




# Goal-Modeling Privacy-by-Design Patterns for Supporting GDPR Compliance

Mohammed Ghazi Al-Obeidallah<sup>1</sup><sup>a</sup>, Luca Piras<sup>2</sup><sup>b</sup>, Onyinye Iloanugo<sup>3</sup>, Haralambos Mouratidis<sup>4</sup><sup>c</sup>,  
Duaa Alkubaisy<sup>5</sup> and Daniele Dellagiocoma<sup>6</sup>

<sup>1</sup>Department of Software Engineering, Al Ain University, Abu Dhabi, U.A.E.

<sup>2</sup>School of Computing, Middlesex University, London, U. K.

<sup>3</sup>School of Computing, Robert Gordon University, Aberdeen, U. K.

<sup>4</sup>Institute for Analytics and Data Science, University of Essex, Colchester, U. K.

<sup>5</sup>College of Applied Studies and Community Service, Imam Abdulrahman Bin Faisal University, Dammam, Saudi Arabia

<sup>6</sup>Centre for Secure, Intelligent and Usable Systems, University of Brighton, Brighton, U. K.

**Keywords:** Requirements Modeling, Requirements Engineering, Privacy-by-Design, Goal Modeling, GDPR, Design Patterns.

**Abstract:** The introduction of the European General Data Protection Regulation (GDPR) has imposed obligations on organisations collecting data in the EU. This has been beneficial to citizens due to rights reinforcement achieved as data subjects. However, obligations heavily affected organisations, and their privacy requirements analysts, having issues with interpreting and implementing GDPR principles. This paper proposes visual GDPR Patterns supporting analysts through Privacy-by- Design (PbD) and GDPR compliance analysis. In order to achieve that, we extended a requirements modeling tool, SecTro, which is used to assist analysts in creating visual requirements models. Specifically, we extended SecTro with novel visual GDPR patterns representing GDPR principles. We evaluated the patterns in a healthcare case study. The evaluation results suggest that the GDPR patterns can help analysts in PbD modeling analysis, by representing GDPR principles and considering relevant ready-to-use alternatives, towards achieving GDPR compliance.


## 1 INTRODUCTION


Data protection regulations are rising, and businesses are facing problems to determine whether their data processing operations are legal, especially in an international setting. Data has become a significant asset in recent years, and it has even been dubbed the “Currency of the future” (Voigt & Von dem Bussche, 2017).


Non-GDPR-compliant organisations can be affected with a fine of a maximum amount of 20 million euros, or 4 percent of the total annual worldwide turnover (Voigt & Von dem Bussche, 2017). Organisations need to exercise extreme caution while implementing their data protection procedures to meet the new GDPR principles.

This paper tries to answer the research question: **RQ1.** How to support privacy requirements analyst to perform Privacy-by-Design (PbD) analysis through representation and fulfilment of GDPR Principles, towards GDPR compliance? During workshops and the final evaluation of DEFEND in the premises of four pilots (Piras *et al.*, 2019), participants have considered several useful methods to support them in PbD activities through modeling. However, even though finding such methods supportive, the most challenging aspect has been the identification of privacy and security mechanisms for fulfilling GDPR principles.

This paper focuses on designing privacy patterns on the top of a goal-modeling tool called SecTro

<sup>a</sup> <https://orcid.org/0000-0003-4976-1380>

<sup>b</sup> <https://orcid.org/0000-0002-7530-4119>

<sup>c</sup> <https://orcid.org/0000-0002-2599-0712>

(Mouratidis & Giorgini, 2007), (Pavlidis *et al.*, 2012), (Pavlidis *et al.*, 2017).

The proposed extended SecTro can be used to assist an organisation in being GDPR compliant. The extended version of SecTro provides the analyst with a set of patterns as models, for GDPR principles, which can be used by the analyst for performing PbD modelling, and checking current compliance of the modeled system with GDPR principles.

Each pattern we designed represents concepts and alternatives for fulfilling one of the GDPR principles. SecTro enables security analysts in creating diagrams that are needed to discover, model, and analyse security and privacy aspects. Thanks to the GDPR Privacy patterns we designed on top of SecTro, the extended SecTro assists analysts in the early and late requirements and architectural design stages of modeling activities by supporting them in the production of relevant concepts and models required during the new (GDPR compliance) modeling activities.

