2022 IEEE 30th International Requirements Engineering Conference Workshops (REW) | 978-1-6654-6000-2/22/$31.00 ©2022 IEEE | DOI: 10.1109/REW56159.2022.00052

Socio-Technical Modelling for GDPR Principles: an Extension for the STS-ml

1st Claudia Negri-Ribalta
Centre de Rechercher en Informatique
Université Paris I Panthéon-Sorbonne
Paris, France
claudia-sofia.negri-ribalta@univ-paris1.fr

2nd Rene Noel
Valencian Research Institute for Artificial Intelligence
Universitat Politècnica de València
Valencia, Spain
rnoel@vrain.upv.es

3rd Nicolas Herbaut
Centre de Rechercher en Informatique
Université Paris I Panthéon-Sorbonne
Paris, France
0000-0003-1540-2099

4thOscar Pastor
PROS Research Centre
Universitat Politècnica de València
Valencia, Spain
0000-0002-1320-8471

5th Camille Salinesi
Centre de Rechercher en Informatique
Université Paris I Panthéon-Sorbonne
Paris, France
0000-0002-1957-0519

***Abstract*—Compliance with data protection regulations is vital for organizations and starts at the requirements level. The General Data Protection Regulation (GDPR) has been the European Union (EU) regulation on the topic since 2018. Organizations that operate within the territorial scope of the GDPR are expected to be compliant; otherwise, they can get high fines, and their reputation can be damaged. Thus, GDPR compliance sets challenges for the design of information systems that must be tackled starting from the requirements level.**

Given the difficulties of translating regulations and the drawbacks of natural language requirements, modeling languages can help requirements engineers analyze data protection. Socio-Technical Security modeling language (STS-ml) is a security modeling method that has been already extended for modeling privacy issues such as personal data, data controllers and processors, and specifying the legal basis for data processing. However, information critical for complying with GDPR principles still lacks modeling support. This article presents a proposal for extending the STS-ml to address GDPR principles. We show the need for modeling data protection requirements for each GDPR principle through a working privacy case and propose a set of five lightweight but meaningful extensions for the method. The extended language is intended to help requirements engineering practitioners with privacy requirements with little additional effort while preventing significant fines for EU organizations.

***Index Terms*—requirements modelling, data protection, privacy**

I. Introduction

The General Data Protection Regulation (GDPR) [1] is the pan-European regulation on data protection. The effects of these rules on the information systems (IS) range from functional requirements (FR), such as retention periods, to ethical requirements, such as fairness and transparency in the processing of data. From a requirements engineering (RE) perspective, there is a longstanding history of creating modeling languages, tools, and methodologies to deal with privacy and data protection legal requirements [2], [3]. Indeed, it has been recognized that extracting requirements from legal instruments can be difficult [3].

Given the complexity of regulatory requirements, sometimes data protection requirements are dealt with by groups with people of diverse backgrounds. The goal of this paper is to contribute to this area and propose a GDPR extension for a modeling language (STS-ml) that can act as a common ground.

In this context, one of the different modeling languages related to security and privacy is the Socio-Technical Security modeling language (STS-ml) [4]. At its core, the STS-ml deals with security requirements and policies, representing social actors and their dependencies for achieving goals, the information needed, and the authorizations for such information. An adaptation for the GDPR was proposed by Robol et al. [5], that enriches the existing language by allowing to identify personal data, distinguishing data controllers from data processors, and defining the legal basis for authorizing data access.

Our contribution builds from [5]. Using the analysis method of the single case mechanism experiment technique [6], we take GDPR's seven principles and propose more elements for the STS-ml. We base our analysis from the GDPR regulation itself [1], data protection authorities' interpretation [7], [8], software engineering ontologies [9], and data protection experts [10], [11]. The idea behind this analysis method is to stress the artifact to propose improvements. In our case, we propose five new elements for the STS-ml so that it can better adapt to the GDPR. These are identification of retention time, special categories of personal data, asymmetrical relationships, when data from a minor is involved, and if actors are EU or non-EU.

