

# **Uncovering privacy threats with Soft Systems Methodology**

**Development of a privacy threat modelling method for  
today's needs**

Tuisku Sarrala

Master's thesis

February 2021

Technology

Master's Degree Programme in Cyber Security

Author(s) Sarrala, Tuisku	Type of publication Master's thesis	Date February 2021 Language of publication: English
	Number of pages 83	Permission for web publication: yes
	Title of publication <b>Uncovering privacy threats with Soft Systems Methodology</b> Development of a privacy threat modelling method for today's needs	
Degree programme Master's Degree in Cyber Security		
Supervisor(s) Kokkonen, Tero; Hautamäki, Jari		
Assigned by Nixu Oyj		
Abstract  <p>While identifying compliance-based privacy threats is common, methods for eliciting context-based privacy threats are lacking, even though there is an increasing need for this. The processing of personal data and the systems involved in it are getting increasingly complex, interlinked, ubiquitous and central to people's lives. Data protection legislation has tightened, people's privacy awareness has increased, and ethics has become a strategic trend, placing pressure on organisations to examine their personal data processing activities for privacy threats and, especially, harmful impact on people.</p> <p>Soft systems methodology (SSM), which was designed to help to understand complex problematic situations and to instigate change in them, was proposed as a solution in the research question "How can privacy threat modelling of complex systems be improved with the soft systems approach?". To answer this, constructive research method was used to develop a privacy threat modelling method that utilises SSM. The developed method, titled Taiga, was piloted in a real setting, which showed that it could produce relevant privacy threats in an efficient manner.</p> <p>The research recognised that privacy is a multifaceted issue and concluded that privacy threat modelling should be divided in two threads, one for compliance aspects and another for threats emerging from the functioning of the target in its context. SSM helps to identify the latter kind of threats that would otherwise be difficult to uncover. The main limitations of the research were that only two pilots were available, and the targets were of a relatively low complexity. Improvements to the Taiga method were identified with further pilots in mind. Development from a proof of concept to a method readily usable by consultants in a professional setting should be a longer-term goal.</p>		
Keywords/tags ( <a href="#">subjects</a> )  threat modeling, privacy risk, privacy, GDPR, systems thinking, soft systems methodology		
Miscellaneous ( <a href="#">Confidential information</a> )  n/a		

Tekijä(t) Sarrala, Tuisku	Julkaisun laji Opinnäytetyö, ylempi AMK	Päivämäärä helmikuu 2021
	Sivumäärä 83	Julkaisun kieli englanti
		Verkojulkaisulupa myönnetty: kyllä
Työn nimi <b>Uncovering privacy threats with Soft Systems Methodology</b> Development of a privacy threat modelling method for today's needs		
Tutkinto-ohjelma Master's Degree in Cyber Security		
Työn ohjaaja(t) Tero Kokkonen, Jari Hautamäki		
Toimeksiantaja(t) Nixu Oyj		
Abstract  Uhkia tietosuojan vaatimustenmukaisuudelle osataan tunnistaa, mutta menetelmät puuttuvat sellaisten tietosuojan ja yksityisyyden uhkien tunnistamiseen, jotka nousevat järjestelmien toiminnasta kontekstissa ja henkilötietojen käsittelystä itsestään. Käsittelystä ja järjestelmästä on tulossa yhä monimutkaisempia, linkitetympiä, kaikkialle levinnyttä ja keskeistä elämässä. Samanaikaisesti tietosuojalainsäädäntö on kiristynyt, ihmisten tietoisuus lisääntynyt ja etiikasta on tullut strateginen trendi, mikä vaatii organisaatioita olemaan kattavasti selvillä käsittelyn aiheuttamista uhista tietosuojalle ja yksityisyyden suojalle, ja erityisesti käsittelyn haitallisista vaikutuksista ihmisille.  Pehmeä systeemimetodologia (SSM) on tarkoitettu monimutkaisten ongelmatilanteiden ymmärtämiseen ja parantamiseen, ja sitä ehdotetaan ratkaisuksi tutkimuskysymykseen "Kuinka monimutkaisten järjestelmien yksityisyyden suojan ja tietosuojan uhkamallinnusta voidaan parantaa systeemisellä lähestymistavalla?". Vastauksena kehitettiin konstruktiivisella tutkimusotteella uhkamallinnusmenetelmä, joka hyödyntää SSM:aa. Taiga-menetelmäksi nimettyä menetelmää pilotoitiin todellisessa kohteessa, mikä osoitti sen avulla voitavan tehokkaasti tunnistaa merkityksellisiä, kontekstilähtöisiä uhkia.  Tutkimuksessa todettiin, että uhkamallinnuksessa tulee erotella vaatimustenmukaisuuden tarkastelu ja kontekstilähtöisten uhkien tunnistaminen. SSM auttaa tunnistamaan nimenomaan kontekstilähtöisiä uhkia, joita olisi muuten vaikea löytää. Tutkimusta rajoitti pilottien vähäinen määrä sekä kohteiden matala kompleksisuus. Seuraavia pilotteja varten ehdotettiin mahdollisia parannuksia Taiga-menetelmään. Menetelmän kehittäminen edelleen konsulttikäyttöön on asetettu pidemmän aikavälin tavoitteeksi. Tämä tutkimus osoitti konseptin toimivuuden.		
Avainsanat ( <a href="#">asiasanat</a> ) uhkamallinnus, tietosuojariskit, tietosuoja, yksityisyydensuoja, GDPR, systeemijattelu, pehmeä systeemimetodologia		
Muut tiedot ( <a href="#">salassa pidettävät liitteet</a> ) n/a		

## Contents

<b>Abbreviations .....</b>	<b>4</b>
<b>1 Introduction.....</b>	<b>5</b>
<b>2 Research methodology .....</b>	<b>7</b>
2.1 Research question and objectives .....	7
2.2 Research methodology .....	8
2.3 Constructive research method .....	10
2.4 Evaluation.....	12
2.5 Research ethics.....	14
<b>3 Data protection and privacy .....</b>	<b>16</b>
3.1 Terminology in legal and professional context .....	16
3.2 Aspects of privacy .....	18
<b>4 Privacy threat modelling.....</b>	<b>20</b>
4.1 Descriptions of selected methods .....	20
4.1.1 PRIAM .....	20
4.1.2 Design science approach .....	21
4.1.3 DPIA, UK Information Commissioner’s Office.....	22
4.1.4 Elevation of privacy .....	24
4.1.5 LINDDUN .....	24
4.1.6 Seattle residents’ privacy threat model .....	25
4.2 Analysis and discussion of the methods .....	27
<b>5 Systems thinking, complexity and Soft Systems Methodology.....</b>	<b>29</b>
5.1 The rise of systems approaches .....	29
5.2 Complexity science .....	30
5.3 Soft systems methodology .....	32

	2
5.4 Applications of SSM .....	34
<b>6 Innovation and testing of the method .....</b>	<b>37</b>
6.1 Setting up .....	37
6.2 Drafting the method .....	39
6.3 The first pilot .....	47
6.3.1 Interview (for models) .....	48
6.3.2 GDPR compliance workshop .....	49
6.3.3 Debate workshop .....	50
6.3.4 Threat catalogue .....	52
6.3.5 Learning from the pilot .....	54
6.4 Review with privacy specialists .....	56
6.5 The second pilot .....	56
6.6 Ending the innovation phase .....	57
<b>7 Results and discussion .....</b>	<b>58</b>
7.1 Success factors .....	59
7.2 Implementation .....	60
7.3 Effects and value to stakeholders .....	62
<b>8 Conclusions .....</b>	<b>63</b>
8.1 Limitations and future research .....	64
8.2 Wider effects .....	65
<b>9 References .....</b>	<b>68</b>
<b>10 Appendices .....</b>	<b>73</b>
Appendix 1. Stakeholder evaluation needs .....	73
Appendix 2. Summary table of privacy threat modelling methods .....	74
Appendix 3. Privacy threat modelling method marketing leaflet .....	76
Appendix 4. First draft of Taiga .....	77

Appendix 5. Hard aspects .....	80
Appendix 6. Excerpts from the Learning journal .....	81

## Figures

Figure 1: Constructive research method with an embedded learning cycle .....	10
Figure 2: Research permission contents .....	15
Figure 3: EU and international privacy and data protection rights .....	18
Figure 4: SSM action learning cycle .....	33
Figure 5: First draft of Taiga method overview .....	43
Figure 6: First draft, System definition - Step 1a .....	45
Figure 7: First draft, template for the inquiry device .....	45
Figure 8: First draft, Profile / persona template.....	46
Figure 9: First pilot, Model built from the data subject's view .....	49
Figure 10: First pilot, Model from the view of causing harm to data subjects .....	49
Figure 11: First pilot, model of the official activity (WAI) .....	51
Figure 12: Overview of Taiga method .....	57

## Tables

Table 1: Constructive research method steps and their application in this research project .....	11
Table 2: Approach and data to be collected .....	38
Table 3: First draft, Question set .....	44
Table 4: First pilot, schedule.....	47
Table 5: First pilot, threats produced.....	52
Table 6: First pilot, analysis of how the threats were identified .....	55

## Abbreviations

CJEU	Court of Justice of the European Union
DPIA	Data Protection Impact Assessment
EDPS	European Data Protection Supervisor
ECtHR	The European Court of Human Rights
GDPR	General Data Protection Act
IAPP	International Association of Privacy Professionals
JAMK	Jyväskylä University of Applied Sciences
PIA	Privacy Impact Assessment
PTM	Privacy threat modelling
SSM	Soft Systems Method/Methodology
WAD	Work-as-done
WAI	Work-as-imagined

## 1 Introduction

This research was inspired by two intertwining notions: the systems in which personal data is processed are becoming increasingly complex, and methods for eliciting privacy threats are lacking. Soft systems methodology, which was designed to help understanding highly complex problematic situations and instigate change in them, is proposed as a solution and explored through the research question “How can privacy threat modelling of complex systems be improved with the soft systems methodology?”.

Organisations need to ensure privacy and data protection compliance in their systems, which is a demand placed on them by legislation, data subjects and the organisations themselves. Privacy and data protection legislation has been changing over the years as a response to technological changes. In recent years, the EU General Data Protection Regulation (GDPR) has brought the most impactful changes for companies operating in the EU. The GDPR requires organisations to assess their personal data processing but leaves it open how exactly to carry out these assessments (Regulation (EU) 2016/679). The task is only becoming more difficult as new novel ways of utilising personal data are being invented. Personal data breaches and privacy issues are getting more media attention and consumers’ awareness is on the rise, placing pressure on organisations. One recent example is the huge leak of patient records from psychotherapy provider Vastaamo in Finland (Yleisradio, 2020). While organisations are primarily concerned about the legality and compliance of their personal data processing, individuals are concerned about matters touching them more directly, such as their personal privacy and control over their personal data (Gartner, 2019; Panetta, 2018; Which?, 2018). Additionally, concern over digital ethics has been a rising trend, fuelled by the rise of AI. Gartner has reported privacy and ethics as top 10 technological trends in 2019, 2020 and 2021, including calling companies to move from “Are we compliant?” towards “Are we doing the right thing?” and to support digital ethics and privacy with transparency and traceability (Gartner, 2019; Miller, 2020; Panetta, 2018).



Ethics, data protection and privacy are strongly linked. To satisfy the GDPR, consumers and ethical requirements, organisations need to understand the relevant threats in these areas. Methods for privacy threat modelling in the engineering field exist, but even with GDPR-inspired modifications and additions, they do not fully answer these new human and ethical centred demands. Current methods are largely based on carefully analysing and depicting all the system's constituent parts and data flows. Some methods have a narrow view of what privacy means. Some only consider confidentiality or GDPR compliance requirements. Threats arising from the system's context remain uncovered as only the software components are in scope.

The systems' complexity presents further challenges for threat modelling, especially if the threat elicitation relies on the full dissection of the system. For 2021 trends Gartner paints a picture of people centricity and big data, where the individual is subject to facial recognition, location tracking and such technologies combined with the individual's behaviours, with the resulting decision having direct financial or other impacts on individuals (Miller, 2020). Breaking the system in smaller parts and examining these parts in their isolated static states will reveal very little of the nature of the processing activity as a whole, emergent ethical issues and impacts on people. The desire for 360-degree digitalisation of everything about people means uncountable personal data purposes by uncountable parties and applications, all interacting with each other. New information and new personal data is generated through the interactions and organisations will want to accumulate and retain personal data for future yet unknown purposes that developing advanced technologies bring.

Systems thinking provides a way to approach these multifaceted problematic situations. Systems thinking approach was developed to understand complex systems with high interconnectivity, multiple purposes and the human element, and also to instigate change in them. The approach seems very fitting to privacy threat modelling since the aspects they deal with have significant overlap. The aim of this the thesis is to explore whether systems thinking approach could help privacy threat modelling of complex systems, especially by uncovering issues that arise from the context and are difficult to identify with conventional or "engineering" threat modelling methods. To answer the research question, a new method based on

systems thinking is developed and tested in a real setting and the results are reported.