The rest of this paper is organized as follows: Section 2 presents the paper baseline and our designed patterns. Section 3 illustrates our case study and evaluation. Section 4 presents the related work, and Section 5 concludes the paper.

## 2 BASELINE AND PATTERNS DESIGN

This section illustrates the paper baseline, the DEFEND project, and SecTro tool. We also indicate the design of our GDPR patterns, developed on top of SecTro.

### 2.1 DEFEND Project

GDPR introduced regulations to address the problem of citizen data protection, due to lack of control over management and privacy issue of citizen data. These regulations have posed challenges and difficulties for organisations, which have led to pay heavy fines for not being GDPR compliant. DEFEND provided tools and methods that can be reused to support and guide organisations in achieving GDPR compliance (Piras *et al.*, 2019).

DEFEND platform reviewed tools and prototypes from the industry and the literature and discovered that while there are many tools and prototypes that can help organisations comply with specific/isolated GDPR requirements, there was no comprehensive

platform that could help organisations comply with all of the GDPR requirements.

### 2.2 SecTro Tool

It is already agreed, by the industry and relevant research communities, that security should be considered from the early phases of the development process. SecTro is an automated tool offering well-established security requirements method (Pavlidis *et al.*, 2012). SecTro tool guides and supports analysts in the building of appropriate models (Piras *et al.*, 2020). Moreover, SecTro supports the designers during the security modelling activities and assists them in producing the output based on these activities (Pavlidis *et al.*, 2011).

Secure Tropos is an extension of Tropos methodology that takes security into account (Mouratidis & Giorgini, 2007). Secure Tropos considers the basic Tropos concepts such as dependency, goal, task, resource, and capability and adds security concepts, such as security constraint, secure goal, secure plan, secure resource, and secure capability. The SecTro tool was developed to support the Secure Tropos modeling activities for the creation of the visual models and to assist the designers with the automation of some aspects of the methodology. The main functionalities of the SecTro tool are to support the security modelling activities of Secure Tropos. Therefore, the tool enables the designer to perform security reference modelling, security constraint modelling, secure entities modelling, and secure capability-modelling activities (Pavlidis *et al.*, 2011).

### 2.3 Principles and Design of GDPR Patterns

EDPB (European Data Protection Board) guidelines provide general guidance on the GDPR Data Protection by Design and by Default mandate, requiring the implementation of data protection principles and data subjects' rights and freedoms by design and by default (Bincoletto, 2020).

However, the EDPB guidelines are still high-level and abstract. According to our research on DEFEND EU Project (Piras *et al.*, 2019), pilots (from different important sectors such as banking, healthcare, energy and public administration) found such guidelines are not enough to be used in systematic and comprehensive model supported PbD analysis (Piras *et al.*, 2020). Consequently, this paper started from that structure and, realised on the literature and on the

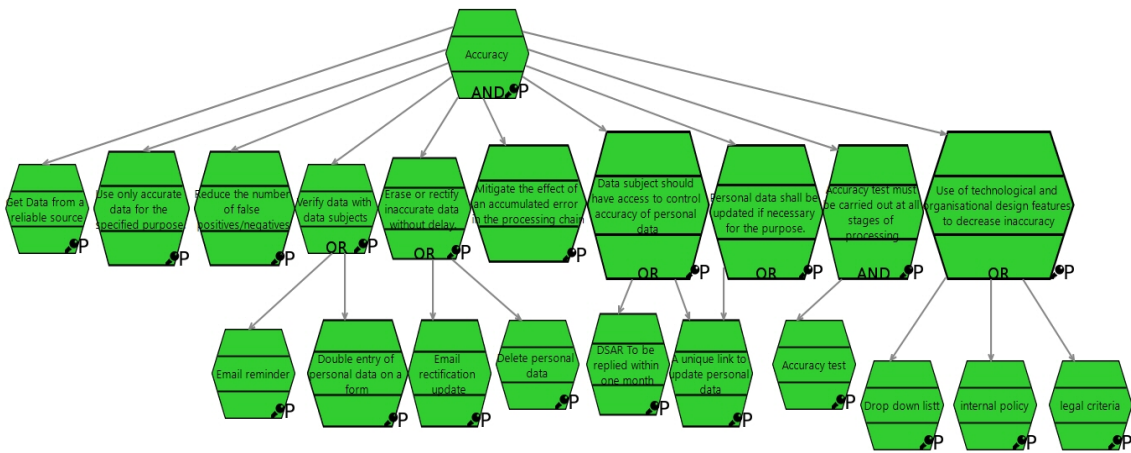


Figure 1: The Pattern of the Accuracy GDPR Principle modeled using SecTro.

