Exploring Understandability in Socio-Technical Models for Data Protection Analysis: Results from a Focus Group*

Rosa Velasquez[1], Claudia Negri-Ribalta[2], Rene Noel[1,3], and Oscar Pastor[1]

[1] Valencian Research Institute for Artificial Intelligence, Universitat Politècnica de València, València, Spain, rvelasquez,rnoel@vrain.upv.es
[2] SnT, University of Luxembourg, Luxembourg
[3] Escuela de Ingeniería Informática, Universidad de Valparaíso, Chile

Abstract. The understandability of conceptual models depends not only on the model's inner complexity and representation but also on the personal factors of the model's audience. This is critical when conceptual models are used for achieving common ground during the early stages of requirements engineering for information systems and, moreover, for complex domains such as data protection. In this article, we present the results of an exploratory study consisting of eight focus groups with 21 experts on software development, business analysis and data protection, examining socio-technical models of an information system to identify privacy risks. We surveyed participants on their backgrounds to characterize the personal factors of understandability and performed an initial understandability assessment on a socio-technical model. We compared these values with the outcome of the focus group, i.e., the effectiveness of the participants in identifying privacy risks, annotating whether the risks are identified individually by a participant or collaboratively by two or more participants. The results suggest that most of the privacy risks were identified collaboratively, regardless of the previous understandability scores and personal factors such as experience and background.

Keywords: understandability · requirements engineering · conceptual model quality.

1 Introduction

Understandability is a critical quality attribute in conceptual modeling, as stakeholders need to understand the conceptual model to deliver and convey their message effectively [8, 4]. Misunderstandings and syntactical errors may occur, affecting the efficiency and usage of artifacts [8]. Previous research has recognized that model and personal factors affect the understandability of artifacts, such as education, practice, or professional background [14, 4]. The differences in how different backgrounds affect the understandability of models could be critical

* This article present some partial results of Negri-Ribalta's PhD thesis

when stakeholders seek to achieve common ground on privacy. This paper focuses on privacy and data protection requirements. On the one hand, privacy experts are specialists in data protection but may not be familiar with modeling, while developers may be familiar with modeling but lack domain expertise.

From a requirements engineering (RE) perspective, data protection requirements should be elicited from the early phases of the software development life cycle [1, 6]. However, different studies have shown that data protection requirements are not elicited nor analyzed in early phases [1]. Furthermore, software engineers have difficulties understanding and analyzing these, given their mental model and knowledge, complicating collaborative processes and communication [6, 1].

This paper aims to explore the relationship between the stakeholders' personal factors and their effectiveness in eliciting regulatory data protection requirements in a collaborative setting. We conducted eight focus groups with 21 privacy (PRI), business analysis (BUS), and software development (DEV) experts. The participants were asked to elicit privacy risk from a conceptual model based on the Socio-Technical Security modeling language (STS-ml) [2], extended to address GDPR principles by the STAGE language [11]. We previously and individually tested whether the participants could understand a model similar to what was collaboratively discussed in the focus group. We measured the participants' effectiveness in identifying privacy risks during the focus group and their perception of the understandability of the models.

Our results suggest that privacy experts had the highest performance, even though their scores in the understandability pretests were low understandability. However, the privacy experts did not identify most privacy risks individually but collaboratively with business and software development experts. We think the insight of this exploratory study could be relevant for further research on the social factors of understandability of conceptual models in the context of such models being a communication mean among team members.

This article is structured as follows: in Section 2, we review empirical studies on the understandability of conceptual models. The research method is explained in Section 3. The results are presented and discussed in Section 4, and the conclusions are presented in Section 5.

2 Related Work

Understandability is the ability of the stakeholder to comprehend, extract information and infer specific elements from a model [8, 4, 5, 15]. To give one precise definition, [4] describes understandability as "... typically associated with the ease of use and the effort required for reading and correctly interpreting a process model". Yet, there are a variety of models on understandability, each evaluating and analyzing different variables [14]. Given this situation, [8] gathered different approaches to understandability available and provided a unified model. Nevertheless, it is still a stretched and flexible concept.