The proposal is a work in progress that can help organizations asses GDPR compliance and verify their policies and business processes. It adds key elements to the STS-ml language, based on the seven principles of the GDPR, to avoid high fines [1].

II. Background

The GDPR sets out the 7 data protection principles in Art.5. Below we present each principle, reviewing the specific legal elements that represent the motivation for our proposal.

Lawfulness, fairness, and transparency is the first principle, in Art.5(1) of the GDPR. It specifically says that

2770-6834/22/$31.00 ©2022 IEEE
DOI 10.1109/REW56159.2022.00052

personal data shall be "processed lawfully, fairly and in a transparent manner in relation to the data subject" [1]. Lawfulness is the idea that a controller must have a legal reason for processing the data and is linked to articles 6 - 10 of the GDPR [1], [8]–[10]. In Art.6(1), the GDPR provides six legal bases for processing data, ranging from consent to vital interest [1]. Transparency means that data subjects must be informed about the processing of their data (Art. 13 and 14). Indeed, Recital 39 states that data subjects should be informed in an easy and accessible way about how their data will be processed, its purpose, the controller's identity, and how to exercise their rights [1]. Data subjects should be able to understand what is happening and not just publish the source code [7], [10]. Understandability can be challenging when dealing with *minors data*. Finally, fairness can be understood as processing the data in a manner that will not negatively impact the data subjects and as context-dependent [11], [12]. Thus, due to the risks of processing *special categories* of data, it is critical to do it fairly.

This first principle is vital, as it deals with fairness, understanding it as transparency and lawfulness. According to [12], the idea of fairness in GDPR also relates to non-discrimination, unfair imbalance (or *asymmetrical relationship*), and non-discrimination. This implies that this principle aims to protect data subjects' integrity and avoid unfair treatment and discrimination, among others.

Purpose limitationis the idea that personal data should only be gathered and processed if there is an identified, clear and legitimate reason for processing; the data has a well-identified goal [1], [9], [11]. This concept is also related to transparency and the right to be informed (Art. 13 and 14) [8]. Purpose limitation is very important when processing *minor information* and *special categories*, given the risks of processing this data; it should only be processed when clear, legitimate, and identified reason, i.e. data shouldn't be gathered "just for the sake of it".

Data minimization refers to the idea that personal data collected and the process should be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" [1]. As indicated by [7], [8], it's important to know if a goal can be achieved without or less amount of personal data.It also indicates that access to personal data should be limited, and "state of the art" technology should be applied to protect the data, whilst more copies than necessary shouldn't be created. Finally, *special categories of personal data* should be kept to the minimum - due to its risks - and is context-dependent (i.e. if the subject is a *a minor* or there is a *asymmetrical relationship*) [8]. Therefore, although data minimization is important for all categories of personal data, it acquires a vital role for special categories of personal data.

Accuracy and Storage limitation are two different values, yet they go well together. The accuracy principle is straightforward: organizations should take reasonable steps to keep personal data accurate and up-to-date. Thus, if a data subject contest the accuracy of such data, the organization should rectify the data (Right to Rectification, Art.16) [1].

On the other hand, storage limitation means that data shouldn't be kept longer than for what is necessary [1]. Hence, *retention periods* for the personal data should be identified. These retention periods should be recorded, informed to the data subject, and processes should be placed to delete the data [8], [9]. The right to erasure in Art.17 and Art.19 relates to this principle [1].

Integrity and confidentiality is the principle mostly related to data security, of secure data processing based on its risk [1], [8], [10], [11]. Based on the purpose of the processing, the context, the type of data, and the risk, the controller must put in place organizational, technical, and policy measures to protect the data. The GDPR states that the controller should ensure the integrity, confidentiality, and resilience of the data processing, alongside the data processor [1]. Measures shouldn't be just technical, but also organizational and policy based.