best practices from the industry. The new proposed GDPR patterns have been adopted based on our collaboration with the DEFEND pilots (including companies and university privacy/security experts). The baseline elements of our proposed patterns are abstract representing the EDPB guidelines, and further levels can be achieved by extending the abstract layers to more concrete elements.

In the following sub sections, we present our proposed GDPR patterns. These patterns represented as models are provided by SecTro tool. The models aim at supporting the requirements analyst, during PbD modelling analysis, to represent the GDPR principles, and offering ready-to-use concepts, such as privacy and security mechanisms for fulfilling GDPR principles. Due to lack of space, we present the first two patterns, and then, we just summarise the other GDPR principles in one Section.

### 2.3.1 Accuracy

According to the EDPB guidelines, “Personal data shall be accurate and kept up-to-date, and every reasonable step must be taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay” (Bincoletto, 2020). Other elements of the GDPR, such as data subjects’ rights to rectification and erasure of their personal data, support this notion. This gives the data subject the right to have inaccurate personal data corrected and incomplete personal data completed (Finck & Pallas, 2020). The “right to be forgotten” gives Data Subjects the right to ask that their information be destroyed (Finck & Pallas, 2020).

The key aspects included in our new proposed design pattern implementing the GDPR Accuracy

principle are presented in in Figure 1. These aspects can be summarized as follows:

- The data controller must ensure that data is gotten from a reliable source.
- The controller should verify the accuracy of personal data at various stages of the processing, depending on the nature of data and how frequently it may change.
- Inaccurate data must be erased or corrected as soon as possible by the controller.
- The impact of an accumulated error in the processing chain must be mitigated by controllers.
- Data subjects should have an overview of their personal data and simple access to it so that they can check for accuracy and correct it as needed. Individuals must also be allowed to make a DSAR (Data subject access request) and “to exercise that right easily and at acceptable intervals”, according to the controller. This may demand a review of customer-facing processes and procedures, as well as additional staff training, to ensure compliance with the Regulation’s data access and portability requirements.
- Accuracy testing should be performed at key points to ensure all personal data are correct.

### 2.3.2 Data Minimization

According to the EDPB guidelines, “Only personal data that is adequate, relevant and limited to what is necessary for the purpose shall be processed” (Bincoletto, 2020).

Data minimization as the name implies requires that data collection is minimized to only the purpose it is intended for. This involves the controller

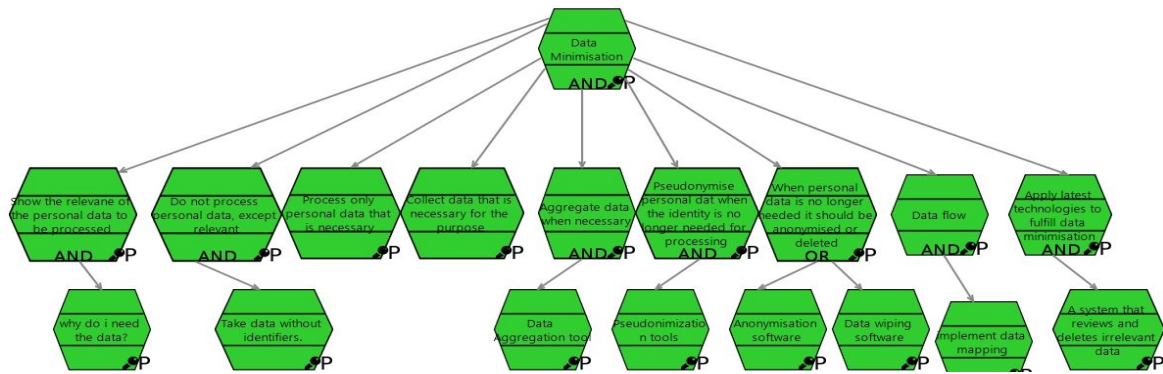


Figure 2: The pattern of the Data Minimisation GDPR Principle modeled using SecTro.

avoiding personal data processing where possible except when necessary, demonstrating the relevance of the personal data processed. Avoid creating more copies of personal data by having an efficient data flow. Figure 2 shows our proposed pattern for the data minimisation principle implemented on the top of SecTro tool as mechanisms entities.