This research project contributes to a wider international research programme titled Mad@Work, which is described as follows: “[Mad@Work] focuses on the detection and mitigation of poor mental health conditions, such as work stress and burnout, which have not yet resulted in a diagnosed mental health disorder. The Mad@Work research programme aims at a major breakthrough in the development of software-intensive applications that combine multiple heterogeneous environmental and/or wearable data sources into actionable information for improving employees' wellbeing, engagement and performance. Mad@Work will develop truly unobtrusive, privacy-safe, appealing solutions, smoothly integrated into the work environment and appropriate for long-term use in diverse real-life settings.”. (ITEA, 2020)

The privacy threat modelling method to be developed in this project will be piloted on Mad@Work programme participants' solutions, furthering the programme's goals of developing privacy-safe solutions. The sponsor of this research project was Nixu Oyj, a Finnish cybersecurity company, where the author is employed as a senior privacy consultant. Nixu's motivations as the sponsor were to develop its privacy threat modelling practices and to contribute to the Mad@Work programme as one of the participating organisations.

## **2 Research methodology**

### **2.1 Research question and objectives**

The main research question which this thesis is set to answer is: *How can privacy threat modelling (PTM) of complex systems be improved with the soft systems approach?* The following three sub-questions have been formulated to answer the main research question.

- a. What kind of a PTM method achieves this?
- b. How well was the PTM method implemented?
- c. What were the effects of using soft systems approach in PTM?

The question is answered by developing and testing a PTM method based on soft systems methodology (SSM). Additionally, a proof of concept is sought for the use of SSM to in threat modelling. It is hoped that the project results in a PTM method that may be researched and developed further. Further research topics may include the method's efficiency and effectiveness, comparisons to other available methods, and how to productise it for use in a professional setting by a consultant.

## 2.2 Research methodology

Basic research finds answers to the questions “what” and “why” and provides the ground for applied research. Applied research takes the theoretical base and finds answers to the question of “how” (Toikko & Rantanen, 2009, p. 19). In this thesis, the “how” research question is answered through the development of a new threat modelling method in a professional setting. This narrows the method selection to research and development methods where the researcher is an active participant, such as action research or design research, in contrast to quantitative and qualitative research where the researcher takes the stance of an objective outside observer.

Kananen (2013) makes a useful distinction between action research and design research, stating that design research is better suited for the development of non-social things, products and processes and action research for social things and human activities. Since the research question is to be answered by developing a PTM method, which is a process and a non-social thing, a design research method could be chosen. However, the proposed threat modelling method is to be based on the soft systems methodology, a socially immersive action research approach that deals with people-centric issues (Checkland, 2000).

Using the soft systems approach not only for improving PTM but as the main research method was considered, but discarded, since it carries the risk that the project would be poorly framed and potentially uncontrollably expand (Rubin, 2004). However, a combined method can mitigate these risks. The general idea of integrating systems and design methods is supported in literature. Jones (2019) states that “the integration of systemics to enrich design methodologies and practice

has now become imminent.”. He then proceeds to suggest practical models for this, such as mapping various systemic design methods against the five design stages of strategy, discover, design, develop and deploy, with the aim of enhancing the design process but not make it systemic. This approach was not chosen due to its linearity. The research question’s explorative nature called for iterative approach, which is provided in an action research method.

Another way to include soft systems approach in a design method while retaining its iterative action learning nature is to wholly embed it inside the design method. The open-ended systemic learning process would benefit from being placed on a linear process which would formally open and close the enquiry. According to Rubin (2004), when using the soft systems method, overall research methodology needs to be defined as well, and points to the constructive research methodology as a natural solution to this.

The constructive research method was developed by Kari Lukka (Lukka, 2001). It involves seven stages, with an innovation stage (stage number 4) in the middle, which is envisaged to be a creative, heuristic and potentially iterative process. For this reason, Lukka refrains from prescribing a method for the innovation stage, leaving this for the researcher to decide. This creative slot allows the researcher to embed an action learning cycle within the research method and use systemic techniques to support innovation. The constructive method itself includes action research aspects such as iterative inquiry, the expectation for experiential learning and the researcher immersing themselves in the inquiry, rather than posing as an outside observer (Lukka, 2001). These aspects resonate well with the soft systems methodology, which is further analysed in chapter Systems thinking, complexity and Soft Systems Methodology. Overall, the constructive research method aims to produce a construction by supplying a clear frame for the otherwise open-ended innovative cycle. The tailored method for this project is shown in Figure 1.

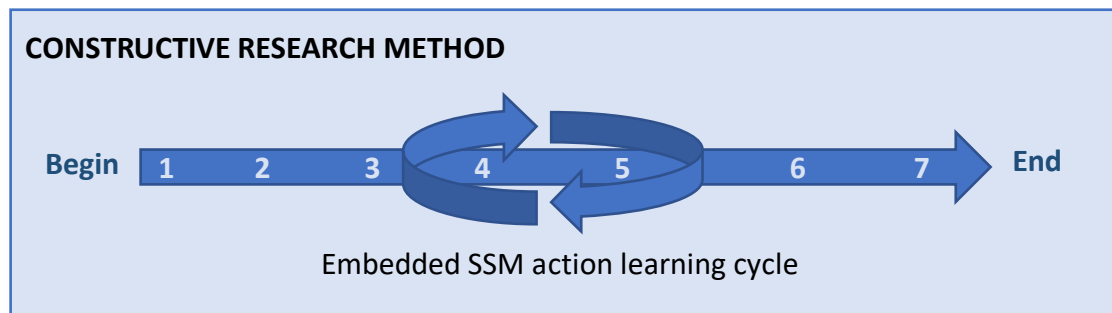


Figure 1: Constructive research method with an embedded learning cycle

### 2.3 Constructive research method

The constructive method with an embedded action learning cycle was chosen as the research method. The method's suitability is examined in more detail in this chapter. The requirements for constructive research are that it focuses on a real-world problem with a need for a solution; innovates a construction to solve it and attempts to implement it, effectively testing in practice; expects experiential learning to arise from the close team-like collaboration of the researcher and representative of the practice; is carefully connected to existing scientific theory base; and especially focuses on reflecting empirical findings back to theory (Lukka, 2001).

The real-world problem in this project was described in chapter Introduction, and the sub-question (a) asks what kind of a PTM method achieves this. The research question to be answered with the development of a new PTM method, which becomes the innovative construction to be developed and tested in a real setting with customers. The PTM method uses a soft systems approach, which gives rise to experiential learning through the creation of systemic models of the real-world situation and debating them with the customer and possibly others. Central to the soft systems approach is that learning is expected to happen about the learning system (i.e., the PTM method) as well as the research target (i.e., threats being identified in the threat modelling target) (Checkland, 2000). The constructive method takes this learning as whole back to the real world by requiring it to be connected to the existing scientific theory base and its findings to be reflected on that. The exact steps of the constructive method are shown on Table 1 alongside with their application in this research project.

Table 1: Constructive research method steps and their application in this research project

Step	Application of method in this project
<b>1. Find a relevant real-world problem</b>	The problem is described in chapter Introduction.
<b>2. Agreement for long-term research collaboration with the target organisation</b>	Long term agreement was made with the research sponsor, Nixu Oyj. Short term agreements were made with the organisations whose projects the method was piloted in, through the Mad@Work research programme.
<b>3. Gain deep theoretical and practical knowledge base for the research topic</b>	The theoretical knowledge base is documented under chapters Data protection and privacy; Privacy threat modelling; and Systems thinking, complexity and Soft Systems Methodology. Practical knowledge was gained through the author's career as a privacy consultant and expanded through the piloting of the method in this project.
<b>4. Innovate a solving model and develop a construction that solves the problem and which could also contribute to the theory</b>	Developing a new method with iterative action learning approach was chosen as the solving model for the research question. The development is described in chapter Innovation and testing of the method.  Action learning approach ensures that learning is reflected to theory in every cycle. The overall contribution to theory is explored in chapter Results and Conclusions.
<b>5. Implement the solution and test it ('market test')</b>	This step is carried out within the previous step. The method is tested in a real setting with customers. This project does not attempt to create a final 'product' as such that goes through final testing, but rather aims to prove the concept.
<b>6. Consider the field of applicability for the solution</b>	Considered in chapters Results and Conclusions from the viewpoint of having proven a concept, together with topics for further research.
<b>7. Recognise and analyse theoretical contribution; either a new construction or dependencies behind the construction</b>	This is documented in chapter Conclusions.

## 2.4 Evaluation

Six different parties have interest in this project, each with their distinct evaluation needs: the researcher, the sponsor, the university, the pilot organisations, and the wider business and academic environment. An analysis of these stakeholders' evaluation needs along with suitable evaluation methods and the relevant project stage in which the evaluation should take place are detailed in Appendix 1. The analysis includes division of the evaluation into accountability, information generation and development evaluations, and on the other hand, to summative and formative evaluations, as suggested by Seppänen-Järvelä (2004, p. 19). The researcher has evaluation needs throughout the project. The sponsor and the university have evaluation needs early in the process when the relevant real-world problem is identified, and the research agreement is made, as well as at the end when the produced benefits and quality of the research can be evaluated. The pilot organisations have interest in the method innovation and testing phase. Evaluation by the wider business and academic environment happens after publication over a longer time period and concerns the wider effects of the research.

The researcher is responsible of embedding evaluation in the whole project. In research and development activities, the word 'research' signifies that critical evaluation is aimed to be part of the development activity (Toikko & Rantanen, 2009, p.156). Checkland (2000) notes that unlike traditional scientific research, action research validity cannot be evaluated by repeating the study and comparing the results, because of its context-dependency and social and human dimensions. The focus should be shifted to the way of knowing: does the epistemology of the research process withstand scrutiny? Scrutiny can be enabled by making the research process transparent and recoverable. This is also recognised by Seppänen-Järvelä (2004, p.22) who states that in open innovative projects evaluation of the process is essential so that its results can be validated and reused. In this project, transparency is largely achieved by reporting the learning cycles in detail in chapter Innovation and testing of the method.

The piloting phase (innovation and testing) plays a significant role in ensuring reliability and objectivity. Lukka (2001) states that in constructive research it proves

that the process which was chosen to develop the construct has been successful and also that the construct itself has been successful. Lindhult (2019), discussing reliability and objectivity in action research, suggests that reliability may be achieved through effectively organised participatory learning process and dynamically adaptive goal-seeking. These are fundamental aspects of the SSM and consequently part of the piloting phase. The customer pilots are participatory, and the method is reviewed with privacy specialists in between. Furthermore, SSM emphasises that the approach in use is continuously monitored and expects it to be dynamically adapted. SSM appears to cover Lindhult's (2019) definition for objectivity in action research, which is the impartial involvement of the interests of various stakeholders; intersubjectivity achieved through the subjective views of many in a democratic dialogic process. Overall Lindhult summarises that objectivity may be achieved through critical subjectivity, intersubjectivity, practical wisdom, impartial norms of inquiry and an open democratic dialogue.

Lukka (2001) states that the researcher must maintain neutral and critical approach in general. True neutrality may not be reachable in action research where the researcher is immersed in their own research. Instead, critical subjectivity, self-reflection and awareness of one's own biases should be sought (Lindhult, 2019). One way to bring this about is keeping a learning journal, which helps the researcher to monitor the situation simultaneously at various levels and to retain a critical approach. In this project, a learning journal with a list of headings was used to ensure all aspects were monitored: date, what I have done (facts), intuitions/ideas, problems/conflicts, about me (emotions, approach, bias etc.), about the learning cycle (e.g. where I am in the learning cycle), about the research method (e.g. is it helping me to answer the research question, are adjustments needed) and about the PTM method (e.g. is it becoming more effective). Excerpts from the journal have been included in Appendix 6.

The learning cycle in action research contributes to research validity. Toikko and Rantanen (2009, p. 156) note that in development activities, as opposed to research, the essence is in the usefulness of the information produced, and that experience-based information can hold equal value to information generated by research. This could be taken as the 'practical wisdom' that Lindhult (2019) refers to. In research



and development activities the researcher needs to make a choice how much weight to give to each of the theoretical/research and experience/development sides. Checkland's (2000, p. S12) choice was not to let either the ideas or the experiences dominate. This project aims for achieving an ongoing dialogue between theory and practice through the learning cycle as the instrument. The action learning cycle contains a built-in evaluation step, and the SSM promoting learning not only of the research target but also of the learning system keeps the research method under continuous scrutiny.

Within action research and systems approaches, which are further explored under the section Systems thinking, complexity and Soft Systems Methodology, the idea of objectivity is regularly challenged. Within that tradition of science, topics such as can reality exist independent of the viewer, multiple perspectives, the researcher's own worldview and how to approach the subjective are discussed. Hence, the measures for ensuring objectivity and reliability also differ from that of traditional sciences. On the whole, achieving reliability and objectivity in action research requires special effort from the researcher which is taken into account in this project.

## 2.5 Research ethics

This research project followed the ethical guidelines from the Finnish Advisory Board on Research Integrity (Finnish Advisory Board on Research Integrity, 2013). The research was carried out with integrity, meticulousness and the appropriate level of accuracy required by the research question. In the innovation and testing stage customer engagement was necessary to acquire data. The approach taken is described below. A written cooperation agreement was made between the research sponsor (Nixu Oyj, the employer of the researcher), the researcher and the university regarding the rights, responsibilities, obligations, publicity and confidentiality relating to the research. No compensation was offered for the work besides the researcher's regular salary as an employee to the sponsor. No conflicts of interest were identified. The project respects copyright and IPR rights. All sources used have been referred to according to JAMK project reporting instructions (Stevens & Crawford, 2020). All software used was properly licenced. Since the thesis topic relates to cyber security,

it should be stated that the results have been presented in such a way that they cannot be used for malicious purposes by a third party.