Understandability depends on various factors, including model characteristics and personal variables [15, 4]. For instance, [15] distinguishes between "model

factors" (related to the model itself, like density and structure) and "personal factors" (related to the reader). This distinction is also discussed by [4], who includes modeling notation, complexity, modularity, approach, visual layout, and coloring as process model factors. Both process model and personal factors influence understandability, though not necessarily perceived understandability [4]. Empirical personal factors include theoretical knowledge, practice, education [15], as well as learning style, motive, cognitive abilities, professional background, and domain familiarity, among others [4].

Previous work has measured if there were significant differences in understanding BPMN and HPN between subjects of health science background and engineers [17]. The study concluded that there seems to be a statistical difference in some aspects of understandability [17]. From a RE perspective, [7] compared the comprehensibility of Tropos versus Use Case (UC), concluding that Tropos was more comprehensible but at the trade-off of higher time consumption. Research on the personal factors of understandability has focused on how individuals process conceptual models, using eye-tracking technologies [20, 13] or by exploring the mental models of the audience [9]. These initiatives provide a deep understanding of the context of users reading models individually, which might be valuable when models are used for documentation or code generation purposes.

However, mainly in agile software development contexts, models are used to collaborate among the members of cross-disciplinary teams [16]. In collaborative contexts, models are used to achieve "common ground" between interdisciplinary teams[3]. Common ground can be understood as "establish and achieve shared goals" [18]. Regardless of the agility of the methodology, common ground is relevant in requirements engineering since it "aims to establish a common ground of shared understanding between users and software engineers" [18].

3 Research method

This article presents partial results of a larger study that analyses how participants interact around conceptual models from an interdisciplinary perspective for regulatory data protection requirements. The models reviewed and the data collected are available online[4].

3.1 Research Questions and Approach

We define the research goal following the recommendation by [21]: Analyze *socio-technical requirement models* for the purpose of *exploring the relationships of personal understandability factors* concerning *the objective and subjective understandability* of the models from the perspective of the *researcher* within the context of *stakeholders with diverse backgrounds collaboratively performing an understandability task focused on identifying privacy risks in the socio-technical models.* Using Dikici's quality framework [4], we study risk identification's *effectiveness*

[4] https://zenodo.org/record/7729512

for objective understandability and participants *perception* for subjective understandability. To address the research goal, we formulate three research questions:

- ***RQ1:*** What is the relationship between the personal factors of understandability and the understandability task effectiveness of subjects with different backgrounds collaboratively identifying privacy risk in socio-technical requirement models?
- ***RQ2:*** What is the relationship between the understandability score of a single subject and the understandability task effectiveness of subjects with different backgrounds collaboratively identifying privacy risk in socio-technical requirement models?
- ***RQ3:*** What is the relationship between the understandability task effectiveness and the perceived understandability of subjects with different backgrounds collaboratively identifying privacy risk in socio-technical requirement models?

The questions were explored through focus groups, where participants were given tasks through which we measured their understandability and explanation. We qualitatively analyzed participant interventions to detect when the privacy risk was identified individually or collaboratively.

3.2 Measurement Design

We define the variables and metrics detailed below to explore the relationship between understandability and the collaborative identification of privacy risks.

Initial Understandability: An online quiz assessed participants' initial understandability before the collaborative task. The quiz included six true or false questions about a simple, well-formed STAGE model to gauge their ability to extract basic information. The metric for this variable is *Initial Understandability Score (IUS)*, with values from 0 to 100, as a normalization of the six-point score from the quiz.