Some of the key aspects included in our new proposed design pattern implementing the data minimisation principle are:

- Aggregate personal data when possible. Data aggregation technologies integrate data from numerous sources into a single location to gain new insights and uncover new linkages and patterns. Ideally, without losing track of the source data and its history.
- Pseudonymize personal data when the identifier is no longer needed, and store the identification key separately.
- When personal data is no longer needed, it should be anonymised or deleted.
- The data flow must be efficient enough that no additional copies or entry points for data collecting are required. This can be facilitated by data mapping.
- Finally, the controller should implement the criteria of “State of the art” which requires controllers to keep up with technological advancements to ensure that data minimisation principles are implemented effectively in the future (Bincoletto, 2020).

### 2.3.3 Other GDPR Principles

Other GDPR principles must be considered during the modelling process, such as integrity and confidentiality, transparency, lawfulness, fairness, and storage limitation. The security attributes of confidentiality, integrity, and availability are included in the security principle, which increase data

processing resilience. To reinforce principles and allow individuals to exercise their rights in a seamless manner, personal data security must both prevent data breach occurrences and promote the appropriate execution of data processing duties, independent of individuals (Bincoletto, 2020). The controller must be transparent and upfront with the data subject about how they will collect, use, and share personal data. Transparency makes easier for data subjects to understand and, if necessary, exercise their rights (Bincoletto, 2020).

The controller must identify a valid legal basis for the processing of personal data. Measures and safeguards put in place to support the concept of lawfulness should also support the requirement that the entire processing life cycle is compliant with the appropriate legal grounds for processing (Bincoletto, 2020).

Fairness is a broad principle that states that personal data should not be processed in a way that is harmful, discriminating, surprising, or misleading to the data subject. Measures and safeguards that implement the idea of fairness protect data rights and freedoms (Bincoletto, 2020).

Personal data must be maintained in a form that allows data subjects to be identified for no longer than is required for the purposes for which they are processed, according to the controller. The controller must understand exactly what personal data the organisation processes and why (Bincoletto, 2020).

### 2.4 SecTro Extension

Our proposed GDPR patterns were integrated as models on the top of SecTro tool. More specifically, we enriched the currently supported library of SecTro with our privacy and security patterns as models. Hence, the analyst can use our patterns via the library and integrate them with the PbD analysis, and other views of SecTro. For example, the patterns of Figures



1 and 2 can be added into the privacy by design view of SecTro to model the GDPR principles. The analyst can drag and drop the required model (green bold in the Figure). Each addressed GDPR principle has its own model in the library. The privacy by design view of SecTro presented in Section 3 shows an example about how the model will appear after using our proposed patterns.

### 3 CASE STUDY AND EVALUATION

The functionality of the extended SecTro tool, alongside with the models created by using our GDPR patterns, will be demonstrated using a real case scenario from the DEFEND Project (Piras *et al.*, 2020). The preliminary case study was originally conducted by (Maguire, 2001) and (Wohlin *et al.*, 2012). We considered the complete case study performed within the EU DEFEND Project (Piras *et al.*, 2019) related to healthcare, and we repeated it by using the extended SecTro tool, this time by using our new proposed GDPR patterns. We compared the resulting mechanisms offered by the GDPR patterns, we designed, compared to the mechanisms identified within the DEFEND case study for fulfilling GDPR principles (e.g., accuracy, integrity and confidentiality, etc.). Accordingly, we performed quantitative and qualitative analysis: quantitative by identifying per principle how many mechanisms have been identified in the DEFEND case study before and after the use of our proposed GDPR patterns, and qualitative on the basis of the overall solution and concepts provided by each model fulfilling a principle.

