scores. */†: resp. did not attend/participate
IA = Identified and agree, A = Agreed, I = identified, as presented in Section 3.2. Understandability scores explained in Section 2

> *"**PRI:** Is all that data necessary to do the marketing profile? [Group laughs]*
> ***Moderator:** What do you think?*
> ***PRI:** honestly, no [laughs] [...] The sexual orientation data might be complicated for marketing and I don't really know why they need it for targeting for people. Pf... I don't know, maybe they need it for toys? [...]*
> ***DEV:** One that I see on this topic that I really don't see how it can be used is the picture. Because the only thing that I see with the pictures really is mostly ehh racial profiling in ads, and I'm pretty sure that is a big no no ... but yeah I find this very flimsy"*

Fig. 4. Verbatim focus group 3, coded as discussing the GDPR principles of data minimization and lawfulness, fairness and transparency

Alternatively, model red flags (MRF) were less consistently identified by the subjects. Only group 3 could identify and agree upon all the MRFs. Groups 5, 6, and 8 also identified all the MRFs; however, the other participants agreed only with some. The MRF generally sparked less discussion between the subjects when reviewing the recordings and model modifications. Most subjects would agree upon identified MRF and would not generate discussion. The exception to this situation is group 8, which, although it did not identify all MRFs, did have a rich debate over the ones identified.

Interdisciplinary Aspects. The results in Table 3 show that, except for group 5, groups with the three disciplines were highly effective in identifying the red flags. Groups 2 and 7 identified only 55% and 64% of the red flags, respectively. Although a PRI was present in group 2— playing the role of domain expert — with a DEV, most of their remarks were on presentation elements of the model (such as colors) than the data protection requirements. Even though the moderator tried guiding them into more data protection topics, they focused on design elements. While in group 7, they asked and requested the moderator to act as a privacy expert, given their data protection misconceptions and struggled to identify MRF. Both of these situations highlight the importance of the interdisciplinary approach for discussing GDPR compliance and the importance of having a triangulation in STAGE for its successfulness.

As a result, looking at the group results and our analysis, we see that the groups with three subjects (DEV, PRI, and BUS) were the only ones that identified all the seeded red flags and had proper discussions about them. It seems the groups achieved synergy in identifying red flags when discussing STAGE models. Moreover, groups 3, 6, and 8 had the higher proportion of red flags identified by collaboration as shown in Table 3; i.e., the group identified the red flags and not by a single subject. Although the number of participants and focus groups offer exploratory and preliminary results, it does show a trend that might be interesting to look at in the future.

To summarize the answer to RQ1, subjects use the STAGE's models as prompts to discuss data protection requirements. Subjects would identify a compliance risk to the group depending on their background. Afterward, the other subjects would either (1) agree/disagree on the identification and complement with information depending on their expertise; (2) agree/disagree without adding extra information; (3) not interact at all. Most of the interactions we saw fall under the first category, which is a promising result.

4.2 RQ2 - What are the GDPR principles discussed? And how?

Qualitative Analysis. As previously exemplified in Figure 2, we analyzed each participant's interventions to identify whether they were talking about a GDPR principle. The results are shown in the column "Discussion of GDPR principles" in table 4.

GDPR Principles. Most GDPR principles were discussed in all focus groups, with all groups discussing at least six principles. Only "accuracy" was not systematically discussed, as seen in table 4, with one DEV and PRI sharing their preoccupation in groups 3 and 4. This principle might not have appeared so frequently in the discussion because there is no clear primitive in [24,26] about it, except for "Retention Time".

All focus groups and participants (except one) showed interactions that were coded under principles 1, 3, and 7. Principle 1, lawfulness, fairness, and transparency, is one of the important values behind the GDPR [13]. Therefore, it is not surprising that most subjects discussed this topic. This principle is closely related to PRF2, PRF4-5, PRF7 and MRF1. Usually, the topic would appear when discussing the asymmetrical relationship between the employee/employer, the re-purposing of personal data and the legal basis for data processing. To illustrate, PRF2 was identified mainly by PRIs, but when highlighted, some DEVs would raise the concern that fairness and