Accountability is the principle that, at its core, is the sum of all the previous principles of the GDPR. It is the idea that organizations should be held responsible for their actions.

A. Privacy Requirements and STS-ml Modeling Language

RE has a longstanding history of privacy engineering [3]. The community has recognized the importance of including privacy requirements from early phases of the software development lifecycle (SDLC) [2]. Several methods have been proposed, some of the most well-known being: LIDDUN, SQUARE, PRiS, RBAC, STRAP, and the i* method [2].

The Socio-Technical Modelling Language (STS-ml) is a goal and actor-oriented security modeling language, that uses elements and primitives from i* [4]. It was developed by the University of Trento (https://www.sts-tool.eu/) and allows for the analysis of socio-technical requirements throughout different phases of software engineering [4]. It is used for security analysis [4] and it has been adapted for GDPR analysis [5], adding features such as the legal basis for data processing.

STS-ml has both agents and roles. It helps model the dependencies between actors, through the usage of goals, document items, and other i* primitives [13]. These "goals can be delegated among actors and documents can be transmitted" [5].

For achieving its purpose, the STS-ml has three views, each with its own objective: (1) the social, (2) the informational, and (3) the authorization view. The social view manifests the actors' intentions, their goals, dependencies, and the document transmission and models the "social and organizational aspects" [4]. The information view models the "information asset", i.e. what information the actors have,which is represented through documents [4]. Lastly, the authorization view models "the flow of permissions and prohibitions regarding information among the actors" [4]. The authorization view is then the diagram that deals with the governance of information.

The reason for choosing STS-ml is its adaptability to GDPR and the work already done by [5] to adapt the language for GDPR purposes. However, their proposal doesn't address some concerns related to the GDPR principles presented in the previous subsection.

III. Analysis and Proposal

In this section, we present our proposal to extend STS-ml for addressing GDPR privacy principles, that would help analysts reflect about legal compliance of the system at the socio-technical level. While existing approaches have conceptualised GDPR elements for modelling privacy requirements [14], [15], we focus on identifying concepts which are valuable for compliance analysis, guided by the GDPR principles.

A. *Method and Privacy Case*

The analysis method used in this article consists of exposing an artifact to cases that are designed to produce deviations from the wanted effects, and draw possible explanations in terms of the artifact's architecture [6]. In our analysis, the artifact is the STS-ml Metamodel [5] and the stimuli is a real-world privacy case for each of the GDPR principles, which we relate to a specific requirement(s) expressed in the EARS syntax [16].

These cases produce the unwanted effect of being unsupported by STS-ml and its GDPR extension, and we draw explanations by examining the lack of concepts, attributes, or relationships in the STS-ml Metamodel. For solving the unwanted effect, we present five extensions to the existing metamodel [5], which are presented in Fig.1.

We test the STS-ml using the following scenario: There is a fictional non-governmental organization (NGO), which we identify as NGO in the STS-ml figures) working in providing housing to displaced people, particularly refugees and asylum seekers. The NGO gives special priority to families (those that have children, elderly people or members with diseases in their units, as defined by the NGO). They use cloud services to store the data and, consequently, the NGO wants to verify if it is GDPR compliant, check their current policies, security requirements, and business process. This scenario is inspired by real life use cases.

B. *STS Extended Metamodel*

We present five proposals on new attributes for the STS-ml GDPR adapted metamodel (Fig.1) for compliance. Our proposal is highlighted in yellow in Fig.1. Each proposal presents a specific situation of the privacy case, and we show that it can not be modeled using the current constructs of the STS-ml GDPR metamodel. Then, we comment on the need and importance for modeling the situation for compliance and auditability objectives. Finally, we describe the proposal of the new attributes for the STS-ml GDPR metamodel.