The organisations for the pilots were approached through the international Mad@Work research programme, which they were participating in and which this research project is also contributing to. Therefore, the organisations were already committed to the furthering of research in this area. The participating companies were approached by an open offer to carry out PTM with a SSM enhanced method, as shown in Appendix 3. Once a company had expressed interest, a kick-off meeting was held where the process was clarified, and the ethical principles shown in Figure 2 were established. This was verbally iterated at the beginning of the workshops. No ethical review was necessary for this research project.

#### Research permission

... I also need to ask you for an agreement to that you are happy for this [PTM exercise] to contribute to my research. I am writing a thesis for my Masters in Cyber Security degree at Jyväskylä University of Applied Sciences. As my research topic I am developing a new privacy threat modelling method that utilises systems thinking. I am now testing the method in different projects, through the Mad at Work programme. Please could you confirm you're are happy for the information from the session to be used for the research. We can discuss this on [date] if you have any questions. I will be collecting data and reporting on:

- Types of stakeholders at the meetings, e.g. Technical specialist, business owner, user
- Brief description of threat modelling target
- Headlines of privacy threats found
- General remarks of the use of the method
- General closing comments from the participants, anonymous (e.g. was it useful, how did you find it)

I will not report the company name or identify individuals although these may be derived from the Mad@work connection. The research concentrates on the use and development of the tool. ...

[contact details]

Figure 2: Research permission contents

No directly identifiable personal data was required for the research project. Comments from participants were recorded at a general level during project meetings, and if relevant, the type of role for the person was recorded alongside the comment (such as 'technical' or 'project lead'). Word by word comments were not required. These meeting notes contain information that may be classed as personal data, since they include the participant names and general comments that may be attributed to them through their job types. The purpose of personal data processing was scientific research in the field of cyber security, privacy and data protection. The meeting notes will be retained securely by the researcher until they do not fulfil this purpose anymore.

### **3 Data protection and privacy**

#### **3.1 Terminology in legal and professional context**

This chapter explores the terms privacy and data protection. The terms are often used interchangeably but there are the differences and conflicts between different sectors' and jurisdictions' definitions for them. The International Association of Privacy Professionals (IAPP) states that the definition of privacy depends on who you ask (International Association of Privacy Professionals, n.d.b). IAPP defines privacy as 'the right to be let alone' in line with the United States (US) privacy tradition which arises from Warren and Brandeis' 1890 publication where privacy was defined as an individual's right to private life that is not published to the others. The definition links to the advent of photo capturing methods and the press starting to publish stories of individuals (Warren & Brandeis, 1890). IAPP separately defines 'information privacy' as individuals' control over how their data is collected (n.d.a). This mirrors Alan Westin's 1967 privacy definition (as cited in Reynolds, O. M., 1969): privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Westin also recognises the need to continually adjust and balance what is disclosed. IAPP defines also a third related term, 'data privacy', as the appropriate governance of personal data, somewhat mirroring the GDPR term 'data protection' (n.d.a). In US legislation similar to the GDPR, such as in the California Consumer Privacy Act, the word privacy

is used, as opposed to the term data protection that is in use in Europe in the personal data governance context (Blitz, 2017). Hence, the US 'privacy' may mean the same as the European 'data protection'.

To mix the issue, in Europe the two terms are distinct. The Charter of Fundamental Rights of the European Union presents privacy and data protection as two separate fundamental rights, with privacy meaning the preservation of people's privacy and data protection meaning fair, purpose-specific and lawful use of people's data (European Union, 2012). The GDPR was set up to implement the latter. As if to underline the distinction, the GDPR does not in fact contain the word privacy at all. It refers to fundamental rights which should be protected and the right to private and family life is one of these rights (Regulation (EU) 2016/679). Privacy is widely recognised as a fundamental right across the globe, and in addition to the Charter of Fundamental Rights of the EU, it appears for example in the UN human rights declaration (United Nations General Assembly, 1948) and the European Convention on Human Rights (Council of Europe, 2010).

European courts' decisions further illustrate the terms' multifaceted nature. the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECtHR), internationally influential European courts, appear to treat the right to data protection as an expression of the right to privacy. ECtHR has applied the EU Fundamental Charter Article 8, the right to privacy, to mean that information about a person's private life should be safeguarded. Data protection is different since applies to *all* personal data, not just what might be considered "private". Important points to note are that even if personal data is processed in line with the right to data protection, it may still interfere with the right to privacy, and that the right to data protection may include additional protections to those that the right to privacy offers. (Kokott & Sobotta, 2013)

Figure 3 gives an overview of the articles in EU privacy and data protection legislation and charters. The EU Fundamental Rights Charter Article 7 mirrors Article 8 in The European Convention of Human Rights and they should be interpreted the same way (European Union Agency for Fundamental Rights, n.d.). The European Convention on Human Rights definition additionally defines that public authorities shall not interfere with this right, implying that they may be a threat to privacy through e.g.

surveillance of citizens. The Universal Declaration of Human Rights explicitly states that no one should be subject to “attacks upon his honour and reputation” (United Nations General Assembly, 1948).

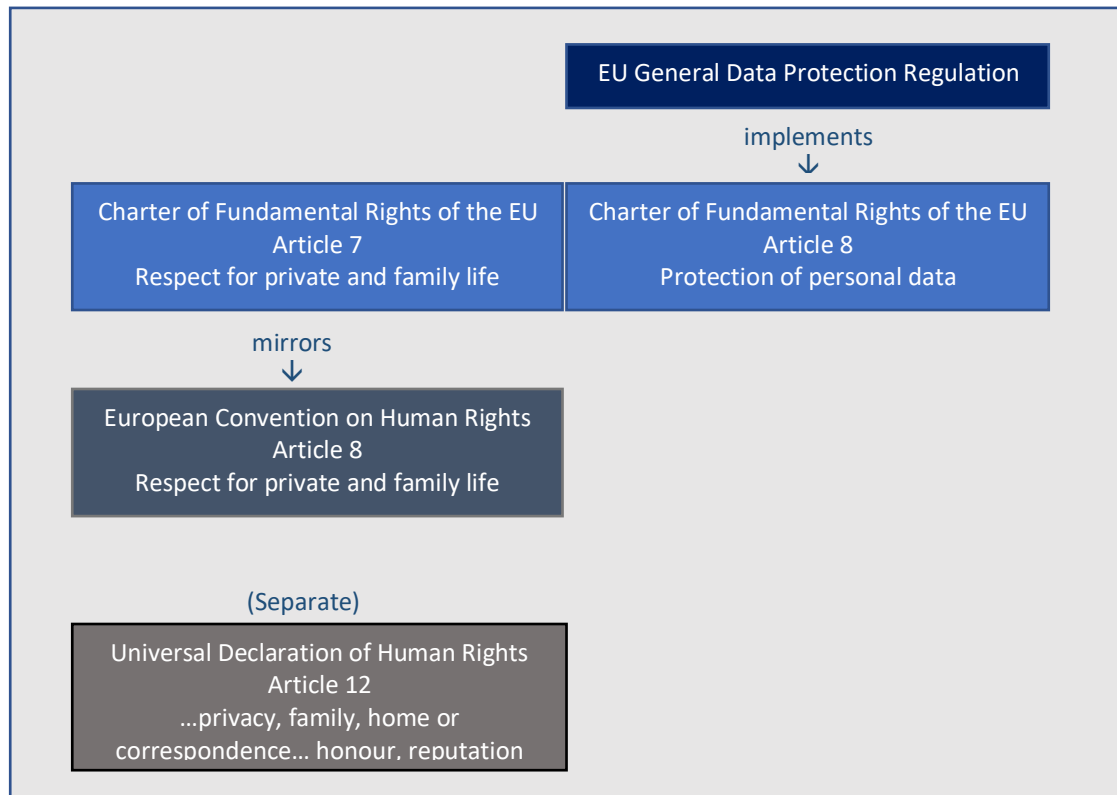


Figure 3: EU and international privacy and data protection rights

### 3.2 Aspects of privacy

In cyber security, privacy may be viewed as a security issue, concerning mostly the confidentiality of personal data, but it may be used as likely to mean the self-determination of one’s private boundaries, the control over one’s personal data, the ethical and well-governed use of personal data or legislative compliance.

Daniel Solove (2006), a prominent privacy researcher, has produced a list of privacy aspects stemming from the US privacy tradition called Solove’s taxonomy. An analysis by Oetzel and Spiekermann (2014) of Solove’s taxonomy against data protection legislation (the EU Data Protection Directive and the 2012 proposal for the EU GDPR) found that if data protection regulation was strictly followed, all of the Solove’s listed privacy aspects would be covered. The additional aspects which Solove’s taxonomy did not cover but the regulation did, were that people should be

informed of how their data is used and may request its portability (Spiekermann-Hoff & Oetzel, 2014). This significant overlap leads to the argument that one does not necessarily need to choose between privacy and data protection, and to the realisation that the GDPR highly likely covers privacy from all angles. Interestingly, following their analysis, Oetzel and Spiekermann decided to use the term privacy rather than data protection. This admittedly mirrors the European courts' view that data protection may be a subset of privacy, as discussed earlier.

One aspect that Oetzel and Spiekermann's analysis overlooks is the question of ethics. The GDPR has an ethical base; it refers to the protection of fundamental rights and freedoms overall, fairness towards data subjects and how the processing of personal data should serve mankind (Regulation (EU) 2016/679). Therefore, for data processing to be compliant in the wider sense, it should also be ethical. The question of ethics is a highly topical one as seen in chapter Introduction and in Gartner's technological trend analyses. In Autumn 2019 The Financial Times set a new agenda calling for a capitalism reset: companies to have a purpose beyond creating wealth for shareholders, consider the "perils of big tech" and investing ethically (The Financial Times, 2019). EU expert group published guidelines for the ethical use of AI (High-Level Expert Group on Artificial Intelligence, 2019). The European Data Protection Supervisor's (EDPS) digital ethics work currently focuses on the increasingly complex, large scale and interconnected ways people's data is used and how it presents a threat to data protection and privacy, and consequently to people's dignity and autonomy and the democratic society. Organisations should aim beyond mere legal compliance and consider the ethics of personal data processing (Buttarelli, n.d.). In the US, NIST privacy framework 1.0 recognises that privacy and compliance risks should be distinguished, and that a fully compliant system may still cause problems to individuals, calling for ethical decision making (The National Institute of Standards and Technology, 2020).

Westin's privacy definition includes the person's right to draw their private boundaries, termed 'informational self-determination'. However, in digital ecosystems, it is the systems' designers and owners who make these choices. Data protection legislation regulates how companies use peoples' data, and includes only slight informational self-determination rights to people, such as giving consent and

right to know how their data is used. New technological initiatives are trying to combat the issues arising from large enterprises holding power over peoples' data, such as the Finnish-born MyData initiative, which has the purpose to "empower individuals by improving their right to self-determination regarding their personal data" (MyData, n.d.). Another similar project in progress is SOLID, led by Tim Berners-Lee, where users are "personally and directly able to manage who and what can see your data and when, at global scale" (Ottenheimer, 2020).

To summarise the discussion in this chapter, the various aspects that privacy can cover include legal compliance, ethical processing of personal data, informational self-determination, the right to be let alone and the implementation of a human right. Out of these, compliance and privacy are two distinct strands of the matter.

## **4 Privacy threat modelling**

### **4.1 Descriptions of selected methods**

This chapter describes and analyses six privacy threat modelling and related methods, such as the data protection impact assessment (DPIA), for how they see privacy, what kind of privacy threats they are designed to uncover, what kind of techniques they use, and what limitations they have. Each method is described in more detail under the following subchapters and an analysis is provided at the end. A summary table is found in Appendix 2.