Personal Understandability Factors: Within the previous day of the focus group, we surveyed the participants on the personal factors which, according to [4], could affect the understandability of the models. They are:

- Education (Ed): The participant received training to work with privacy and data protection. The possible values are university, work training, self-training, and others.
- Experience (Ex): The participant's experience with conceptual modeling. We grouped the participant's experience into the following categories: [0-1] Low, [2-5] Medium, [5-8] High, [8+] Expert.
- Training (Tr): On data protection training (GDPR). Measured in hours (hrs), we categorized the participants into: [0-30] Low, [30-60] Medium, [60-90] High, [90+] Expert.
- Familiarity (F): The participant's familiarity with the modeling method, particularly with STAGE. Possible values: yes and no.

– Theory (Th): Concerns the participant's knowledge of GDPR. Possible values: yes and no.

Understandability Task Effectiveness: is if the subjects can understand the "tasks or questions about the process models [4]." This variable is measured by reviewing the transcripts and video from the focus groups and identifying the contributions of each participant to the discussion in the following metrics:

– *Individual Identifications (II):* identifies and discusses a privacy risk based on their understanding of the model without inputs from other participants.
– *Identification and Agreement (IA):* participates in the collaborative identification of privacy risk and discusses it.
– *Agreements (A):* Agrees in privacy risks identified by other participants, without contributing with their perspective on the issue.
– *Percentage of Identifications (% Identification):* Provides an overview of a participant's contribution to the understandability task. Corresponds to the sum of the identifications where the participant contributes with their knowledge (II+IA) with respect to the total seeded privacy risks.

Subjective Understandability: After the focus group, we surveyed the participants' perception of the model. The metrics for his variable are detailed below.

– *Perceived Ease of Use (PEU):* Per [4], it is the perceived easiness of the subject on using this model. It usually "involves a set of questions with answers in Likert scale that aims to capture participants' subjective perception on the ease of use" [4]. Measured using [10].
– *Perceived Usefulness (PU):* how probable does the subject believe it can be of utility to use such model [4], measured using [10] guidelines.
– *Intention to Use (IU):* if the subjects intends to use the model [4], measured using [10] guidelines.

3.3 Focus Group Design

As part of the larger study, we organized focus groups with volunteers we gathered through online surveys. The objective of the larger study is to analyze the interaction between subjects with specific characteristics; thus, we used a purposive sampling approach. Given this, we did focus groups with a triangulation approach; i.e., each focus group ideally would have three participants with different professional backgrounds to perform different roles accordingly: a developer (DEV), a privacy specialist (PRI), and a business analyst (BUS). We opted for a reduced number of participants to ensure that all of them could participate as much as possible. Before starting the activity, we provided a handout on the STAGE modeling language with examples. The subjects took a quiz on the understandability of a STAGE model, where they answered six questions regarding the model's content, mirroring the approach of [15].

After filling out the understandability quiz, we conducted an online focus group. Participants were presented with an unfamiliar scenario and three views

of STAGE's models containing seeded privacy risks. They were tasked with identifying privacy risks through a straightforward reading of the model or by assessing modeling quality within the context. Following the focus group, participants were surveyed to gauge their perception of the usefulness, utility, and intention to use as a subjective assessment of understandability [4].

4 Results and Discussion

4.1 Results

We carried out eight focus groups, with 21 participants - as some subjects did not attend the activity - from October 2022 to February 2023. This made a total of 400 minutes of recorded focus groups we analyzed, as focus groups lasted a maximum of 50 minutes. Two participants, a BUS and a DEV, did not speak during the focus group, so they were discarded from the study. Table 1 show the total privacy risks identified per group and their composition (19 subjects in total).

Group	Participant Role	Total ident.
1	PRI, DEV	10
2	PRI, DEV	6
3	PRI, DEV, BUS	11
4	PRI, DEV, BUS	11
5	PRI, DEV	10
6	PRI, DEV, BUS	11
7	DEV, BUS	7
8	PRI, BUS	11

Table 1. Participant roles and total privacy risk identifications per group.