1) ***Retention Time****:*

> **Privacy Case:** *The NGO receives family units' data and, wants to store it for up to one year after the unit has been housed. It runs security and data protection reviews yearly. Requirement: WHEN 12 months have passed since the data has been collected the organization shall delete the data*

In the proposal of [5], no class or attribute allows specifying the retention time of personal data. They have proposed a class for legitimate basis in their proposal, which can help define the retention time [5]. Having data for a defined and limited time is critical for the GDPR, as previously shared in Background. When data is collected and processed, the organization should define a time frame for the processing, and afterward, the data should be deleted or anonymized [9]. Indeed in the PrOnto ontology, this is represented by the "interval" element [9]. The data retention period is determined by each organization and is context-dependent. A common way to define the data retention period is on the legal basis of the data processing. From an organizational point of view, retention time is a FR, as it sets an action that the IS should do Additionally, when a controller transfers data to a processor, the controller should indicate the retention time for the processing of this data - per GDPR indication (Art.6(2), 24, 25) [1]. The idea of having data for a specific time frame relates primarily to the GDPR's values of (4) Accuracy and (5) Storage limitation (Table I).

Accordingly, we propose to add the attribute *Retention Time* as an integer (representing months) in the "Legal Basis" class of the authorization view, given that this view is about the governance of data and has a legal basis. As explained, the retention time of personal data can be related to the legal basis chosen for such processing. In visual terms, we propose adding the integer in parenthesis next to the legal basis, as shown in Fig. 2.

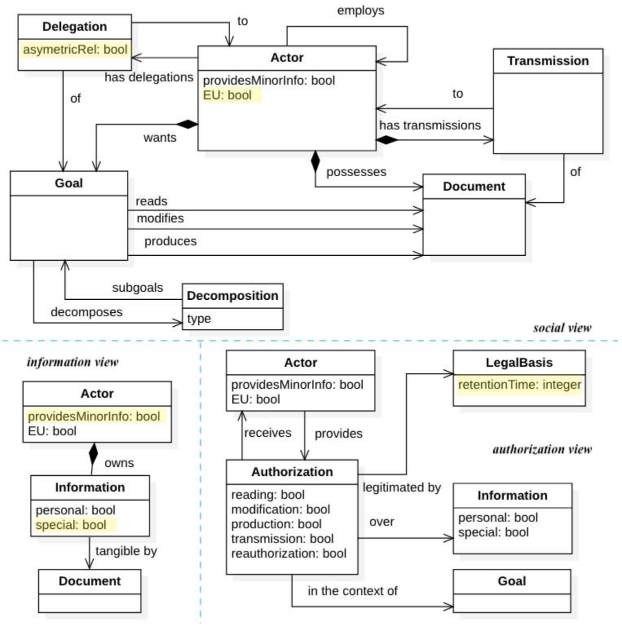

Fig. 1. Extended STS metamodel.

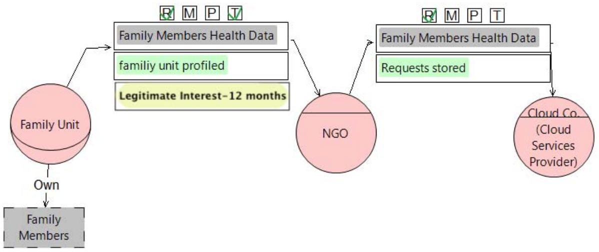
R
M
P
T
Family Members Health Data
familiy unit profiled
Legitimate Interest-12 months
R
M
P
T
Family Members Health Data
Requests stored
Family Unit
NGO
Cloud Co.
(Cloud Services Provider)
Own
Family Members

Fig. 2. Graphical representation of Retention Time in authorization view.