#### **4.1.1 PRIAM**

De and Le Métayer's PRIAM method was published in 2016. It addresses the privacy impact assessment (PIA) requirement contained in the GDPR, aiming to be embedded within a PIA to fill the gap for a technical risk assessment. PRIAM acknowledges the difference between security and privacy assessments, stating that the latter is more complex and multifaceted, and that the former does not consider privacy harms (to people) within the risk assessment. Anticipating a variety of privacy harms is a clear strength of the PRIAM approach. It acknowledges harms that relate to people, groups of people or the society as a whole, and lists for example

reputation, dignity, acceptance in society and “any fundamental right” as aspects that may be harmed. Victims of the harm are categorised. PRIAM recognises various risk sources, including the system interface, gaps in compliance and misactors, which include the organisation itself since the way the organisation handles people’s data may harm people. PRIAM is sensitive to terminology and has insightfully chosen terms that do not link too strongly to security assessment methods, to underline the significant differences between security and privacy approaches. To begin the assessment, the target is analysed: the system, stakeholders, data, risk sources, privacy weaknesses, feared events and harms. Each of these is described with relevant privacy attributes, such as ‘sensitivity’ for ‘data’. The components are labelled in detail and re-constructed into a diagram representing the system from a privacy viewpoint. The relationships and connections between the parts and how privacy harm may arise from those are added. This linkage differentiates PRIAM from the other analysed methodologies. PRIAM represents the results as harm trees which link the privacy weaknesses and risk sources to the feared events and, finally, to the identified harms. PRIAM includes a disclaimer that the accuracy of the assessment depends on the accuracy and detail of the labelling and mapping of the system. (De & Le Métayer, 2016)

#### 4.1.2 Design science approach

Spiekermann-Hoff and Oetzel’s research paper on the Design science approach to PIA was published in 2014 and it describes a systematic way for conducting PIAs. In the paper, PIA is defined as a risk assessment methodology for making an IT system privacy friendly and compliant with data protection legislation. The vagueness of privacy terminology is acknowledged and addressed by cross-referencing and combining Solove’s taxonomy of privacy threats with the requirements from data protection legislation to create privacy targets. The wider term ‘privacy’ was chosen over data protection, to emphasise that their approach to PIA covered more than just data protection compliance. The assessment begins with documenting the system from four views: the system view, functional view, data view and physical environment view. The paper notes that typical companies do not usually have extensive detailed documentation readily available to support this. Then relevant



privacy targets are set for the system, which largely correspond to legal requirements, such as having data subject rights implemented. Then threats to the targets are identified – threats are primarily legal compliance failures – and finally suitable controls are identified. One weakness of this approach is that writing detailed enough descriptions for the privacy targets as well as identifying satisfactory controls requires extensive analysis and assessment, which probably should have been done when the system was made GDPR compliant. Another weakness is that no method is included for identifying threats that are not directly related to legal compliance, apart from asking stakeholders or trying to anticipate stakeholders' views. Both options appeared challenging. Fully understanding data subjects' point of view and evaluating the privacy harm required significant effort from the stakeholders. According to the paper, practitioners with information security background seem to prefer clearly defined targets, but this also made the assessment look too straightforward to them, perhaps leading to a too simple assessment. As for the rating of threats, a qualitative approach felt a better fit to privacy threats than assigning likelihood and probability as numbers. The authors conclude that their approach was proven to work in the discovery of privacy issues. (Spiekermann-Hoff & Oetzel, 2014)

#### 4.1.3 DPIA, UK Information Commissioner's Office

DPIA is an impact assessment and risk management framework and as such its completion is dependent on having knowledge of relevant threats. The official EU level DPIA guidance states that DPIA methodology can be freely chosen as long as the mandatory elements are included. It is mandatory to assess whether the personal data processing is necessary and proportional compared to what it is trying to achieve, and also to assess the impact to the rights and freedoms of individuals. If high risks can be foreseen, a DPIA is mandatory. Certain high-risk indicators are already listed in the GDPR, and they include the use of new innovative technologies; large scale processing; systematic and extensive evaluation of peoples' personal aspects based on automated processing, including profiling; systematic monitoring of a publicly accessible area on a large scale; use of sensitive information; vulnerable

data subjects; matching or combining datasets; and situations where data subjects are prevented from using their rights. (Article 29 Working Party, 2017, p. 8, 17 & 22)

The United Kingdom Information Commissioner's Office (ICO) DPIA template approaches threat elicitation through probing questions. Many of the questions are data oriented, such as "What is the source of the data?" and "How long will you keep it?". The questions approach the target widely and include many angles which can help the assessor to think of threats. Creating a data flow diagram to help is suggested. The template includes people-oriented questions, for example regarding people's relationship with the organisation, their expectations and how much control they have in the situation. The necessity and proportionality section questions personal data use purposes: does the intended purpose get fulfilled by what the system actually does and whether there is another way of achieving the purpose. So-called function creep, where the system's functionalities and data use purposes gradually widen via e.g. software version updates, is mentioned as a threat. These purpose-related questions indicate that exploring the organisation's intentions is relevant since there may be hidden discrepancies between what is thought or planned to happen and what is actually happening. A section for seeking people's views on the system is also included on the template. The question set is simple, yet it guides the assessor to consider the target widely and deeply. The responses for each section are to be written in text boxes. For a larger system, the amount of data is likely to get too large to handle within the template's text boxes. The last pages of the template include a table for writing down the identified threats. No method for threat identification is given, so the assumption is that a skilled assessor will be able to extract threats from the answers to the various questions. The likelihood and severity of the impact on individuals is recorded. Assessors are invited to record compliance and corporate risks as well, not only risks to people. This highlights that compliance risks are seen to belong to a separate category from risks to people. Two more tables are provided; one for recording actions and one for risk approval and tracking. (Information Commissioner's Office, 2018)

#### 4.1.4 Elevation of privacy

Elevation of privacy cards by F-Secure extend Microsoft's "Elevation of privilege" security threat modelling card deck by introducing privacy compliance related threats that have been observed in real life. The deck is aimed at software developers. It comes with a notion that privacy cannot exist without security and a disclaimer that not all GDPR threats are covered. To carry out modelling, a data flow diagram is constructed, and the cards are used as prompts to identify relevant threats. Users are asked to consider both privacy and data protection. The cards contain GDPR compliance related prompts such as the security of personal data, contractual arrangements and non-EU data transfers, individuals' data rights, data retention, legal bases for data processing, and transparency. There are a few targeted prompts concerning the purposes of personal data use, such as personal data use for machine learning, testing or advertising, and prompts that question whether personal data is needed for a certain purpose and whether the personal data (even) has a purpose. Using the cards requires some background knowledge of privacy and data protection, and it takes a certain skill to take an idea presented on a card and to apply it to the target context. The cards do not cover harm to individuals nor risk assessment. (F-Secure, 2018)

#### 4.1.5 LINDDUN

LINDDUN privacy threat modelling method was created in 2010 by KU Leuven research groups DistriNet and COSIC in Belgium (DistriNet Research Group, n.d.). The method is available online and subject to continuous development. LINDDUN is described as 'knowledge-based', with threat knowledge contained in threat trees and 'model-based' as it utilises data flow maps to systemically examine the entire system. LINDDUN is aimed at software systems and is designed to not require any domain-specific knowledge. The LINDDUN mnemonic lists the aspects through which threats may arise: linkability, identifiability, non-repudiation, detectability, disclosure of information, unawareness and non-compliance. The first three (LIND) are largely based on Pfitzmann and Hansen's work on the confidentiality of identity, and the fourth (D) on Microsoft's STRIDE (Wuyts, 2015). Privacy is treated mainly as a security aspect, preventing personal information from being revealed to

unauthorised subjects, and data minimisation is recognised as a major mitigation strategy. LINDDUN takes a technical rather than legal perspective and so data protection threats are not fully covered. The non-compliance aspect only exists to make analysts aware of the abstract threat at a high level. Separate legal expert involvement is advised to achieve compliance. Threat modelling with LINDDUN starts with the creation of a data flow diagram at a desired level of detail (high or low). Then the four types of elements found in the data flow diagram, data stores, data flows, processes and entities, are mapped against LINDDUN threat categories. After that, threat trees provided on the LINDDUN website are used to identify threats. The trees contain breakdowns of how each of the LINDDUN threats may materialise. Identified threats are documented on a template and if certain trees or parts of them are left out, that decision is formally recorded. Identified threats are risk assessed to prioritise them and then corresponding mitigation strategies from LINDDUN mitigation taxonomy are selected. The taxonomy is available on LINDDUN website, along with a table offering concrete privacy enhancing techniques to match them, which is the final step of the LINDDUN method. Alternatively, the mitigation strategies can be used to define privacy requirements for further development cycles. (Wuyts & Joosen, 2015)

Many of today's privacy issues are not covered by LINDDUN, such as organisations using personal data unlawfully for unfair purposes. Furthermore, LINDDUN does not cover harm caused to individuals but recognises that privacy-specific risk assessment techniques are lacking (Wuyts, 2015, p. 61). The researchers working on LINDDUN have since published further papers that address its limitations and relationship with the GDPR, but this analysis focused on the published version on the LINDDUN website, which is the 2015 version.

#### 4.1.6 Seattle residents' privacy threat model

The Seattle residents' privacy threat model was a project conceived by Adam Shostack in 2017 in collaboration with Settle Privacy Coalition, and it attempted to build a model of threats that Seattle residents face during their usual commute. Shostack is best known for his 2014 book "Threat modeling, designing for security" that bases threat modelling around four questions: what are you doing, what can go

wrong, what are we going to do about it and did we do a good enough job. The Seattle project approached privacy as a fundamental right and focused on the data subjects' view. The target system comprised of the city; namely any data collection that the residents were subjected to during their daily commute. The method was created as the modelling proceeded. The model was built in brainstorming workshops with a variety of stakeholders, including Seattle residents. Using a whiteboard, the various ways their privacy could be breached were listed together with mitigations that the people could apply themselves, with the help of the four questions above (the last two modified as: what are your possible defences, and what are the costs of your alternatives). This generated a lot of unordered data. To analyse it further, the commuting methods were identified and then relevant data gathering technologies attached to them were identified, along with defences against the data gathering and the costs of the defences (privacy trade-offs), such as privacy loss, social stigma, financial or time loss. The exercise produced new surprising information about privacy threats. (Bultmann, 2017)

Shostack's draft white paper consolidates the exercise and describes the resulting method, titled "Black Hole Sun (Alpha release)". The method has three stages, again built around the core questions (what are we working on, what can go wrong, what can be done). "What are we working on" involves brainstorming to create an activity list, which is then used to create a model, i.e. an activity category list. The next stage, "what can go wrong" involves the analysis of each activity category for data gathering and listing who gathers what data and how. The final stage looks at "what can be done" through a trade-off analysis and outputs a list of trade-offs. The outcome of the exercise is a kind of a privacy self-defence guide for the data subject. The paper notes a few differences to traditional threat modelling: usually threat modelling targets a computer system, but in this case the focus was data subjects, and threats are usually modelled by software engineers to produce a list of bugs that they could fix, but the 'bugs' resulting from the Seattle model contained many issues out of the modellers' control. The paper also suggests policymakers and technologists to learn from it to make improvements to privacy. The paper ends with a list of possible next steps for improving the method. Focus on vulnerable data subject groups and further data gathering and piloting is suggested. (Shostack, 2017)

## 4.2 Analysis and discussion of the methods

Privacy threat modelling has its roots in security threat modelling and privacy engineering, and in the idea that software must preserve confidentiality of private information (Sion et al., 2019). In the last few years, data protection legislation has brought in new viewpoints, including legal compliance, harm to data subjects' rights and freedoms, and the purposes which personal data is used for. In addition, interest in ethical issues and informational self-determination has risen recently. Although privacy threat modelling descends from security threat modelling, PRIAM authors De and Le Métayer (2016, p. 4) note that security threat modelling methodologies cannot be simply copied into the privacy domain since privacy is a much more complex concept, involving the human element, social norms etc. In privacy, the asset to be protected does not belong to the company; the 'assets' are autonomous human beings, and they may be harmed in various ways. The PRIAM paper acknowledges that it is a challenge to consider all of the factors and factor combinations that can have privacy impact (De & Le Métayer, 2016). The research group behind LINDDUN have also developed new versions of their method to incorporate legal compliance viewpoints. On their data subject-aware threat modelling paper Sion et al. (2019) discuss how the currently available LINDDUN method does not account for data subjects, even though they are central to the GDPR. The authors also acknowledge that methods that inspect every element in a system, such as LINDDUN, can generate an unmanageable number of threats.

One issue with GDPR compliance focussed modelling is that the potential threats are known already – they are GDPR requirements not implemented or GDPR requirements poorly implemented. This effectively makes the threat modelling exercise a GDPR compliance check. However, setting GDPR requirements for a system and checking a system's compliance should be done with a method designed for that purpose, instead of threat modelling which has not been invented to address that kind of a need. Furthermore, investing effort in implementing GDPR requirements pays off by raising awareness of compliance issues and can lead to threat discovery.

Other than a compliance check, privacy threat modelling may work as a quick tool to pinpoint issues early in the system development. LINDDUN and Elevation of privacy present a techie-friendly way to get privacy included in system development and educate technically minded people about privacy issues. Both are inspired by Microsoft's STRIDE (F-Secure, 2018; Wuyts, 2015, p. 101). Both acknowledge that their approaches do not fully cover the GDPR requirements and suggest a separate exercise for that, with a legal compliance specialist.

The third type of privacy threat modelling method focuses on the data subject viewpoint and is open to threats arising from the context. PRIAM is a privacy impact assessment (PIA) method that aims to unearth privacy harms that affect people and does it by mapping everything in the target system in detail. The Design science approach also provides a PIA method, but approaches it like a compliance check, limiting the kind of threats it can cover to compliance threats. The Seattle model aims to unearth privacy harms to people but unlike PRIAM, it does not rely on extensive mapping and does not cover compliance matters. It lines up with Westin's definition of self-determined privacy and sees data gathering as a threat in general.