In the next paragraph, we briefly introduce the scenario and the case study adopted from DEFEND project (Piras *et al.*, 2019). The scenario can be summarized as follows: a healthcare facility, with an electronic record, aims to improve its GDPR compliance. The healthcare facility collects and manages the patient medical record, and obtains supervisory approval for any modifications made to it. These modifications can be adding new medical results or records as well as defining data retention periods (Piras *et al.*, 2019). Ensuring that only accurate medical data is collected, while limiting personal data collection to the purpose it was intended for. Data from the hospital should not be stolen or compromised, for example, in the case of possible threats and data breaches. As a result, the hospital must analyse, create, and implement a monitoring

system for those possible issues (Piras *et al.*, 2019). Some of the relevant aspects to consider: the Hospital collects data about the patients; the Hospital staff access data to add and update medical records (unless authorised by default). Only staff assigned to a patient can view and edit medical record at the time of appointment.

The application of the previous scenario using the extended version of SecTro which supports our new proposed GDPR patterns can be summarized in two phases. In the first phase, the organisational analysis is performed. During this phase, the structure of the organization will be defined by identifying the key scenario concepts, such as actors, departments, divisions, third parties, involved during data processing activities. Fig 3 presents the organisational view of our case study modeled using SecTro tool. The scenario has been represented using numerous goals, and each goal has been assigned to a related requirement. For example, we have modeled some aspects, such as the Doctor must obtain patient medical results from an employee, and such information must be kept discreetly and handled with integrity. This task must remain anonymous while the doctor performs a patient examination or updates the patient's medical records. On the other hand, a Supervisor who should create an account must validate the data. Any changes made by the doctor to the patient's medical records must be performed under GDPR principles (Alkubaisy *et al.*, 2021). In the first phase, we identify the organisational elements for representing the dynamics between actors. Most of GDPR principles will be modeled in the second phase, where the analyst is supported by our GDPR patterns.

In the second phase, the Privacy-by-Design Analysis supported with GDPR Patterns is performed. Based on the organisational concepts and dynamics modeled during the organisational view, it is possible to perform the PbD design analysis by using our GDPR patterns as shown in Fig. 4. We identified for each activity of an actor, the GDPR principles that should be satisfied. These principles are modeled, in SecTro, as privacy requirements and are supported by using our ready-to-use GDPR patterns. For example, the doctor updates patients' medical records in the hospital system which requires various GDPR principles, including the Accuracy, Integrity and Confidentiality principles, as shown in Figure 4. In fact, personal data that is inaccurate may jeopardise data subjects' rights and freedoms.

Table 1 below shows a comparison between the number of mechanisms identified in the DEFEND Case Study before and after the application of our