TABLE I
GDPR VALUES

Name of proposal	**Metamodel and Model View**	Relationship to GDPR values ((number) value name)
Retention time	*Metamodel:* Class `LegalGaleBasis`, add attribute `retentionTime` *(type: integer) View:* Authorization view	(4) Accuracy, (5) Storage limitation
Provider of Minor Information	Metamodel: Class `Actor`, add attribute `providesMinorInfo` *(type:boolean) View:* Information view	(1) Lawfulness, fairness and transparency, (2) Purpose limitation, (3) Data minimization, (4) Accuracy, (5) Storage limitation, (6) Integrity and confidentiality
Special category of data	*Metamodel:* Class `Information`, add attribute `special` (*type:boolean*) *View:* Information view.	(1) Lawfulness, fairness and transparency, (2) Purpose limitation, (3) Data minimization, (6) Integrity and confidentiality
Asymmetrical Relationship	*Metamodel:* Class `Delegation`, add attribute `asymmetricRel` (*type:boolean*) *View:*Social view.	(1) Lawfulness, fairness and transparency, (3) Data minimization, (6) Integrity and confidentiality
EU actor	*Metamodel:* Class `Actor`, add attribute `EU actor` (*type:boolean*). *View:* Social view.	(1) Lawfulness, fairness and transparency, (6) Integrity and confidentiality

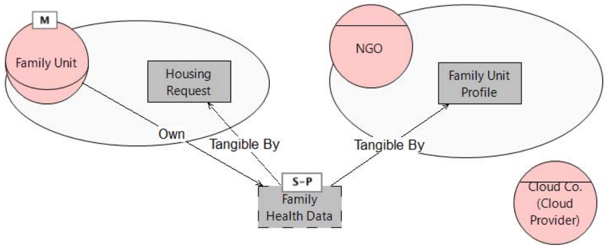

Fig. 3. Graphical representation of Special Category of Data and Provider of Minor Information attributes in the information view.

In our use case, the NGO has defined that its legal basis is *legitimate interest* for processing the family members' health data. Given the sensibility of this data (*special category*) retention time should be as least as possible. For this scenario, the requirements sets 12 months as retention period[1]. For example, if the NGO had defined 120 months for data retention, this should raise alarms and, it should be verified.

*2) **Special category of personal data**:*

> **Privacy Case:** The NGO asks the family if they have members in their household with important diseases to give them priority in providing them with household. *Requirement: THE NGO shall ask for the minimum amount of special categories of data. THE NGO shall store special categories of data securely*

In the current STS-ml GDPR metamodel (Fig.1) there is no attribute to know if the personal data is a special category or not. Health data, according to Art.9 of the GDPR, is part of this type of personal data [1], [9]. In the PrOnto ontology, there are distintions between the types of personal data and which categories make up for special categories of data [9].

Throughout the GDPR, special categories of personal data (SPD) are mentioned as a particular type of personal data, where its' processing conveys higher risks than normal personal data, thus having more stringent requirements for its processing. Particularly, recital 75 of the GDPR, exemplifies why this is important [1]. Hence, if processing special categories of personal data, organizations must identify them

Identifying the need for processing SPD relates to different values of the GDPR (see Table I). Data minimization is especially relevant, as the organization should inquire how to achieve a goal with the least amount of personal data possible, trying to avoid SPD - if possible - to achieve its' objectives [7], [8]. If the actor must process SPD, the security and data protection teams should verify the security requirements.

In [5] they propose the attribute of personal data as "a boolean attribute discriminates a personal data from an information". In this extension, we propose an attribute (type boolean) named "special category" in the "information" class for both the information and authorization view. Proposing "special category" in the information view helps the modeler know about the type of personal data. In the authorization view, it aids the modeler to see what types of rights should be in place for this type of data. This attribute can be true if, and only if the personal data attribute is also true. For graphical representation, our approach is similar to [5]; we propose to add an S next to the P that corresponds to personal data, representing the "special category" as seen in Fig. 3.

Without the special category notation, the person in charge of analyzing finds itself limited to identifying the type of personal data. In the privacy case, the NGO prioritizes families with members that might have a disease.Knowing if a subject has a disease is an SPD;in this case, the goal and legal basis for processing the data are clear, so the modeler must check if these elements are in line with requesting SPD, and place notices if a process is highly sensible and shall store it securely.