Many of these methods attempt to map every aspect of the system and rely on the accuracy and detail of this for the validity of the assessment, such as PRIAM and the Design science approach. This is also a weakness since detailed mapping takes time and resources, and a typical company will not have extensive detailed documentation readily available as noted by Spiekermann-Hoff and Oetzel (2014). Constructing data flow diagrams is a common alternative. These are promoted in the Design science approach, Elevation of Privacy and the ICO DPIA model. In the Seattle case, no depiction of the system was attempted since the target was an activity rather than a computer system – a Seattle resident's journey to work. In DPIA the target may also be an activity, a personal data processing activity, which may span across physical and digital boundaries, and personal data lifecycle viewpoint may also be used. PRIAM uses the data lifecycle as the boundary, but states that it only contains hardware and software components (De & Le Métayer, 2016). Methods which rely on the accurate mapping of the target may not be suitable for more complex systems since the representations would become too vast and complex to handle. For those kind of cases methods which use structured questioning and

brainstorming may be better suited because they offer flexibility and may be quicker to pinpoint problem areas for deeper focus. They are also more likely to include probing 'who' and 'why' questions in addition to the plain 'what, where and how'. The modelling purpose can also drive the choice. Security, confidentiality and compliance violations may be extracted from the detailed mapping of the system, but harms to people, ethical issues and fundamental rights violations require a more holistic, human-centric and context aware approach.

The methods utilise various assistive techniques for threat elicitation, such as brainstorming; stakeholder involvement; use of checklists, prompt cards or mnemonics; and comparison against GDPR or other requirements. Expertise required varies from none or very little (as in the Seattle project) to clear understanding of the concepts being required (as in the ICO DPIA or Elevation of Privacy), all the way to the requirement for a deep understanding of the method (as in LINDDUN, PRIAM and the Design science approach). At the end, all the methods return a list of privacy issues, usually prioritised. The results are presented either as a written description, a risk table with ratings, harm trees with risk ratings, or in a freer form such as threat lists. The Design science approach and LINDDUN incorporate controls as well. In the other methods control selection is done more informally.

Out of the analysed methods, PRIAM appears to best answer today's privacy threat modelling needs, but its detailed mapping requirement is resource intensive and impractical for more complex systems. It seems that highly complex targets may be threat modelled satisfactorily with a participatory action research style approach as seen in the Seattle threat model, which produced interesting and relevant threats and was fast to pinpoint problem areas for deeper exploration.

## **5 Systems thinking, complexity and Soft Systems**

### **Methodology**

#### **5.1 The rise of systems approaches**

This research project was inspired by Peter Checkland's Soft Systems Methodology (SSM), which he worked on from the 1970s until his parting address in 2018 (The OR



Society, 2018). SSM belongs to the tradition of systems approaches and it is one of the best-known methodologies based on cybernetics (White, 2015). Systems approaches can be traced back to the Second World War and operational research in the army. Following the war, these ideas were further developed to be used in the business and governmental contexts. (Checkland, 2000)

General systems theory was formulated with the aim of researchers of different disciplines bringing together a holistic view of the interrelated issues from their fields, but instead, against the intentions, general systems theory slowly took foothold within separate single fields such as biology, education and engineering. (Warren, Sauser & Nowicki, 2019)

Hard systems approach emerged to deal with systems that exist in the real world, meaning systems that could be engineered, and systems approach in the business context evolved into the field of cybernetics. Literature of the 1960s approached management challenges from the point of view that the goal is already known but the means to get there need to be discovered. In 1970s and 1980s an understanding started to develop that perhaps the goals cannot be taken as granted, and that the problem expands when humans are part of the picture, and so richer viewpoint is needed. This is the stage where the soft systems approach begun to develop. (Checkland, 2000, S46-S50)

Checkland's work into Soft Systems Methodology established the divide between hard and soft systems thinking. Checkland articulates the difference between these as follows: the hard systems approach assumes that the world contains systems that may be engineered, whereas the soft systems approach appreciates that the world is multi-faceted and problematic and so an inquiry into should arranged as a system, a learning system. (Reynolds & Holwell, 2010)

## 5.2 Complexity science

Systems approaches in general were designed to target complex systems. The intended target of soft systems approach may best be described as a complex problem situation needing human intervention. Complexity can refer to very big issues, such as global political or ecological crises but it can also refer to local politics,

family or organisational issues, or the kind of a topic that this thesis looks at, the increasing complexity that technological advancement brings. None of these have clear answers and importantly, no clear questions either. Due to the complexity, interventions may have unintended consequences, positive but also negative. (Reynolds & Holwell, 2010, p3; White, 2015)

Different branches of complexity science attempt to make sense, intervene in or predict the behaviour of complex systems. One characteristic of systems approaches is the vocabulary around complexity. Various authors have their own takes on it, but they all portray a situation that cannot be tackled by traditional approaches, such as the reductionist approach that breaks the target to its constituent parts and examines those, or having enough resources, such as computing power. Another common attribute of a complex system is the human aspect, the inclusion of which appears to elevate a system to a level of high complexity. (Reynolds & Holwell, 2010)

Kurtz and Snowden (2003) warn that not everything should be classed 'complex'. They worked on the Cynefin framework, a device for sense-making developed in association with IBM for use in action research, which establishes the complexity levels of known, knowable, complex and chaos. In the Cynefin model, these lie in the domains of order and un-order, between which is crack where disorder is found. Kurtz and Snowden suggest that the concepts of systems thinking and learning organisation are located in the 'knowable' rather than the 'complex' domain, but their definition of systems thinking may differ of that of Checkland. In the 'complex' domain Kurtz and Snowden have placed the concepts of multiple perspectives and narrative techniques. Checkland's systems thinking relies on multiple perspectives which places it in the complex domain.

An influential systems thinker, Russell Ackoff (1997, p.427) uses the word 'mess' to describe complex problem situations and to differentiate them from simple problems or mere difficulties: messes are characterised by the presence uncertainty, lack of boundaries, likely involvement of many people, interlocking issues and serious implications. Ackoff (1999, p.22) describes complex system characteristics as: its parts affect the whole set's behaviour; the parts' behaviour is interdependent; and if the parts are formed into subgroups, subgroups behave this way too.

Other examples of characteristics for complex systems are: surprising emergent behaviours; multiple viewpoints and decentralised decisionmaking can be identified; its parts may not be removed or changed without affecting the whole; it may self-organise; and it has feedback loops and interaction between its large number of parts (Armson & Ison, 2004).

There are differing views as to whether systems exist in the 'real' world or whether they are mental constructs of the observer (Checkland, 2000). For this thesis, the view is taken that systems are epistemological devices, the practitioner's constructs for knowing about the problem situation. Key features of systems thinking approach are appreciation of complexity, looking at the connections in situations and the interaction of the connected parts as well as choosing to 'see the wood from the trees', which means looking at the whole in order to see its parts in context (Armson & Ison, 2004). According to Ackoff (awal street journal, 2015, at 1:05), complex situations need to be approached with holism: if a problem is taken apart and reduced to the parts that it is composed of, the essential parts of reality and the essential properties of the parts are both lost.

### 5.3 Soft systems methodology

The aim of SSM is to understand and to instigate change in complex problematic situations. The SSM approach stems from action research: people trying take purposeful action on real situations by taking part in them. The learning cycle can be observed within the SSM, as shown in the simplified illustration of the SSM in Figure 4. First the problem situation is explored to find out about it. Then epistemological devices, conceptual models each representing a purposeful activity from a selected viewpoint, are built. In the next stage, they are used for a debate and gaining insights into the real-world perceived problem situation. Social and political dimensions are taken into account when debating the feasibility and desirability of improving actions. Finally, the planned action is taken in the real world in order to improve the situation. The cycle may then be repeated. In SSM, problems are not known but instead situations are known to be somehow problematic, and the exploration of the problem situation is organised as a learning system. Open democratic dialogue and

participation are used to identify positive improvement actions that are meaningful to people in the situation. (Checkland, 2000)



Figure 4: SSM action learning cycle

Over the years, SSM crystallised as a powerful learning system (Checkland, 2000; Watson, 2012). An aware systems practitioner using it anticipates learning about not only the target of the research but also about their method and approach. The given methodology is developed to a situation-sensitive method in the hands of the aware skilled practitioner during the iterative inquiry. Figure 4 shows Mode 1 application of SSM, where SSM is applied as prescribed and the methodology is in focus. Mode 1 serves best as a way of getting acquainted with the approach. In Mode 2 the practitioner has internalised the approach and may skilfully adjust it to fit the situation and more fluidly move between the stages. Mode 2 is the one to strive for. (Checkland, 2000)

Mode 1 SSM includes detailed steps and assistive techniques for carrying out the stages. Finding out about the situation may be aided with building a *rich picture*, drawing out the situation to gain a holistic view. The information gained is suggested to be analysed for three aspects: who the problem owners might be, what are the social aspects such as roles, norms and values, and where power is located in the situation. The activity model building stage starts with building the root definition for the model. The viewpoints for the models are chosen by the modeller, and they should be chosen in terms of learning value. Rigour is added to the models by

defining their CATWOE and PQR. CATWOE stands for the customers, actors, transformation, worldview, owners and environment for the purposeful activity that the model represents. PQR can be laid out as “do P by Q in order to help achieve R”, where P is what the activity does, Q how it does it and R why it does it. It can be used to check the level of the viewpoint for the model: P can be seen as the system, Q as the sub-system and R as the super-system. Since the model should be a logical system that could in theory work, measures of performance are also defined for it, to capability to adapt and again, rigour. These are defined as Es: efficacy, efficiency and effectiveness, and perhaps also ethics or other measures, should the model need them. Once the activity is defined this way, activities essential to it are listed and arranged in order, and then drawn into a visual model, with the activities placed in blobs and arrows drawn between them indicating the order in which they happen. The system boundary is drawn around the blobs. Monitoring and control measures are added in the picture, again using blobs and arrows. Hand-drawn informal representation is recommended, to underline the throw-away nature of the models: they are only devices through which the situation is explored, not end-results of any kind. The models are then used for structuring debates with the stakeholders. One way of doing this is going through the models step by step and asking does the activity appear in the real-world situation, how, and what is there to learn through this. The social and political analyses from the earlier stage are utilised to inform the feasibility and desirability of the suggestions for improving actions that come up in the debate. Finally, those actions are implemented in the real-world situation. (Checkland, 2000)

#### 5.4 Applications of SSM

Watson (2012) provides an analysis of the SSM's applications, noting that it has commonly been applied to information systems, which interesting for such an old methodology, now nearly 50 years old. In the UK, for example, it has been used in army and national health service information systems planning. Now information systems impact every moment of human life. Watson states that new applications are constantly found and believes the SSM was ahead of its time. As an example of potential application, Watson suggests using SSM for research into privacy

compromises arising from ubiquitous computing. However, a more recent analysis by Warren et al. (2019) shows that the use of SSM had its high time between 1990-2010 with decline in the last three years which the analysis covered (2015-2018). The authors contemplate that perhaps today's researchers no longer find value in SSM, but nevertheless conclude that SSM had a significant impact in academic thinking in USA and Europe between 1980-2018. Their analysis revealed 286 relevant publications of research in which SSM had been applied in engineering, business or other social sciences context between 1980-2018, with the highest impact on business (33%) and engineering (27%) fields. The paper notes that many uses of SSM do not end in publication since the method is used in organisations for practical rather than research purposes. Watson's analysis refers to this issue as well (Watson, 2012, p. 454).

To review the application of SSM in the technology context within the last few years, a publication search for "soft systems" in all metadata covering the years 2015-2020 was conducted on the IEEE Xplore database. 24 publications concerning the application of the SSM were found, and of those eight could be considered relevant to this project since they related to the modelling of issues in computer or sociotechnical systems. One publication was a high-level overview of systems approaches and one applied SSM to a hard context with no human element. Three were poor quality and another three concerned the use of Systemigrams, a technique for visualising complex targets developed from the idea of rich pictures. This search result could indicate that skills and understanding of how to apply SSM are lacking and that simpler looking modelling techniques, such as Systemigrams, are favoured in the technology context. Warren et al. (2019) list the lack of training in SSM both at universities and also in public media as a hindrance for its take-up.

A wider search concentrating on threat modelling type applications of SSM identified projects where SSM had been utilised skilfully and topically. A case study by Niu, Lopez and Cheng (2011) applied SSM to software system expectations and requirements practices, and concluded that with the aid of SSM, a relatively complete set of flaws could be uncovered. The overall aim was to address software project failure and SSM was used to identify and communicate the purpose for which the system was used. SSM was selected as it is designed to address situations with

multiple stakeholders with diverse objectives. The study showed that SSM is easy to understand by different stakeholders and it can be applied at low cost and by non-experts. The overall conclusion was that SSM has a rich value in improving human centred requirements engineering activities, and that it achieved this by holistic thinking. It should not however replace 'hard' methodologies but complement them.

Similarly, in another study, SSM was used as part of a multimethodology approach in Mode 2 to help to define role based access requirements for a sociotechnical system. The authors stress that no matter how useful a certain method is thought to be in theory, its usefulness in reality depends on how it is applied in a specific situation. The target of the study was subject to legal requirements, but the developed methodology did not specifically incorporate this dimension. The models were well received by the participants. The SSM was tailored by exposing it in the more easily communicable Mode 1 to the participants, while the researchers were working in Mode 2. Again, it was noted that the developed methodology would work well as a complementary one to a hard (project management) methodology. (Small & Wainwright, 2018)

Organ and Stapleton (2016) used SSM in a study that explored the meaning of risk and risk management approaches and attitudes in sociotechnical systems development. Risk is recognised to affect humans and society, not only finances. Failure to recognise the dynamic relationship between people and technology is seen to lead to poor coverage of socially derived risks, such as privacy risks. Organ and Stapleton point out the weaknesses of reductionist approach that breaks systems into parts and examines them in isolation: losing sight of the whole and missing risks arising from the interconnections, both technical and social. The authors also note the potential for risk emergence, emergence being a property of complexity. In the study a SSM based risk management approach for sociotechnical systems was devised. Modified version of CATWOE, BATWOVE by Midgeley and Reynolds (2001), was used. This replaces customers (C) with beneficiaries (B), but more importantly, and adds victims of risk as the V. As a conclusion, the authors present that risk management has compartmentalised and ask for risks management to move from the current positivist and reductionist base towards a holistic and systemic approach.