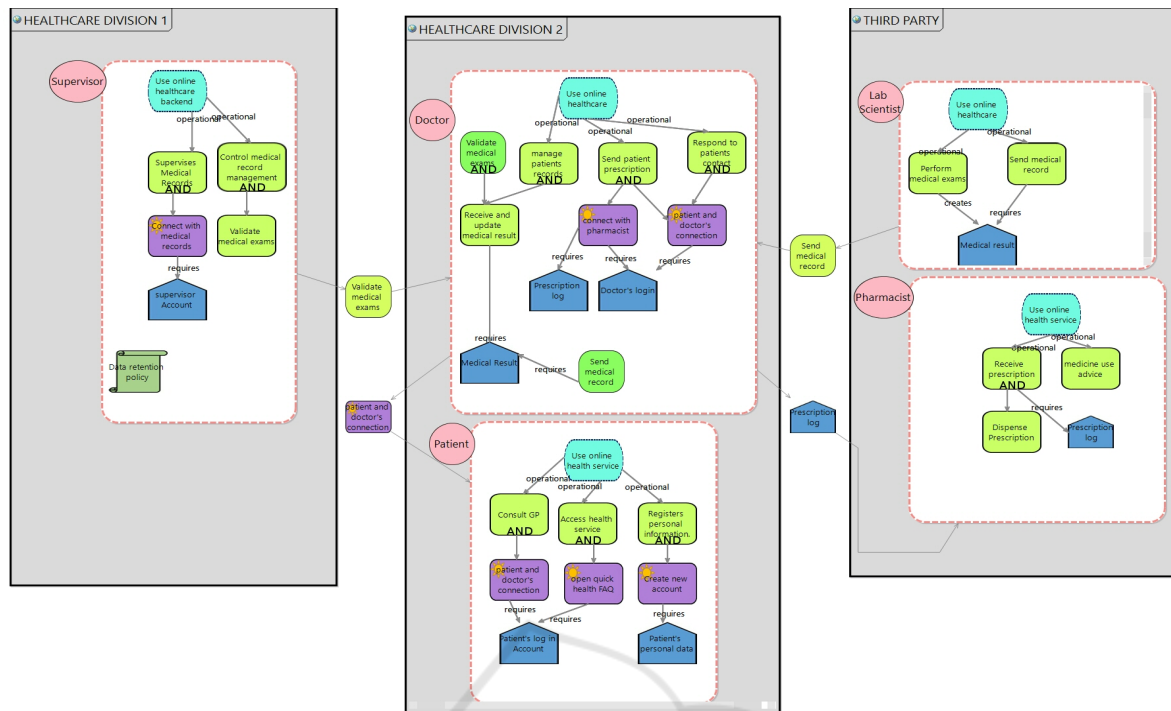


Figure 3: The Case Study Modeled using the Organisational View of SecTro.

proposed GDPR patterns. As Table 1 illustrates, more mechanism were identified after the application of our GDPR patterns. The new proposed GDPR patterns presented in this paper helped in identifying more mechanisms and potential alternatives, per GDPR principle, than the ones of the original DEFEND case study. This is particularly evident in relation to Integrity and Confidentiality, and Transparency principles. Concerning Accuracy principle (Table 1), the advantage is slightly less important, but still valuable. Regarding the Accountability principle, the original DEFEND case study identified three mechanisms. After the application of our GDPR patterns, Zero mechanism identified.

Table 1: GDPR Mechanisms Comparison between DEFEND Case Study and this one.

GDPR Principle	Number of mechanisms in the DEFEND case study before the application of our GDPR patterns	Number of mechanisms in the DEFEND case study after the application of our GDPR patterns
Accuracy	0	4
Integrity and Confidentiality	2	33
Transparency	0	12
Accountability	3	0

This is because we have not developed an Accountability GDPR pattern. Moreover, based on Table 1, and on our qualitative observations on the overall models produced by SecTro, in particular the one of Fig. 4 with the GDPR patterns, we noticed that the subject case study helped the analyst in PbD modeling analysis, by representing GDPR principles and considering relevant ready-to-use alternatives, towards achieving GDPR compliance. The extended version of SecTro provides the analyst with a set of patterns as models, for GDPR principles, which can be used by the analyst for performing PbD modelling, and checking current compliance of the modelled system with GDPR principles.

Our study has different limitations, which will be handled in our future work. For example, we only considered the principles indicated in Table 1, and in our future work we will take into account more principles. We will also involve more participants and actors in the case study. Moreover, we will consider other different scenarios from other fields.

## 4 RELATED WORK

VICINITY is an IoT platform that addresses IoT security and privacy challenges to provide a comprehensive and reliable solution. VICINITY