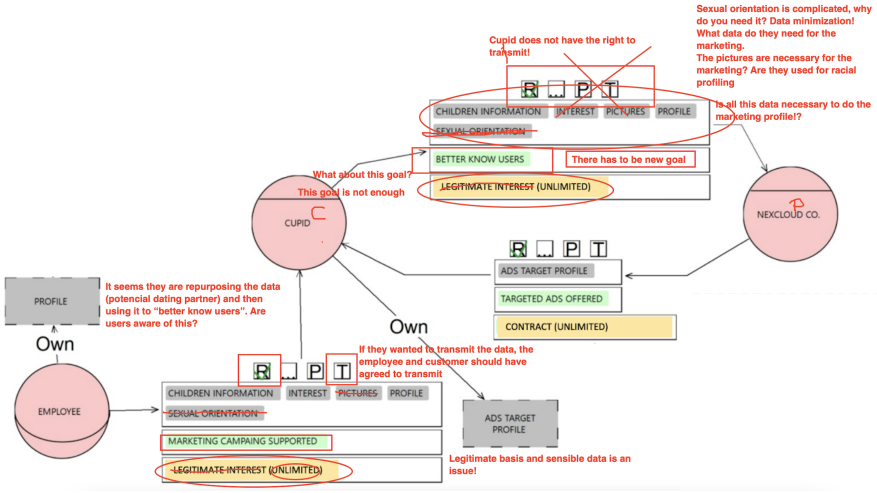

Fig. 5. Original model, with annotations in red of the modifications of Group 3. Other model modification are available online, at https://doi.org/10.5281/zenodo.7729512.

asymmetry were not part of data protection principles. We saw this situation, for example, in groups 1, 2, and 5. In group 1, the DEV thought that an "asymmetrical" relationship referred to the actors' geographical location; in groups 2 and 5, the DEV did not know this was a requirement. What happened next was that PRIs would explain the GDPR and the logic behind the asymmetrical relationship. DEVs would either nod or acknowledge that they did not know that and agree it is a red flag.

Principle 1 also appear between PRIs, when discussing the legal basis of "legitimate interest". For example, verbatim of PRI#4 in the authorization view *"legitimate interest is nowadays abused for everything and not everything is legitimate interest. I think it is too much, um unfair, to use..."*. Alternatively, verbatim PRI#3 *"It is complicated to use that legal basis, every time, everywhere..."*. Or the verbatim of PRI of groups 4 and 5 (Figure 2) show how principle 1 appeared in the discussions. This principle would also appear in the discussion during the authorization and social views regarding the re-purposing of data and the lack of transparency from the company. Fairness was also discussed regarding using minors' information for marketing.

The subjects would also discuss principle 3, data minimization. This discussion happened on the information and authorization view. Several subjects would question the amount and type of data used for marketing. They even highlighted that the information "interest" could be special categories of data. Data minimization was also discussed in the authorization view, as subjects could relate the amount of information used to a specific goal, illustrated in Figure 4. Finally, most subjects would talk about accountability. Accountability is the GDPR principle that sums up all the other values, as it implies holding organization accountable for their practices [24]. To summarize the answer to RQ2, we could say that STAGE allowed the subjects

to discuss the GDPR principles, even without proper knowledge. The principle of accuracy is lacking in the discussions, which could be addressed in future work.

4.3 Overall discussion

Overall, the STAGE extension was conceived the GDPR and its regulator(s) have interpreted as vital. This design decision is reflected by the fact that PRIs could understand the models, as they are the domain experts. This could explain why it seems that for PRIs it was not complex to contribute to the discussion, even without knowledge of modeling. Although it may seem "intuitive" or "common knowledge" that PRIs should always find the PRF regardless of the communication medium, this research provides empirical evidence for this assumption. This observation provides evidence on the importance of interdisciplinary reasoning when creating artifacts for multiple stakeholders. Indeed, privacy experts could identify and discuss MRF, implying that STAGE was understandable enough that they could reason about conceptual modeling. Therefore, even if they did not know modeling, they could deduce information from the different views, identify most red flags and participate.

Another focus group finding shows that subjects could extract information from the models and discuss compliance without fully understanding the model's complexity. Seven out of eight groups identified at least 80% of the red flags (as seen in Table 3) hinting that an intuitive and understandable artifact could facilitate communication and establish common ground. Furthermore, given the interdisciplinary reasoning behind STAGE, groups composed of PRI, BUS, and DEV seem to outperform in finding red flags, having richer discussions on GDPR compliance requirements. These observations allow us to deduce that conceptual models can help interdisciplinary teams discuss and analyze regulatory requirements with different mental models.

5 Threats to validity analysis

Concerning threats to internal validity we think that one threat is about subject selection: the participants were recruited purposive, though they were randomly grouped. Furthermore, there was no control over the subjects' years of experience. The study's objective is not to produce statistical nor conclusive results but to validate a proposal through analogical inference [28]; this situation can be tolerated but acknowledged nonetheless.

Regarding the construct validity, whether the study is representative of the theory constructs, we think that the activity and the measurements are consistent with our focus on the collaboration of the subjects around STAGE models from the perspective of cognitive contribution to problem-solving. However, other variables could help study collaboration, such as participants' nonverbal and paraverbal cues. Using different cases would be helpful to discard the effect of the problem on the results. However, it would require more groups to get to the comparative results per role we presented in the article. Finally, it is impossible to generalize the study's conclusions about external and conclusion validity. However, this does not diminish the value of the empirical insights towards the evolution of the proposal.