SSM has been criticised for its inward-looking development that conflicts with its action learning foundations and this is evident through the lack of references in Checkland's work to other systems related research (Mingers, 2000). This is also at odds with the finding that SSM is often combined with other methods in multimethodology research. Various analyses have found that SSM is frequently used in multimethodology applications (Watson, 2012; Mingers, 2000). This was seen in the studies featured above. SSM is also criticised for not offering detailed solutions or implementing the concrete changes following the finding out stage (Mingers, 2000). White's (2015) appraisal of SSM found it particularly useful in a setting where a group of people work well together. The success of SSM is founded on the debate, but in hierarchical organisations with only management around the debating table, there is a danger that an effective participatory debate cannot take place (Jackson, 2000). Despite the criticisms, SSM is widely recognised as a powerful learning tool which can, through its eye-opening nature, bring wider positive changes and new ways of seeing things for its users and organisations (Mingers, 2000; Watson 2012). As a methodology, its flexibility and built-in continual self-improvement are also recognised (Jackson, 2000). It has frequently been described as revolutionary and having significant contribution to various fields (Jackson, 2000; Warren et al., 2019).

## **6 Innovation and testing of the method**

### **6.1 Setting up**

The previous chapters described the steps of the constructive method that concern finding a relevant real-world problem to solve, making an agreement for the research project and gaining an extensive theory and practical knowledge base. This section describes the innovation phase (step four) and the implementing and testing phase (step five). These phases were expected to take place in an SSM-guided learning cycle, as described in the Research Methodology chapter. The development and testing of the PTM method were to be carried out through piloting the method with the various organisations which were part of the Mad@Work research programme. Each of the organisations was developing their own technological and/or organisational solutions that would contribute to the programme. These solutions



were envisaged to be the targets of the PTM. ‘Selling’ the construction to the organisations to recruit them for the pilots corresponded to the market testing phase of the constructive method. The marketing material is found in Appendix 3. Recruitment was ongoing throughout the project and the number of available pilots was not known in advance. At the end, two pilots were obtained and a review with privacy specialists was carried out. Learning from these is described in the coming chapters. During the learning cycles data was collected to contribute to the answering of the research questions as shown in Table 2.

Table 2: Approach and data to be collected

<b>Research question</b>	<b>Approach and data to be collected</b>
<b>1. How can privacy threat modelling of complex systems be improved with the soft systems approach?</b>	A modelling method based on SSM is developed and tested to observe its effects. The answer to the main research question is formed through the sub-questions, where question a. concentrates on the method qualities, b. on the method in action and the quality of the research and development process, and question c. on the method’s observed effects and output.
<b>a. What kind of a PTM method achieves this?</b>	Knowledge of current methods and current threat modelling needs was used as the theory base. Initial requirements for the method were drawn up and the first draft of the method was produced. Data was collected from the observations and insights from the method development and testing process, incl. the author’s learning journal notes and meeting notes. The assumptions and results were compared to see if the method was working as intended and changes were made accordingly.
<b>b. How well was the PTM method implemented?</b>	Data was collected on the author's experience using the method as well as observations and comments from the pilot participants. The method’s output (threats) was analysed. The method’s effectiveness, efficacy and efficiency were analysed.
<b>c. What were the effects of using soft systems approach in PTM?</b>	The method output (threats) and the way they were identified were analysed. Observations and comments were sought from the pilot participants. The author’s own experience was also noted. These were related to the theory base and the project stakeholders’ needs.

## 6.2 Drafting the method

To make it easier to refer to the method under development, the working name 'Taiga' was set. Taiga is a term for a boreal forest and the SSM-based PTM method aims to help its user to "see the wood for the trees", i.e. to take a holistic view.

During the first learning cycle the initial design of Taiga method was drawn up and the research project structure and aims were clarified. The questions which dominated the cycle were what is privacy, what is threat modelling, what should this PTM method try to uncover and how does it relate to GDPR compliance assessments. Current privacy threat modelling methods were explored to understand the field and where there might be gaps. The project aims felt very unclear at this point and effort was made to gain clarity and direction. The starting point was that SSM was going to be utilised. SSM was designed for producing action to improve the problem situation and/or finding out about the problem situation (Checkland, 2000). SSM's capabilities for finding out about the situation should be harnessed to answer the first question in threat modelling ("What could go wrong?"). The second question in threat modelling ("What can we do about it?") refers to the possible mitigations to address the identified threats, which in effect are actions to improve the problem as the SSM puts it. Thus, the SSM should have the capacity not only to aid threat elicitation but also to suggest suitable mitigations. To check the practical potential of the mitigations in the real world situation, the SSM asks for a social and political analysis to be carried out. In human systems social and political aspects are a given and should not be ignored (The Open University, 2004, p. 185).

A list of requirements for Taiga was drawn up. The list was not used as a concrete base for the Taiga method but mostly to gain clarity.

1. The method is clear about its definition of privacy.
2. The method is clear about the types of privacy threats it is designed to cover and what it is not designed to cover.
3. The method can be applied to highly complex systems that involve personal data processing and does this in line with the SSM.
4. The method is scalable. The method should be scalable for depth and detail of the assessment: it should produce meaningful results both in a few hours

and in a few months. This scalability objective should be addressed using the SSM.

5. The method is usable in a professional setting with a customer by a privacy consultant who is familiar with the SSM.
6. The method is effective; many important threats are found, which would not otherwise be found.
7. The method is efficient; many threats are found with little effort.
8. The method actually uncovers the kinds of threats that it is designed to uncover.
9. The method is ethical; no people are harmed in the process.
10. The method produces a list of threats which may be fed into the organisation's risk assessment process.
11. The threats are relevant to the customer; they are of a kind which the customer can act on.
12. The threats are presented in a manner that is comprehensible to the participants, who may be non-experts in privacy or technology.

SSM technique of drawing a rich picture of the problem situation was utilised to understand the whole project better. The picture included researcher and the various aspects that made up the project, such as the sponsor, the thesis and graduation, the pilot organisations, and the author's colleagues. From the picture, different stakeholders were extracted, and their needs (especially evaluation needs) were analysed. The resulting table is included in 10 and evaluation is more deeply discussed under chapter 2.4 Evaluation.

According to the author's previous experience, a learning journal had proven to be a fruitful tool for bringing clarity and insights into projects, and consequently such diary was taken into use. Reviewing the project diary during the learning cycles provided a rich source for reflection and reminded the author of where in learning cycle they currently were. This helped to ensure that the research was moving through a cycle and the project was making progress. A significant insight arising from the diary was seeing *privacy as a conflict*, which goes back to the definition of privacy, discussed in chapter Data protection and privacy. Privacy as one's own

experience means that the boundaries of privacy are expected to differ from a person to another which inevitably creates conflicts between the organisation and the data subjects. The Taiga method should somehow address this conflict. The SSM could be used to uncover those conflicts and to suggest culturally and politically sound actions to ease them. The current methods did not appear to offer a structured way for exploring these aspects.

The second main insight concerned the divide between what is officially stated and what is actually happening. This divide can be likened to Checkland's 1981 version of the SSM with a divide between the real-world situation and the systems thinking world (Checkland, 2000, p. S20). Although Checkland has since erased this artificial divide, it prompted the idea of a *fact-fiction metaphor* that could be used in the PTM. Facts would comprise of all the documentation concerning the PTM target and its technical build. Fiction would comprise of the information gathered through interviews: stakeholders' description of the system and its purposes. Central to this metaphor is questioning what actually is fiction and what is fact in the target system – what if the documentation is fiction while the stakeholders describe the facts? A system built and documented one way may be used in a totally different way. For a system to be privacy safe, the purpose of personal data use needs to be clear since compliance is built on that. Uncovering conflicts between fact and fiction could therefore uncover privacy threats. This idea has been researched under the terms work as done (WAD) and work as imagined (WAI) (Braithwaite et al., 2016). WAI is the official description of the system, how the work is imagined to happen. WAD, also described as kludges, workarounds and shadow systems, are the stakeholders' own purposes for the system, the way the work is actually done. When working with IT systems, people commonly use unofficial workarounds to achieve their own goals (Petrides et al., 2004) and by doing that, potentially create new personal data processing purposes. These new purposes can also be described as *conflicts* (linking back to privacy as a conflict) and are one threat type that Taiga should cover.

This idea also links back to systems sciences through cybernetics and Ashby's Law of Requisite variety which expressed that the controls' variety must match the target's variety (Braithwaite et al., 2016, p. xxi). The WAD world is complex with high variety whereas the WAI world is often simplified or standardised with little variety.

Therefore, conflicts are inevitable. SSM appreciates this complexity and opens a way to see beyond WAI and to explore WAD with the appropriate variety in the approach. Taiga method should anticipate complexity, even if the target is first presented as simple, and respond to complexity with variety in the approach (SSM Mode 2). Taiga should explore both sides, WAD and WAI. Interviewing only stakeholders who are high in the hierarchy – people who own, govern or have designed the systems – would likely result in descriptions leaning towards WAI. Interviewing stakeholders lower in the hierarchy may give WAD descriptions more readily. This presents some challenges as these stakeholders may be out of reach and difficult to engage with, engaging them may be resource intensive, or the management is worried that their responses are not in line with the official descriptions. In the privacy threat modelling context these could be the people who manipulate the data in the system (e.g. office workers) or people whose data is collected (e.g. employees, consumers). On the other hand, it can be that WAD information may not be uncovered through interviews. It may be that stakeholders at any level are not aware of WAD or are not ready to admit that work exists which is not in line with the official description. The current PTM methods did not appear to recognise these hidden sides of systems, although some hidden purposes could be revealed through them.

These issues could somewhat be helped by using ‘personas’, made-up stakeholder profiles, and conducting mock interviews on them. Personas are commonly used in interaction design (Sharp et al., 2007, p. 484) but also threat modelling (Selin, 2019). Security threat modelling methods may use personas to capture attackers as ‘persona non grata’. In privacy threat modelling, the role of attacker is not so central, and there is also the important role of a victim. The use of personas has been criticized in the field of user interaction design. Norman (2005) criticizes user-centred design and advocates activity-centred design, where a deep understanding of the activity is central. Users must not be ignored, but the design should revolve around the activity that the design is for rather than the users, and through supporting the activity, the design then supports its users. This idea resonates well with the SSM since the models are about human-purposeful activities, and not about users. Kurtz and Snowden (2003) also touch on the question of modelling people in the Cynefin framework paper while discussing how complex systems may be simulated. The

authors conclude that successful simulation of human behaviour is desirable but unlikely due to the multiple dynamic and collective identities that people encompass, their free will and mechanisms that affect it (group think, lying, etc.), as well as high capacity for scaled awareness to think from local to global scales. Building detailed user profiles and centring threat discovery around them was left aside and the Taiga method continued to concentrate on the system purposes and activities. Some information gathering about the potential victims of the privacy threats was still thought to be relevant.

At this point the Taiga high-level walk through was produced as shown in Figure 5. Looking at the Process step column, the systemic matters and WAD would be explored through the left-hand thread, starting from interviews, followed by the building of inquiry devices. “Hard” matters, compliance and WAI would be explored through the right-hand thread, starting with document review and an interview. Findings from both threads would be consolidated for the final threat workshop. Comparison and debate of WAD to WAI would take place in the threat workshop. The draft included suggestions for assistive methods to be used as the different steps, shown on the right.

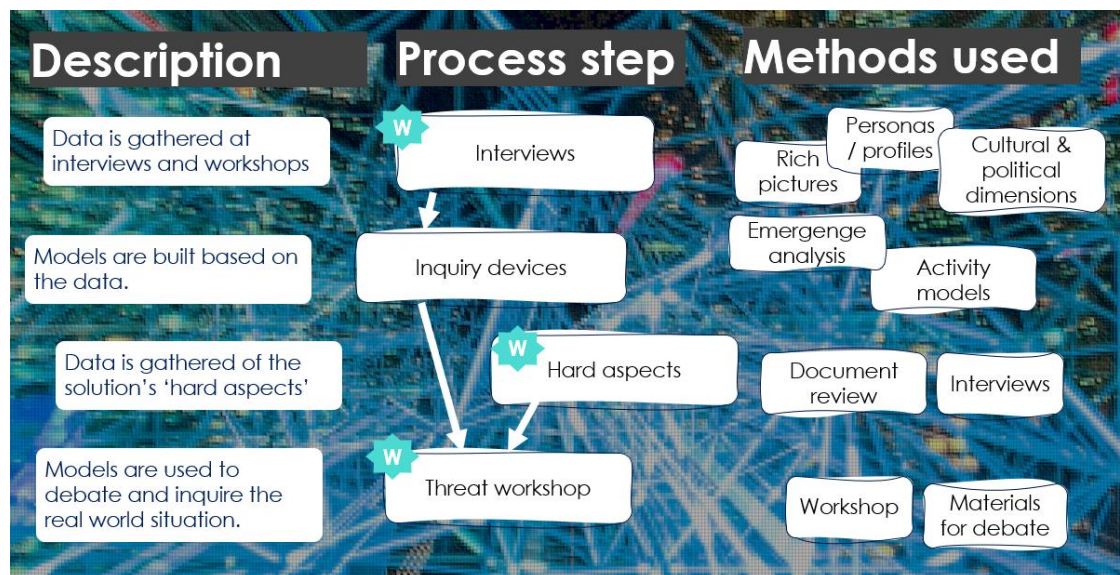


Figure 5: First draft of Taiga method overview

The draft included a question set for interviews, a rough interview plan (who to interview and how to conduct the session), a persona template, templates for SSM

activity model building, and a list of topics and questions for the compliance workshop. The draft is available in full in Appendix 4.