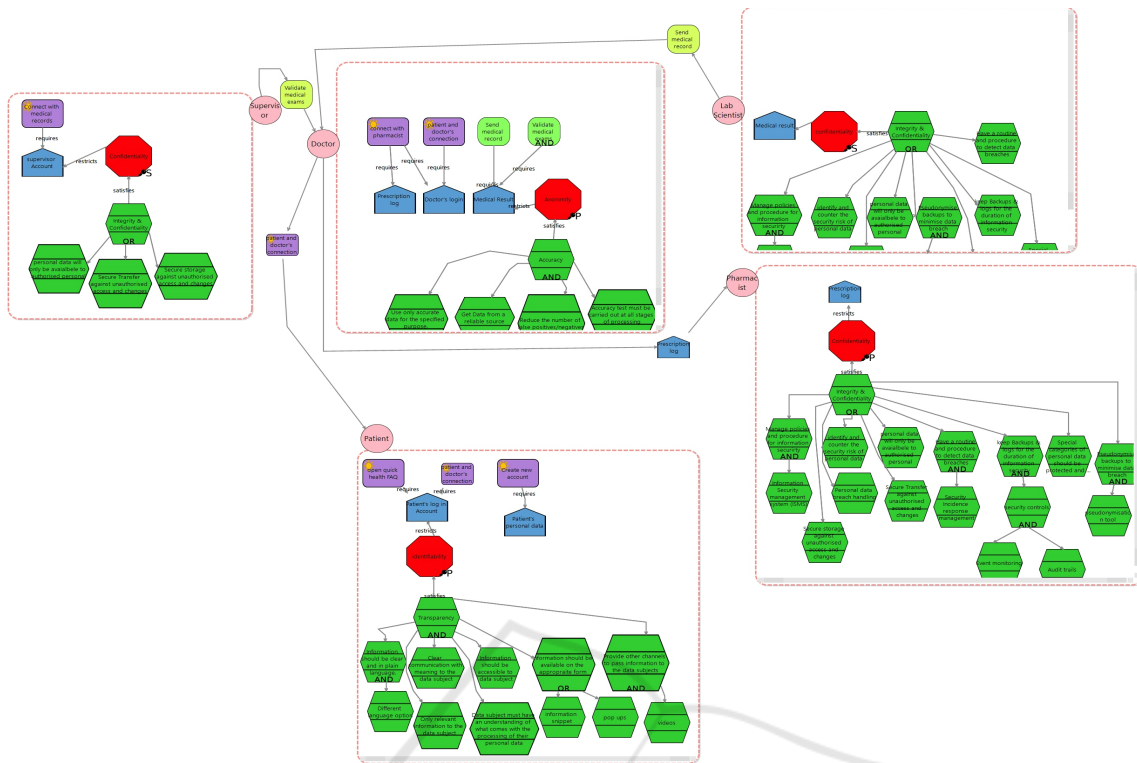


Figure 4: The Case Study Modeled using the Privacy-by-Design View of SecTro where GDPR Patterns implemented (bold green concepts).

allows users with the appropriate role to register their IoT devices and services, discover other registered Things, and enable their Things to be discovered, all while adhering to the privacy limits they set (Koutli *et al.*, 2019). Compared to our work, VICINITY is specifically related to IoT and has been designed ad-hoc towards implementation of GDPR principles for the healthcare. Our GDPR patterns are oriented towards requirements engineering and analysis, and offer generic patterns that can be used to analyse heterogeneous scenarios. We applied our GDPR patterns to a healthcare scenario, and due to the patterns flexibility, it will be possible to use them for modeling analysis within other areas. The work of Amato *et al.* provides a valuable solution that is specific for the important area of e-health systems (Amato *et al.*, 2021). Specifically, a security and privacy validation approach has been developed. To build a comprehensive model for the system that can be analysed using automated model checking and ontology-based reasoning techniques, a methodology for the validation of security and privacy policies in a complex e-Health system was used.

Diamantopoulou *et al.* state that delivering innovative information will aim to contribute to the ecology of e-Participation approaches, notably

crowdsourcing environments. Participants on such platforms may expose sensitive categories of their personal data, compromising their privacy. The key conclusions were of interest to e-Participation organizations. In order to ensure that all of the minimal requirements for the implementation of a compliance framework were met, the public administrations facing GDPR inspections should adopt a methodology. Diamantopoulou *et al.* focused on e-participation and collaboration approaches. In particular, these approaches are oriented towards crowdsourcing environments. Our work is oriented towards providing reference GDPR patterns that can be applied in a wide range of heterogeneous scenarios. Tomashchuk *et al.* conducted a comparison analysis of the privacy and security requirements for e-Health IoT applications (Tomashchuk *et al.*, 2020). They compared between the legal criteria set by the EU’s General Data Protection Regulation (GDPR) and China’s Cybersecurity Law (CSL) into technological requirements for a generic eHealth IoT system. Caruccio *et al.* presented a methodology that exploits relaxed functional dependencies (RFDs) to automatically identify data that could imply the values of sensitive ones, which permits to increase the

confidentiality of a dataset while reducing the number of values to be obscured (Caruccio *et al.*, 2020).