6 Related work

Many initiatives have extended the capabilities of existing modeling languages to address privacy and data protection requirements. In [23], proposed Secure Tropos, a modeling language based on Tropos, to address security requirements in the early requirements stage. The extension allowed users to tag dependencies and entities and added the threat concept. [14] have proposed an automated approach to deal with NL requirements that can detect ambiguities and interpret them. [18] presents Nòmos 3, a continuation of Nòmos2 modeling language, which is "a modeling language for law". Nòmos3 seeks to model roles and responsibilities and analyze compliance through the modeling [18]. Legal GRL [15] is a method proposed to systematically extract legal requirements from regulations. Using the Hohfelding model to extract these requirements, then requirements can be modeled with Legal GRL, which is goal-oriented with deontic modalities language. In [2], present a UML profile for privacy-aware data lifecycle models. The UML profile proposes stereotypes for an eight-step data life cycle and activities and events affecting the data.

Other proposals have sought to include GDPR requirements in their modeling frameworks. In [1], propose a set of business process modeling patterns to model GDPR constraints. The article presents BPMN models representing the behaviors needed to address data breaches, data use consent, right of portability, and rights to access, withdraw, rectify, and be forgotten. In [19], the authors extend use and misuse cases models by introducing templates for specifying misuse cases and mitigation actions. In [30], LINDUUN GO— based on LINDDUN, a privacy threat modeling framework — extension is proposed, which is a lightweight and gamified approach, which also includes a GDPR data subjects rights, but the GDPR principles [30].

Nevertheless, even with all these frameworks, artifacts, tools, and proposals for dealing with regulatory requirements ambiguity and analysis, it still needs to tackle the challenge of specific knowledge in law and software engineering [5]. Lately, [5] have proposed the creation of a new type of quality requirement, namely Legal Accountability. This new requirement would measure legal traceability, completeness, validity, auditability, and continuity [5]. Furthermore, [5] indicates that regulatory requirements are still not properly included in the design, and technical and legal divisions compete. Hence, tools and methods for cooperation are required [5]. STAGE seeks to address this identified gap by helping establish "common ground" between interdisciplinary teams, an essential element for software development [9] and helping with interdisciplinary approaches [5].

7 Conclusions and future work

Through focus groups, we aimed to validate the usage of STAGE extension of the STS-ml [24], as an artifact to analyze and discuss privacy compliance between stakeholders with different privacy backgrounds. Our preliminary data show that STAGE allowed the stakeholders to identify privacy risks, discuss the GDPR principles, and act as a communication tool. These preliminary results are promising, as data protection requirements are not usually included in the early stage of the software development

lifecycle. STAGE could prompt discussion between interdisciplinary teams, helping IS comply with data protection regulations, such as the GDPR.

Although they had little to no knowledge of modeling, privacy experts identified most of the privacy risks and contributed to the discussion. Developers could also identify privacy risks and, when in disagreement with privacy experts relating to privacy requirements - such as asymmetric relationships - could resolve their doubts and agree on the technicalities of this conflicting requirement. Furthermore, even despite the models' complexity, the stakeholders together were able to extract information from the models to check compliance. These results provide preliminary and exploratory evidence on the role of STAGE models as a facilitator for stakeholders with different backgrounds to analyze privacy compliance in the organization. These results provide preliminary and exploratory evidence on the role of STAGE models as a facilitator for stakeholders with different backgrounds to analyze privacy compliance in the organization. Moreover, the results provide new insights into how stakeholders with different backgrounds interact with and discuss around conceptual models. Future research will focus on the experimental validation of the proposal with a larger sample and statistical analysis of the results.

References

1. Agostinelli, S., Maggi, F.M., Marrella, A., Sapio, F.: Achieving gdpr compliance of bpmn process models. In: International Conference on Advanced Information Systems Engineering. pp. 10–22. Springer (2019)
2. Alshammari, M., Simpson, A.: A uml profile for privacy-aware data lifecycle models. In: Computer Security, pp. 189–209. Springer (2017)
3. Babbie, E.R.: The practice of social research. Cengage learning (2020)
4. Basili, V.R., Rombach, H.D.: The tame project: Towards improvement-oriented software environments. IEEE Transactions on software engineering **14**(6) (1988)
5. Breaux, T., Norton, T.: Legal accountability as software quality: A u.s. data processing perspective. In: 2022 IEEE 30th International Requirements Engineering Conference (RE). IEEE (2022)
6. Breaux, T.D., Antón, A.I.: A systematic method for acquiring regulatory requirements: A frame-based approach. RHAS-6), Delhi, India (2007)
7. Creswell, J.W., Creswell, J.D.: Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications (2017)
8. Dalpiaz, F., Paja, E., Giorgini, P.: Security requirements engineering: designing secure socio-technical systems. Cambridge, Massachusetts (2016)
9. Damian, D., Chisan, J.: An empirical study of the complex relationships between requirements engineering processes and other processes that lead to payoffs in productivity, quality, and risk management. IEEE Trans. Software Eng. **32**, 433–453 (07 2006). https://doi.org/10.1109/TSE.2006.61
10. Dikici, A., Turetken, O., Demirors, O.: Factors influencing the understandability of process models: A systematic literature review. Information and Software Technology pp. 112–129 (2018)
11. Elo, S., Kyngäs, H.: The qualitative content analysis. Journal of advanced nursing **62**, 107–15 (05 2008). https://doi.org/10.1111/j.1365-2648.2007.04569.x
12. European Union: Charter of Fundamental Rights (2000), Article 8