Table 2 shows the percentage of privacy risks identified individually **(II)**, collaboratively (IA), or agreed (A) by the participants, grouped by role. As can be seen in column **II**. BUS participants individually identified 5.45% of total privacy risks, while DEVs achieved 9.09%. No role identified more than 10% based solely on their background. On the other hand, most of the identifications were collaborative, as detailed in column **IA** (identification and agreement). PRI participants excelled with 55.80% collaborative identifications, while BUS participants agreed most frequently with' identifications proposed by other participants (as seen in column **A** of Table 2).

Role	II	IA	A	Perc. Identi.
BUS	5.45%	40.00%	32.70%	45.45%
DEV	9.09%	37.70%	29.90%	46.79%
PRI	7.79%	55.80%	15.60%	63.59%

Table 2. Percentage of privacy risks identified individually, collaboratively or agreed by the participants per role.

Regarding RQ1 and the relationship of personal factors in the understandability task effectiveness, Figure 1 depicts the relationship between the training (A), experience (B), and theory (C) personal factors and the percentage of identification of privacy risks, per role. Experimental results for individual understandability assessments show that subjects with higher values for personal factors (PRI) seem to present a higher performance (as seen in Figure 1). It is worth noting that even subjects with near-to-null training in GDPR (BUS) participated and contributed to understanding the model.

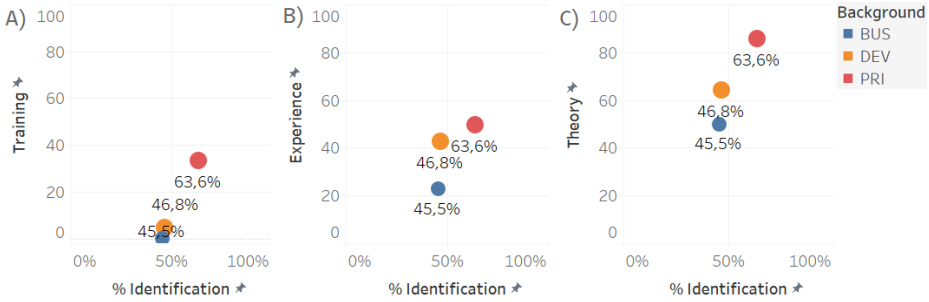

Fig. 1. Personal factors v/s percentage of identification of privacy risks: A) Training, B) Experience, C) Theory.

Role	PEU	PU	IU	Perc. Ident.
BUS	42.5	44.4	32.5	45.50%
DEV	50.6	57.6	53.6	46.80%
PRI	42.9	51.8	50.0	63.60%

Table 3. Perceived understandability measurements: PEU, PU and IU

Concerning RQ2, Figure 2 shows the understandability pretest scores and the percentage of identifications (Perc. Identi.) per role. The understandability pretests do not seem to be positively related to the percentage of identifications since PRIs had the lower pretest scores (71.4%) and the best performance in the understandability task. While DEVs and BUSs scored 81.0% and 86.7% in the pretest and had a lower performance in understandability tasks.

Table 3 presents the values for the subjective understandability measurements: PEU, PU and IU, by role, for RQ3. The difference in percentage identification — favoring PRI users — does not seem to be related to a higher or lower subjective perception of the understandability of the model.

4.2 Discussion

Considering the personal factors of understandability, although the results seem to confirm experimental results [15], the differences between BUS, DEV, and PRI in modeling experience and GDPR training and theory do not seem to be significant. There is less than 20% difference between the higher and lower performers in personal factors. Conversely, the higher and lower understandability pretest scores did not seem to correlate with the understandability task performance during the focus group. However, even with little to no training in modeling, subjects in the collaborative setting could interpret the models, extract information, and establish common ground by identifying most of the privacy risks. Even though some design decisions could favor the participants' performance (toy problem, sequential presentation of the views), we think there are two key enablers: the conceptual modeling language and the collaboration between the participants.