## 5 CONCLUSION

This paper extended SecTro, a requirements modelling tool, to include privacy patterns that incorporate GDPR principles. The extended version of SecTro provides the analyst with a set of patterns as models, for GDPR principles, which can be used by the analyst for performing PbD modelling, and checking current compliance of the modeled system with GDPR principles. The most recent guidelines and relevant documentation on GDPR have been used to identify and design the required privacy patterns, together with relevant literature and collaboration with privacy/security experts (from companies and universities) involved within the DEFEND EU Project. The privacy patterns have been implemented on the top of SecTro, and evaluated using a healthcare scenario where the analyst can model the privacy aspects at early requirements analysis stages. The evaluation results suggest that our proposed GDPR patterns can help analysts in PbD modeling analysis, by representing GDPR principles and considering relevant ready-to-use alternatives, towards achieving GDPR compliance.

## REFERENCES

- Alkubaisy, D., Piras, L., Al-Obeidallah, M., Cox, K., & Mouratidis, H. (2021). Confls: A tool for privacy and Security Analysis and Conflict Resolution for supporting GDPR compliance through privacy-by-design. *Proceedings of the 16th International Conference on Evaluation of Novel Approaches to Software Engineering*.
- Amato, F., Casola, V., Cozzolino, G., De Benedictis, A., Mazzocca, N., & Moscato, F. (2021). A security and privacy validation methodology for e-health systems. *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, 17(2s), 1-22.
- Bincoletto, G. (2020). EDPB Guidelines 4/2019 on Data Protection by Design and by Default. *Eur. Data Prot. L. Rev.*, 6, 574.
- Caruccio, L., Desiato, D., Polese, G., & Tortora, G. (2020). GDPR compliant information confidentiality preservation in big data processing. *IEEE Access*, 8, 205034-205050.
- Diamantopoulou, V., Androutopoulou, A., Gritzalis, S., & Charalabidis, Y. (2020). Preserving digital privacy in e-participation environments: Towards GDPR compliance. *Information*, 11(2), 117.
- Finck, M., & Pallas, F. (2020). They who must not be identified—distinguishing personal from non-personal data under the GDPR. *International Data Privacy Law*, 10(1), 11-36.
- Koutli, M., Theologou, N., Tryferidis, A., Tzouvaras, D., Kagkini, A., Zandes, D., ... & Vanya, S. (2019, May). Secure IoT e-Health applications using VICINITY framework and GDPR guidelines. In *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)* (pp. 263-270). IEEE.
- Maguire, M. (2001). Methods to support human-centred design. *International journal of human-computer studies*, 55(4), 587-634.
- Mouratidis, H., & Giorgini, P. (2007). Secure tropos: a security-oriented extension of the tropos methodology. *International Journal of Software Engineering and Knowledge Engineering*, 17(02), 285-309.
- Pavlidis, M., Islam, S., & Mouratidis, H. (2011, June). A CASE tool to support automated modelling and analysis of security requirements, based on secure tropos. In *International Conference on Advanced Information Systems Engineering* (pp. 95-109). Springer, Berlin, Heidelberg.
- Pavlidis, M., Mouratidis, H., & Islam, S. (2012). Modelling security using trust based concepts. *International Journal of Secure Software Engineering (IJSSSE)*, 3(2), 36-53.
- Pavlidis, M., Mouratidis, H., Panaousis, E., & Argyropoulos, N. (2017, August). Selecting security mechanisms in secure tropos. In *International Conference on Trust and Privacy in Digital Business* (pp. 99-114). Springer, Cham.
- Piras, L., Al-Obeidallah, M. G., Pavlidis, M., Mouratidis, H., Tsohou, A., Magkos, E., ... & Crespo, B. G. N. (2020, September). DEFEND DSM: a data scope management service for model-based privacy by design GDPR compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 186-201). Springer, Cham.
- Piras, L., Al-Obeidallah, M. G., Praitano, A., Tsohou, A., Mouratidis, H., Gallego-Nicasio Crespo, B., ... & Zorzino, G. G. (2019, August). DEFEND architecture: a privacy by design platform for GDPR compliance. In *International Conference on Trust and Privacy in Digital Business* (pp. 78-93). Springer, Cham.
- Tomashchuk, O., Li, Y., Landuyt, D. V., & Joosen, W. (2020, June). Operationalization of privacy and security requirements for eHealth IoT applications in the context of GDPR and CSL. In *Annual Privacy Forum* (pp. 143-160). Springer, Cham.
- Voigt, P., & Von dem Bussche, A. (2017). The eu general data protection regulation (gdpr). *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, 10(3152676), 10-5555.
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., & Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media.