13. European Union: Regulation (EU) 2016/678 of the European Parliament and of the Council - General Data Protection Regulation (2016)
14. Ezzini, S., Abualhaija, S., Arora, C., Sabetzadeh, M., Briand, L.C.: Using domain-specific corpora for improved handling of ambiguity in requirements. In: 2021 IEEE/ACM 43rd International Conference on Software Engineering (ICSE). pp. 1485–1497. IEEE (2021)
15. Ghanavati, S., Amyot, D., Rifaut, A.: Legal goal-oriented requirement language (legal grl) for modeling regulations. In: Proceedings of the 6th international workshop on modeling in software engineering. pp. 1–6 (2014)
16. Hadar, I., Hasson, T., Ayalon, O., Toch, E., Birnhack, M., Sherman, S., Balissa, A.: Privacy by designers: Software developers' privacy mindset. In: Proceedings of the 40th International Conference on Software Engineering, Gothenburg, Sweden. ICSE '18, Association for Computing Machinery, New York, NY, USA (2018)
17. Hsieh, H.F., Shannon, S.E.: Three approaches to qualitative content analysis. Qualitative health research **15**(9), 1277–1288 (2005)
18. Ingolfo, S., Jureta, I., Siena, A., Perini, A., Susi, A.: Nomos 3: Legal compliance of roles and requirements. In: International Conference on Conceptual Modeling. pp. 275–288. Springer (2014)
19. Mai, P.X., Goknil, A., Shar, L.K., Pastore, F., Briand, L.C., Shaame, S.: Modeling security and privacy requirements: a use case-driven approach. Information and Software Technology **100**, 165–182 (2018)
20. Mendling, J., Recker, J., Reijers, H.A., Leopold, H.: An Empirical Review of the Connection Between Model Viewer Characteristics and the Comprehension of Conceptual Process Models. Information Systems Frontiers **21** (2019)
21. Moody, D.L.: The method evaluation model: a theoretical model for validating information systems design methods. In: Proceedings of the European Conference on Information Systems 2003. pp. 1–17. AIS Electronic Library (2003)
22. Morgan, D.L.: Focus groups. Annual review of sociology **22**(1), 129–152 (1996)
23. Mouratidis, H., Giorgini, P.: Secure tropos: a security-oriented extension of the tropos methodology. International Journal of Software Engineering and Knowledge Engineering **17**(02), 285–309 (2007)
24. Negri-Ribalta, C., Noel, R., Herbaut, N., Pastor, O., Salinesi, C.: Socio-technical modelling for gdpr principles: an extension for the sts-ml. In: 2022 IEEE 30th International Requirements Engineering Conference Workshops (REW) (2022)
25. Paja, E., Dalpiaz, F., Poggianella, M., Roberti, P., Giorgini, P.: Sts-tool: socio-technical security requirements through social commitments. In: 2012 20th IEEE International Requirements Engineering Conference (RE). IEEE (2012)
26. Robol, M., Salnitri, M., Giorgini, P.: Toward gdpr-compliant socio-technical systems: modeling language and reasoning framework. In: IFIP Working Conference on The Practice of Enterprise Modeling. pp. 236–250. Springer (2017)
27. Stitzlein, C., Sanderson, P., Indulska, M.: Understanding healthcare processes. Proceedings of the Human Factors and Ergonomics Society Annual Meeting **57**, 240–244 (09 2013). https://doi.org/10.1177/1541931213571053
28. Wieringa, R.: Empirical research methods for technology validation: Scaling up to practice. Journal of systems and software **95**, 19–31 (2014)
29. Wieringa, R.J.: Design science methodology for information systems and software engineering. Springer, Berlin, Heidelberg (2014)
30. Wuyts, K., Sion, L., Joosen, W.: Linddun go: A lightweight approach to privacy threat modeling. IEEE (2020)
31. Yu, E.: Modeling strategic relationships for process reengineering. Social Modeling for Requirements Engineering **11**(2011), 66–87 (2011)