*3) **Asymmetrical relationship**:*

> **Privacy Case:** The NGO works with families that are refugees or asylum seekers to provide them with households. *Requirement: IF the household seeker is vulnerable, THEN the NGO shall avoid consent as a legal basis*

As seen in the current STS-ml GDPR metamodel in Fig. 1, there is no relationship nor attribute in the model to identify if a data subject is vulnerable or is in an asymmetric situation with an actor. Although the employment relationship exists in the proposal from [5], this one is used "...to distinguish third party actors from actors within the same organization".

[1] For illustration purposes, we assume this is the time frame period and legal basis for processing data. However, a legal analysis should be done.

In other words, it helps to identify controllers and processors.

An asymmetric relationship between actors occurs when the data subject is vulnerable [1], [17]. If there is an asymmetry of power, not all the legal basis can be used as justification for the processing, and the GDPR imposes more stringent technical and organizational measures for the data processing [1].

The asymmetry of power is characterized by the imbalance "between the data subjects and the data controller, meaning the individuals may be unable to easily consent or oppose, the processing of their data, or exercise their rights" [17]. This group includes - but is not limited to - children, employees, groups of people that might be at risk or at disadvantage (such as asylum seekers), or in any situation where there are a power asymmetry [17]. For example, recital 75 from the GDPR indicates that if the data processing context includes vulnerable individuals , measures should be taken the secure the data processing (per Art.24 and Art.32(2) of the GDPR [1]).

Accordingly, in the context of asymmetry of power, organizations processing personal data should follow a data minimization approach, revise their information security structure, and verify if the processing is fair and transparent. Given the risk of processing this personal data, organizations must check that they process the data fairly and transparently, alongside having the correct legal basis (that's to say, avoiding consent).

Consequently, we propose the creation of an asymmetrical relationship between actors, inspired by [5], whom proposed the employment relationship between actors. This new relationship aims at visualizing power asymmetry between actors.

With this addition, it could be possible to revise whether the legal basis follows the relationship between actors. It can also help check if the processing is fair. In our privacy scenario, the families seeking a household are vulnerable individuals, ergo there is asymmetry of power [17]. The information security policies should be verified due to the sensibility of asylum seekers' personal data and, consent shall be avoided as a legal basis.

4) *Provider of Minor Information*:

Privacy Case The NGO asks families to provide all sorts of information about their unit, which might or not include minors. If minors are involved, the families receive priority in the housing. *Requirement: THE NGO shall ask for the minimum amount of minors' personal data. THE NGO shall store minors' data securely*

Currently, in the STS-ml GDPR proposal, there is no method for identifying if the personal data the organization is processing, is from a minor. This information is vital to detect, as the GDPR sets specific rules on the processing and governance of children's data [1].

As specified by Recital 38 of the GDPR "children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences, and safeguards ..." [1]. The GDPR is strict on the processing of children's personal data, due to the risks it has for the data subject, as explained in Art.8, Art.32(2), and Recital 75 and 38 [1]. For instance, if consent is used as the legal basis, depending on the national age requirement, the legal guardian might be asked to provide the consent or be notified (Art.8, recital 38 and 65.). If the child is consenting without a guardian's approval, the organization has to share a plain and clear explanation on how their data is used (Recital 16 of [1]). Finally, the WP29 in their opinion 5/2009, has suggested that it should be avoided to ask for special categories of data from children [17].

To sum up, the GDPR has special consideration for children's personal data. The idea is to protect minors,and to prevent the misuse, abuse, and insecure processing of this data. Therefore, we linked this proposal to all GDPR values (Table I).

For this reason, we propose to add a new boolean attribute to the "Actor" class named "Provider of Minor Information". This new attribute would allow modeling in the information view if an actor is providing personal data about a child. If an actor is a provider of minor information, then an M will be written inside the actor. We've made a distinction from "Is it a minor" to "Provider of minor information" with the idea that there might be certain actors (such as a school) who are not themselves minors but are providing information about one.

In our privacy case, the NGO needs to identify if there are minors in the family unit, so they can give them priority when providing household. Given that already the NGO is asking for SPD, it is crucial to also identify if there are minor data.