Regarding conceptual models, we think the STAGE's socio-technical approach is appropriate for identifying privacy risks within multidisciplinary teams. Naturally, some misalignments between the domain and the modeling language were identified. Some participants found that some concepts did not clearly represent some domain elements (PRI3: *"Why is that symbol called actor and no Data Controller?"*). However, most participants successfully identified privacy risks, even

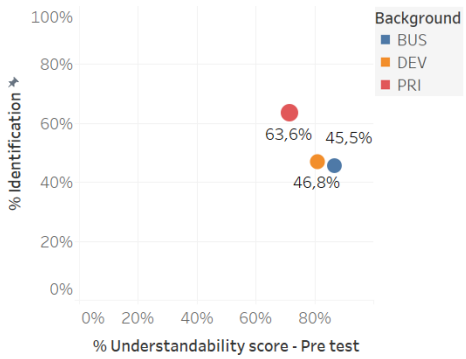

Fig. 2. Understandability pretest scores v/s percentage of identifications per role.

when faced with views that appeared confusing, such as the information view for PRIs and the social view for DEVs (as indicated in Table 4). Two groups identified all seeded privacy risks, reinforcing the effectiveness of multi-view, socio-technical models in alignment with Cognitive Fit theory [19].

The second enabler regards collaboration among participants. We think the study format helped participants focus on discussing the model based on their knowledge, experience, and training, as most privacy risks were collaboratively identified. This could be explained by the ontological foundations of collaboration, which is based on coordination, communication, and cooperation [12]. We think the focus group provided a coordination and communication framework, facilitating the participants' cooperation. The focus group defined how subjects would interact and the sequence to discuss the model views, helping coordination, while the experimenter supported communication by encouraging the team members to speak. With these two elements facilitated, subjects could focus on cooperation, defined as "*a joint effort in a shared space to achieve some goal.*", where each participant contributes according to their commitment (i.e., their roles) to the task.

	Social View	**Info. View**	**Auth. View**
Yaqin Complexity	54.57	24	19.57
Role	**Perc. Ident.**		
BUS	46.7%	46.7%	44.0%
DEV	33.3%	47.6%	54.3%
PRI	71.4%	57.1%	62.9%

Table 4. Percentage of identification (perc. ident.) per view, including Yaqin complexity index [22]

Regarding the study's limitations, the results should be interpreted considering that a single notation (STAGE) was used and that larger groups (more than three participants) could yield different results.

5 Conclusions

Using conceptual modeling artifacts as communication tools between stakeholders with different mental models can be promising for achieving common ground.

These artifacts can help interdisciplinary teams discuss regulatory data protection requirements from early phases. However, these conceptual modeling artifacts must be understandable across various disciplines, making the task challenging. Thus, understandability plays a vital role in this aspect.

This article provides evidence of the importance of interdisciplinary approaches when designing conceptual models. Through focus groups, we aimed to explore the relationship between the personal factors of understandability and the task effectiveness of identifying risks within socio-technical requirement models. Using a collaborative methodology, we engaged participants with different privacy backgrounds to analyze and discuss privacy compliance.

Our findings underscore that participants with major training, theoretical knowledge, and experience exhibit enhanced effectiveness in understandability. Although the privacy experts' understandability scores not being the highest, they identified most of the privacy risks and contributed significantly to the discussion. This demonstrates that a collaborative approach effectively mitigates the limitations posed by individual scores. Furthermore, regarding the subjective understandability metrics, the difference between these metrics and the effectiveness of understanding tasks could be because of how participants with different backgrounds interact. This result highlights the intricate and mutually advantageous nature of collaboration, where even a lower perception of ease of use (as observed among privacy experts) does not hinder the ability to achieve the goal of identifying potential risks in the models.