The formula to build the inquiry devices closely followed Checkland's SSM. Although SSM is not meant to be used in prescriptive way, this was the first iteration to gain learning experience and hence it was appropriate (Checkland, 2000, p. S41). The interview questions (Table 3) were designed to gain information for the system definition, shown in Figure 6. They covered the SSM elements of CATWOE (system customers, actors, transformation, worldviews, owner and environmental constraints), political and cultural dimensions, PQR (what the system does, how and why), E4 (efficiency, effectiveness, efficacy and ethicality), and the system's input and output. For each model, a particular viewpoint is chosen, and the system root definition is constructed and recorded under "This is a system to:". The system's CATWOE, PQR and Es and also recorded.

Table 3: First draft, Question set

Question	Feeds to
What is this system for you? (Capture its essence in one sentence)	Root definition
Whether a tech solution existed or not, what is it that you want to do/need to do/achieve?	Root definition
Who does it serve? Who is it for?	CATWOE – C
Who does it? Who are part of the delivery?	CATWOE – A
What does this activity really do? What would you like it to do?	CATWOE – T, P - What
How do you do your activity? What activities make up your activity?	CATWOE – T, Q - How
What is needed for this activity? Materials, data, money etc.	Input
What comes out? What are you trying to make?	P - What, Output
Where in the wider/bigger picture you see this activity?	CATWOE – W, P/C
Are you (company, team, people) a typical one?	CATWOE – W, P/C
Does it matter to you? Care about it? Who does?	P/C
Who or what has power over this?	P/C
In relation to your other activities, where is this?	P/C
Why do you do the activity?	CATWOE – O, Q - Why
What are the expectations placed on you? Who places them?	CATWOE – O
Are you bound by some rules, laws, money, particular technology, or other constraints placed from the outside?	CATWOE – E

System definition – Step 1a			
This is a system to: (input, transformation, output)			
C - Customers			
A - Actors			
T - Transformation			
W - Worldview			
O - Owner			
E - Environmental constraints			
efficiency		What to do (P)	
effectiveness		How to do it (Q)	
efficacy		Why do it (R)	
ethicity			

Figure 6: First draft, System definition - Step 1a

Step 2 consisted of listing the activities that would be needed to be carried out for the system to work. In Step 3 and 4, the activities would be arranged into an activity sequence model. Figure 7 shows the template for the model.

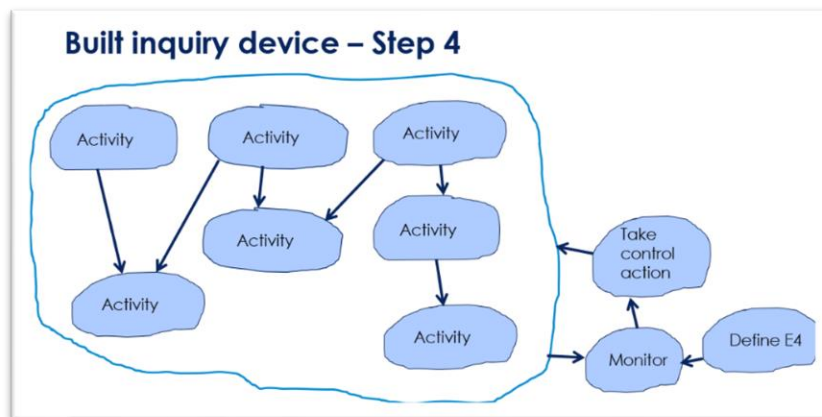


Figure 7: First draft, template for the inquiry device


The profile/persona template (Figure 8) was designed with Norman’s (2005) user-centricity criticisms in mind, by including goals, tasks and motivations for the person. This aspect could be strengthened in further iterations, also by replacing CATWOE with BATWOVE which includes V for victims. The vulnerabilities and environment aspects on the template relate to seeing the persona as a victim. Aspects important to SSM were also included: worldview, political and cultural placement, and role.



## Profile / persona

Question	Fill in
Description	
Goals	
Tasks	
Vulnerabilities	
Likes / dislikes / attitudes	
Worldview*	
Motivations for being a data subject	
Political placement**	
Cultural**	
Environment	

Click icon to add picture



(profile name/title here)

**Role**

Customer / Actor / Owner

\*W of CATWOE

Figure 8: First draft, Profile / persona template

A set of privacy-specific questions about the activity was also drafted, addressing the system's fairness, lawfulness, transparency, purpose limitation, storage limitation, accuracy, data minimisation and security, as well as questions about who defines its privacy boundaries, what are the boundaries and what negative impacts arise. The place and role of these privacy and compliance type of questions proved to be problematic. The analysis of current PTM methods revealed weaknesses in compliance-driven approach (see Design science approach). The target system being compliant with the GDPR principles is highly relevant, but it is probably not useful to carry one out using the model, as that would lead to trying to identify what GDPR compliance issues would arise from imaginary activities. The aim of threat modelling is to answer "what can go wrong" as opposed to "what is wrong", which supports this idea. PTM is not supposed to produce an audit or a GDPR compliance check ("what is wrong"), but to highlight what could potentially go wrong. In chapter Aspects of privacy it was noted that compliance and privacy aspects may be separated. By this argument, a GDPR compliance check should be carried out as a separate activity from the systemic PTM. A similar issue concerned the question of 'facts'. Questions related to *facts* were drafted with a reservation that they may hinder the free creation of *fiction*-based inquiry devices (see earlier discussion regarding the fact and fiction metaphor). These fact-questions concerned the existence of personal data inventories, system diagrams, and other official system

documentation. This thinking helped to separate the GDPR compliance questions and fact-finding questions to their own ‘hard aspects’ thread (see Appendix 5) and leave the systemic aspects thread to concentrate on SSM activity model building.

### 6.3 The first pilot

The second iteration involved testing the drafted first version of Taiga in a quick pilot. The modelling target concerned a part of a research project contributing to the Mad@Work programme where keystroke and application usage data were gathered from volunteers’ laptops. The volunteers were knowledge workers employed by various companies. In addition to the automatic data capture as they carried on their daily work tasks, they were asked to self-report their perceived state of wellbeing at work. The data collected was used by researchers to produce an algorithm for a prototype solution that would identify workers’ wellbeing states based on the keystrokes and application usage.

The schedule for the pilot is shown in Table 4. All the workshops were held online. The PC screen was shared, and no web camera was used. In addition to the meetings below, preparation and analysis in between took 3 working days.

Table 4: First pilot, schedule

<b>Date</b>	<b>Workshops</b>	<b>Participants</b>
<b>11.6.2020, 45 min</b>	Threat modelling kick-off	Technical, scientists, project lead
<b>15.6.2020, 1 hour</b>	Interview (for models)	Scientists
<b>28.8.2020, 1.5 hours</b>	GDPR (compliance/hard aspects) workshop	Technical, scientists, project lead
<b>7.9.2020, 1.5 hours</b>	Model debate workshop	Scientists, project lead
<b>9.9.2020</b>	Threat catalogue sent to the participants	Technical, scientists, project lead

### 6.3.1 Interview (for models)

The interview lasted one hour, during which the stakeholders presented the system and voiced some of their privacy related concerns. They were interviewed using the question set shown in Table 3, with their answers noted down. The question set was not followed word by word at the end, since some of the questions' perspective was unclear, especially regarding whose perspective should be used for answering. All the information was nevertheless gathered by asking around the questions. The question set does not appear from the outset to be privacy focused and this prompted the participants to question its relevance during the interview. This was expected and it underlines the importance of explaining to the participants how the SSM based method is intended to work and how it links to privacy. Privacy can be generally expected to be taken to mean GDPR compliance and/or fundamental right to privacy, but the questionnaire revolves around activities, purposes, attitudes, power relations and so on. Checkland (2000, p. S45) addresses the potential attitudes to the SSM approach by noting that SSM-based threat modelling may appear overly complicated or somewhat 'soft' but defends it as a rigorous approach to the subjective: SSM gives structure for the exploration issues involving the human element. Small and Wainright (2018) also noted some resistance in their study due to the 'softness' of the method.

Based on the systemic aspects interview, three models were built. The stakeholders were not involved in this stage. SSM does not give a formula for choosing the viewpoints for the models, but the 'official' view is not likely to produce as ground-breaking insights as an alternative view (Checkland, 2000, p. S27). Nevertheless, model one view was based on the target as officially described. The reason for this was to test the model building stage and to demonstrate how the models are built to the participants at the future workshop. Since negative effects to data subjects is what privacy threat modelling tries to uncover, the second and third model were based on that idea. The second model (Figure 9) was based on the data subject view. The third model (Figure 10) portrayed an 'evil' system to harm the data subjects. One demonstration model and two alternative models was deemed to be enough to generate debate within the debate workshop's 2-hour timeframe.

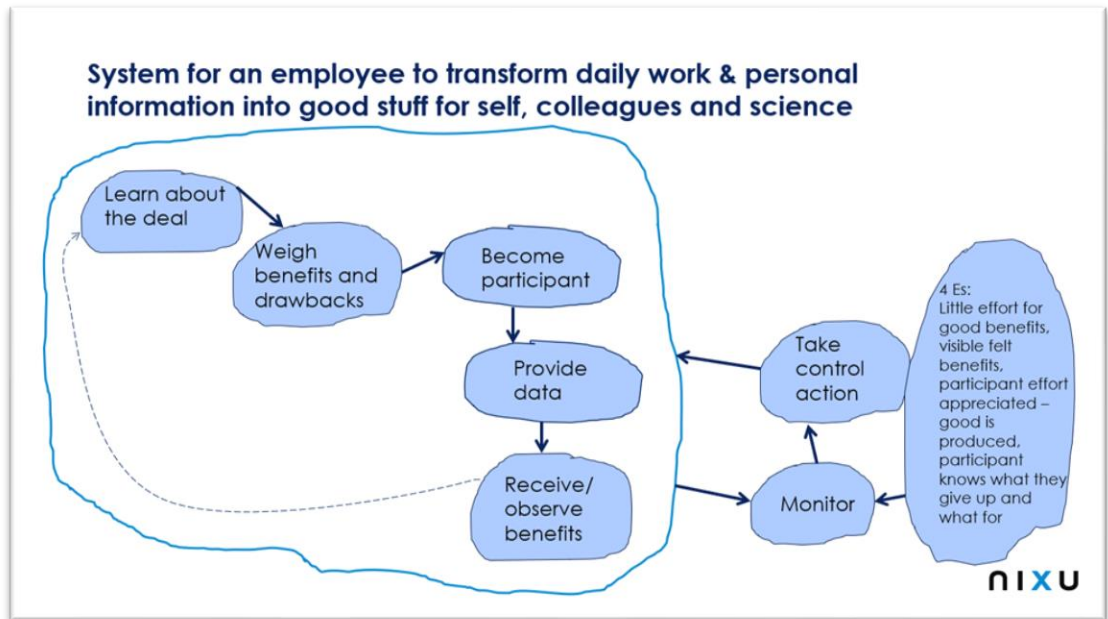


Figure 9: First pilot, Model built from the data subject's view

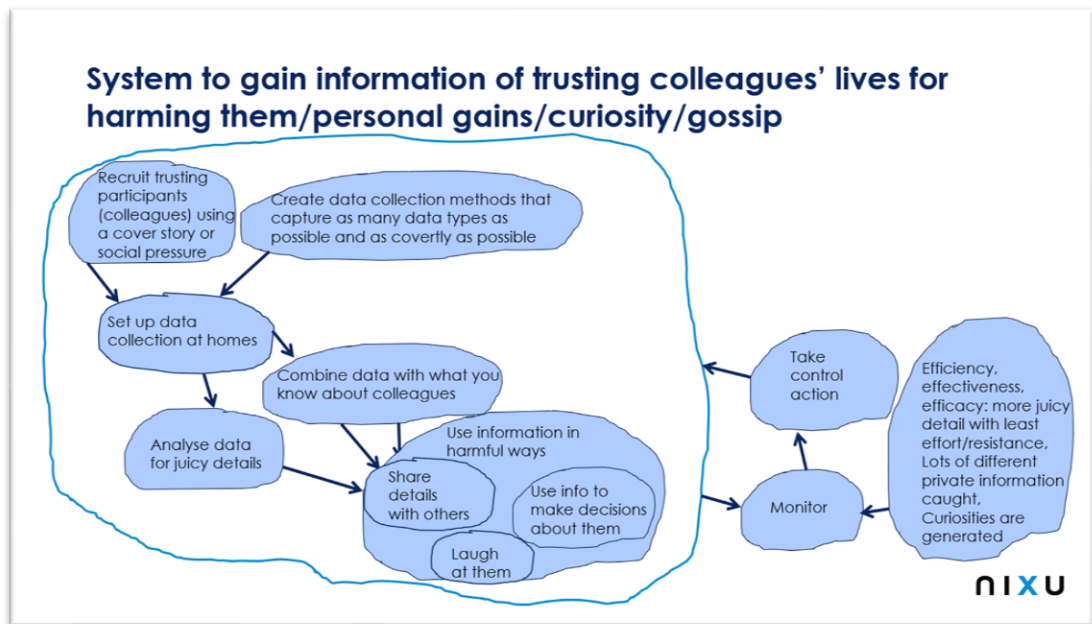


Figure 10: First pilot, Model from the view of causing harm to data subjects

### 6.3.2 GDPR compliance workshop

The hard aspects thread was initiated with a GDPR compliance workshop. The workshop was kept decidedly simple to ensure that the focus would stay on the SSM

based thread development and the pilot would not become a mere GDPR compliance assessment exercise. The analysis of current PTM methods had shown difficulties in incorporating compliance matters in threat modelling. This separation of matters which was recognised in the earlier cycle become pronounced as the innovation phase went on. Both the systemic thread and the GDPR compliance thread did try to uncover issues relating to the GDPR and privacy, so it was important to see how their output differed. There was a concern that whichever was done first would affect the results of the other. The GDPR compliance check could reveal everything that was there to reveal, leaving uncertain whether the systemic thread would have picked these up by itself.