5) *EU Actor:*

Privacy Case Family units' data is stored in a cloud for up to one year. The organization needs to verify if the cloud provider is GDPR compliant. *Requirement: WHEN the cloud provider is not located in the EU, the NGO shall revise that contractual agreements are in place between the NGO and the cloud provider*

There are no attributes for identifying where an actor is based (Fig. 1). If an organization decides to transfer data subjects outside the EU, it must fulfill a specific set of compliance rules. In fact, the PrOnto ontology identifies this with the jurisdiction and place elements [9].

The GDPR indicates how the international transfer should happen in Chapter 5, in Art.44 to 50. In particular Art.46 says that if the data is going to be transferred outside the EU, either this country must be approved by the Commission as part of the list of safe countries or organizations (Art.45(1)), or if there are appropriate safeguards in place [1]. Specifically, Art.46(2) and Art.46(3) of the GDPR define an extensive list of requirements if the data controller or processor wishes to transfer data [1].

Identifying if the actors are EU or not, helps to corroborate if the values of (6) Confidentiality and integrity and (1) Lawfulness, fairness, and transparency are met. In our case, the security acquires a prominent role, as the EU-based organization has to verify that the Non-EU actor has an adequate level of data protection. Furthermore, it needs to have a legal basis for transferring the data and must check that the processing is fair [18].

We propose to add a new boolean attribute to the class Actor named EU Actor. This attribute helps to identify if an actor is either from the EU or the list of safe countries. If it is the case that it is a Non-EU, the actor must decide which path - per Chapter 5 of the GDPR - will follow, verify the

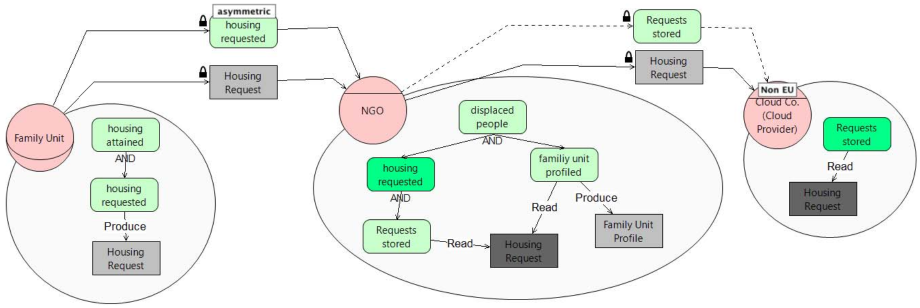

Fig. 4. Graphical representation of Asymmetric Relationship and EU Actor in the social view

legal basis, and if the processing is fair. A tool could alert that if an actor is Non-EU, then the policies and business processes should be checked and verified.

In our use case, the NGO has to be careful with whom it shares the data, given both the that is SPD and has an asymmetrical relationship. By dealing with asylum seekers, if it shares data with Non-EU countries, it shouldn't rely on consent, and has to be careful with the thresholds placed by the GDPR. It, needs to check where are the servers of the cloud service located and their GDPR compliance.

IV. Discussion, threats to validity and conclusion

We believe that the proposed extensions are valuable both for analysing the GDPR compliance of the system and the early identification of functional and non-functional requirements. Regarding system requirements, analysts will be aware of the need to provide mechanisms to comply with retention time constraints, as well as to design workflows to avoid, when possible, when using SPD. Beyond the effect on the system requirements, a new system could introduce social interactions that could affect GDPR compliance, such as asymmetrical relationships, that must be managed at the organizational policy level.