These results offer empirical evidence of the importance of collaboration in enhancing model understandability, particularly with different personal backgrounds in complex domains such as data protection and privacy. Moreover, it prompts a consideration of interdisciplinarity and its pivotal role in advancing conceptual modeling within collaborative environments, offering a promising avenue for improved model understandability.

Acknowledgments

This work was supported by the Generalitat Valenciana through the CoMoDiD project (CIPROM/2021/023) and Santiago Grisolía fellowship (GRISOLIAP/2020/096), and the Spanish State Research Agency through the DELFOS (PDC2021-121243-I00) and SREC (PID2021-123824OB-I00) projects.

References

1. Breaux, T.D., Norton, T.: Legal accountability as software quality: A us data processing perspective. In: 2022 IEEE 30th International Requirements Engineering Conference (RE). IEEE (2022)
2. Dalpiaz, F., Paja, E., Giorgini, P.: Security requirements engineering: designing secure socio-technical systems. Cambridge, Massachusetts (2016)
3. 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** (07 2006)

4. Dikici, A., Turetken, O., Demirors, O.: Factors influencing the understandability of process models: A systematic literature review. Information and Software Technology (2018)
5. Engelsman, W., Wieringa, R.: Understandability of goal-oriented requirements engineering concepts for enterprise architects. In: International Conference on Advanced Information Systems Engineering. Springer (2014)
6. 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. ICSE '18, Association for Computing Machinery (2018)
7. Hadar, I., Reinhartz-Berger, I., Kuflik, T., Perini, A., Ricca, F., Susi, A.: Comparing the comprehensibility of requirements models expressed in use case and tropos: Results from a family of experiments. Information and Software Technology **55** (2013)
8. Houy, C., Fettke, P., Loos, P.: Understanding understandability of conceptual models–what are we actually talking about? In: International Conference on Conceptual Modeling. Springer (2012)
9. Mendling, J., Djurica, D., Malinova, M.: Cognitive effectiveness of representations for process mining. In: International Conference on Business Process Management. Springer (2021)
10. 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. AIS Electronic Library (2003)
11. 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)
12. Oliveira, F.F., Antunes, J.C., Guizzardi, R.S.: Towards a collaboration ontology. In: Proc. of the Snd Brazilian Workshop on Ontologies and Metamodels for Software and Data Engineering. João Pessoa (2007)
13. Petrusel, R., Mendling, J., Reijers, H.A.: Task-specific visual cues for improving process model understanding. Information and Software Technology (2016)
14. Reijers, H.A., Mendling, J.: A Study Into the Factors That Influence the Understandability of Business Process Models. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans (2011)
15. Reijers, H.A., Mendling, J.: A study into the factors that influence the understandability of business process models. IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans **41**(3) (2011)
16. Rumpe, B.: Agile modeling with the uml. In: International Workshop on Radical Innovations of Software and Systems Engineering in the Future. Springer (2002)
17. Stitzlein, C., Sanderson, P., Indulska, M.: Understanding healthcare processes. Proceedings of the Human Factors and Ergonomics Society **57** (2013)
18. Sutcliffe, A.: User-centred requirements engineering. Springer Science & Business Media (2002)
19. Vessey, I.: Cognitive fit: A theory-based analysis of the graphs versus tables literature. Decision sciences **22**(2) (1991)
20. Wang, W., Indulska, M., Sadiq, S., Weber, B.: Effect of linked rules on business process model understanding. In: Business Process Management: 15th International Conference, BPM 2017, Barcelona, Spain, September 10–15, 2017, Proceedings 15. Springer (2017)
21. Wohlin, C., Runeson, P., Höst, M., Ohlsson, M.C., Regnell, B., Wesslén, A.: Experimentation in Software Engineering. Springer-Verlag (2012)

22. Yaqin, M.A., Sarno, R., Rochimah, S.: Measuring scalable business process model complexity based on basic control structure. International Journal of Intelligent Engineering and Systems **13**, 52–65 (2020)