The proposal is limited to the situations presented in section 2, yet, it demonstrates the usefulness of the approach in revealing concepts that have not been covered by existing conceptualisations in requirements engineering [14], [15], but which have been partially addressed in ontologies, such as PrOnto [9]. We aim to extend this work to cover most of the PrOnto ontology concepts while keeping the simplicity and most design principles of the STS-ml. Future research should aim to address other regulations, in order to provide more abstract concepts instead of specific GDPR elements such as the "EU actor" attribute. Part of the future work regards the validation of our proposal; we seek to study its potential effects by asking different practitioners if the proposed notation helps them verify organization policies and processes. We also seek to incorporate of other GDPR elements - such as data subjects' rights - and formally specify the analyses commented for each proposal through an automatic reasoning framework. Furthermore, it would be interesting to test the understandability of the language - among non-engineers - and the usage of goal-oriented modeling for data protection compliance.

References

[1] "Regulation (EU) 2016/678 of the European Parliament and of the Council - General Data Protection Regulation," European Union.

[2] A. Pattakou, A. Mavroeidi, V. Diamantopoulou, C. Kalloniatis, and S. Gritzalis, "Towards the design of usable privacy by design methodologies," 08 2018, pp. 1–8.

[3] P. N. Otto and A. I. Antón, "Addressing legal requirements in requirements engineering," in *15th IEEE international requirements engineering conference (RE 2007)*. IEEE, 2007, pp. 5–14.

[4] E. Paja, F. Dalpiaz, and P. Giorgini, "Modelling and reasoning about security requirements in socio-technical systems," *Data & Knowledge Engineering*, 2015.

[5] M. Robol, M. Salnitri, and P. Giorgini, "Toward gdpr-compliant socio-technical systems: modeling language and reasoning framework," in *IFIP Working Conference on The Practice of Enterprise Modeling*. Springer, 2017, pp. 236–250.

[6] R. J. Wieringa, *Design science methodology for information systems and software engineering*. Springer, 2014.

[7] E. D. P. Board, "Guidelines 4/2019 on article 25 data protection by design and by default version 2.0," European Data Protection Board, Tech. Rep., October 2020, guidelines adopted.

[8] Information Commissioner's Office, "Guide to the General Data Protection Reuglation (GDPR)," Tech. Rep., January 2021.

[9] M. Palmirani, M. Martoni, A. Rossi, C. Bartolini, and L. Robaldo, "Pronto: Privacy ontology for legal reasoning," in *International Conference on Electronic Government and the Information Systems Perspective*. Springer, 2018, pp. 139–152.

[10] P. Voigt and A. Bussche, *The EU General Data Protection Regulation (GDPR): A Practical Guide*, 01 2017.

[11] E. Ustaran, *European Data Protection: Law and Practice*. an IAPP Publication, International Association of Privacy Professionals, 2019.

[12] G. Malgieri, "The concept of fairness in the gdpr: a linguistic and contextual interpretation," in *Proceedings of the 2020 Conference on fairness, accountability, and transparency*, 2020, pp. 154–166.

[13] E. Paja, F. Dalpiaz, M. Poggianella, P. Roberti, and P. Giorgini, "Sts-tool: socio-technical security requirements through social commitments," in *2012 20th IEEE International Requirements Engineering Conference (RE)*. IEEE, 2012, pp. 331–332.

[14] M. Gharib, J. Mylopoulos, and P. Giorgini, "Copri-a core ontology for privacy requirements engineering," in *International Conference on Research Challenges in Information Science*. Springer, 2020, pp. 472–489.

[15] J. Tom, E. Sing, and R. Matulevičius, "Conceptual representation of the gdpr: model and application directions," in *International Conference on Business Informatics Research*. Springer, 2018, pp. 18–28.

[16] A. Mavin, P. Wilkinson, A. Harwood, and M. Novak, "Easy approach to requirements syntax (ears)," in *2009 17th IEEE International Requirements Engineering Conference*. IEEE, 2009, pp. 317–322.

[17] T. W. P. on the Protection of Individuals with regard to the Processing of Personal Data, "Guidelines on data protection impact assessment (dpia) and determining whether processing is "likely to result in a high risk" for the purposes of regulation 2016/679," Tech. Rep., 2017.

[18] "Standard contractual clauses (scc)," European Commission.