At the GDPR compliance workshop a list of relevant GDPR articles was used as the requirements. The project lead, participating scientists and technical staff were present. In addition to the participants' responses, several documents were reviewed, including the research plan, information given to the research subjects and the technical description of the target system. Various shortcomings were identified and noted down during the workshop. Following the workshop, details of the identified threats or shortcomings were recorded in a table. The output was as expected from a GDPR compliance check. The threats corresponded to the requirements and showed gaps in them, for example gaps in informing data subjects and a lack of documentation. The identified threats are listed in Table 5.

### 6.3.3 Debate workshop

The third workshop was reserved for the debate around the models. This is the stage where threats are identified by debating the models against the real-world situation. The workshop was held two months after the initial interview due to the summer break. The break did not appear to affect the running of the workshop. At the workshop first the 'official' model was presented to illustrate to the participants how the models are built and how to read them (see Figure 11). The model represents the known situation. After this introduction, the alternative models showing the data subject and evil views were examined.

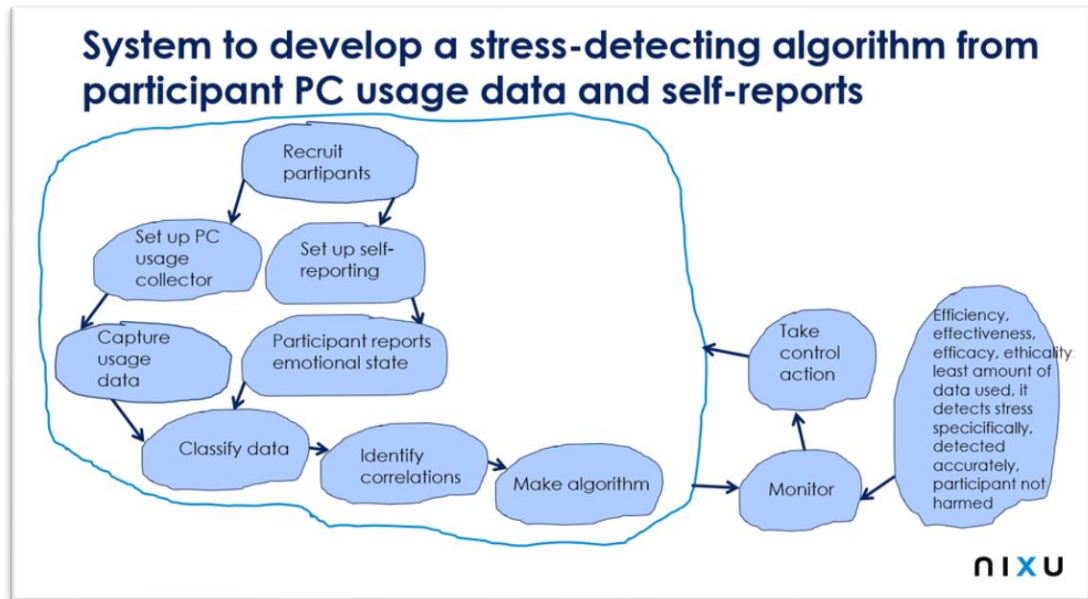


Figure 11: First pilot, model of the official activity (WAI)

It was crucial to get the participants to join in the debate with interest. The models provide a focus point and should feel like safe topics for all participants since they do not represent the reality, but something imaginary that may be freely questioned. The project lead engaged well and talked through any thoughts that the models sparked. At times other participants joined. It is possible that wider or more lively engagement could be achieved in a face-to-face debate, or with additional facilitation techniques. The group dynamics and the individual participants' current frame of mind (energised, tired, busy etc.) also play a role.

The main purpose of the models as inquiry devices is to generate dialogue, debate, and insights about the problem situation. Chekland's SSM does not prescribe what viewpoints they should represent. The models show an alternative reality and are therefore 'wrong', which can help to fuel the conversation. On the other hand, outrageously ridiculous activity model might cause the participants to disengage. The viewpoint of choice for the third model was more outrageous, since it presented the scientists acting unethically, but it was nevertheless received well.

At the workshop each of the steps on the activity models was considered one by one, and the questions "Does it exist in the real world? How? Could it? How?" were asked. The follow up question "What privacy issues may arise from it?" prompted the participants to consider the privacy threat aspect. This approach could be criticized

for not offering anything but the basic question “What privacy issues may arise from it?” for uncovering privacy issues. The Taiga method was to offer a new way to uncover privacy threats. Taiga does this by offering new viewpoints into the target, and expects that insights can be gained through them. It is an intriguing question whether privacy threats could be uncovered without ever asking that question, by following some defined steps. The models offer systems that can be more freely questioned than the real world, which helps the threat elicitation, but the user still needs to understand what might constitute a privacy threat to identify one.

The debate revealed a number of privacy threats, which were noted down. Following the workshop, the threats were recorded in the same table as the threats identified at the GDPR compliance workshop. The identified threats are listed in Table 5.

#### 6.3.4 Threat catalogue

Following the debate and the GDPR compliance workshop, a combined threat catalogue was produced containing the threats from both workshops, sent to the pilot organisation for comments and then finalised. The catalogue listed the identified threats, and for each, the scenarios in which they could arise, impact, likelihood, impact descriptions, mitigations, consultant’s assessment, and references related to the threat. The threat headlines are presented in Table 5, divided between threats identified at the GDPR compliance workshop and threats identified with the aid of the models.

Table 5: First pilot, threats produced

GDPR compliance threats ('hard' thread)	Threats from the models (systemic thread)
<p><b>H1) The information given to participant does not match the actual uses for their data:</b> Data use purposes are contained in various documents, archived data is used for other purposes than just storage, data is anonymised for further research</p> <p><b>H2) Consent does not meet GDPR requirements:</b> Consent for participation and consent for personal data use intertwined - consent for personal data use not clearly</p>	<p><b>S1) Researchers can identify their colleagues from the participants or make conclusions of who the participants might be:</b> Researchers carry out research on their colleagues, researchers know roughly who is taking part or hear at work who is taking part, researchers may combine their existing knowledge of participants with knowledge gained through research project, work colleagues figure out from PC usage patterns whose data it is (eg. they know a</p>

distinguishable, consent for personal data use missing, consent does not contain a clear description of processing purposes

**H3) Anonymised personal data is used for a kind of further research that the participant would not have consented to, if they had had a chance:** Anonymisation not recognised as a processing activity, consent form or privacy notice wording is not explicit of the purposes for which the data is anonymised for

**H4) Participant personal data in system components or back-ups is not managed:** Not all personal data locations are mapped, and data controller does not know about them, vendors take back-ups, employer takes back-ups of laptop or phone

**H5) Sensitive data is not managed according to the GDPR requirements:** Sensitive data not explicitly identified

**H6) Data protection by design and default principle not adhered to:** Lack of documentation to show data protection related design decisions and processes in the project development

**H7) Participant data is misused by software/hardware/platform vendor (processed in non-compliant manner):** Unfavourable, unclear or complex service terms and conditions, transfers outside EEA not safeguarded

**H8) Participants' use of their GDPR rights is impaired:** Joint controllership is not stated on privacy notice, participant data processed by various controllers

particular colleague always works very early mornings, and see this pattern on PC usage data)

**S2) Participant's employer gets access to participant data:** Participant uses work PC/phone and employer gains access to the data remotely, employer gains access to data when participant returns physical device to employer, PC hardware identifier gets linked to research data, employer's monitoring system picks up on research tools/research data as suspicious

**S3) Technical staff access participant/research data without a reason:** Employer IT staff install software or monitor PCs, research project technical staff has access to the databases and tools, IT department has access to databases and tools used in research

**S4) Participants are pressured to take part:** Consent is asked at the workplace, companies have promised to provide a certain number of participants and in turn put this pressure on their employees, company culture may lead to employees being obliged to take part

**S5) Participant data collection takes place when not intended:** participant forgets that system is collecting PC usage data because there is no visible cue to remind them



### 6.3.5 Learning from the pilot

General comments regarding the threat modelling exercise were also sought from the participants. The participants commented that they were not new to privacy or security issues and actively try to address them in their work. The scientists and the project lead were accustomed to considering ethical issues since the organisation was focused on research. In general, the participants felt that the exercise was useful and that they were left with actionable items, in the form of identified threats and potential mitigations for them. Regarding the systemic threat modelling thread, the participants felt that the models used in the debate stage were understandable. They also felt that the threat modelling exercise as whole went beyond what a regular GDPR compliance assessment would cover, and a comment was made that the target could be awarded a GDPR+ mark, if one existed, as a recognition of having gone further with compliance efforts. The systemic PTM thread was described as eye opening, referring to the new viewpoints that the models generated for the participants. They enabled the participants to see their work from new angles and revealed potential privacy and security issues. In later interactions, the participants continued to refer to the exercise as very useful, an opportunity to learn more and to see the target from new points of view and continued to encourage other organisations which were part of the larger research project to do this exercise.

The first pilot showed that the Taiga method's systemic PTM thread has potential for producing threats that are relevant and would potentially otherwise go unnoticed. The models opened completely new viewpoints and let the participants inside the data subject's or an evil scientist's way of seeing the target. The models as coherent wholes and working systems provided a rich ground for the debate. The GDPR compliance questions were clearly targeted at the technical solution and the officially described activity. The SSM models were not bound by these, but drew attention to the context, including the people in it, their potential expectations, culture and norms, and all the other aspects that made the context. This appeared to be major factor through which new threats were identified. An analysis is provided in Table 6 below.

Table 6: First pilot, analysis of how the threats were identified

Threat	Threat type and how the models revealed it
<b>S1) Researchers can identify their colleagues from the participants or make conclusions of who the participants might be</b>	<b>GDPR, privacy, research ethics, security</b> Model 3, the evil scientist view, revealed that the scientists and certain technical staff had access to data that could reveal identities of the participants.
<b>S2) Participant's employer gets access to participant data</b>	<b>GDPR, security</b> Model 2, the data subject view, showed the data subjects as employees and in turn, revealed that their employer would likely have access to employee devices and data.
<b>S3) Technical staff access participant/research data without a reason</b>	<b>GDPR, security</b> Model 3, the evil scientist view, gave further understanding of who has access to the research data and the systems storing or collecting the data.
<b>S4) Participants are pressured to take part</b>	<b>GDPR, rules around consent and ethical issues</b> Model 2, the data subject view, provided a richer understanding of the context in which consent is asked, i.e., the workplace, which uncovered this threat.
<b>S5) Participant data collection takes place when not intended</b>	<b>GDPR, transparency principle and UX/usability design</b> Model 3, the evil scientist view, gave ideas of how to make data collection invisible which pointed to the lack of information given to the data subject about ongoing data collection (such as a red recording light, or other a visual cue).

Based on the pilot, the following improvements were made to the method. Steps 1b and 1c (shown in Appendix 4) concerning the GDPR/privacy properties of the models were removed from the method. GDRP compliance check was useful to conduct alongside the SSM exploration but it became clear that *how* it is carried out does not need to be specifically defined in the Taiga method. The main idea is that they are two separate threads. Any suitable GDPR compliance assessment method may be used. The results showed that the three selected viewpoints for the models were useful and should be used next time as well. The introductory materials aimed at the participants were revised to further explain how the method works and how it relates to privacy, and linked to this, the question set was revised to make it easier to understand for the interviewees.

## 6.4 Review with privacy specialists

The first pilot had showed that the method was working as expected. Next, the method and the results of the pilot were presented to three colleagues for comments and discussion. These were all privacy specialists not involved with the method development. This informal review was used as a quick sense-check before the second pilot and to gain more objective evaluation. The receipt was positive and the difference between the threats found in compliance and systemic threat modelling threads was noted. One person commented that when carrying out threat modelling, an experienced privacy specialist commonly considers the context and risks arising from the context, but does this informally, and so a clear benefit of the SSM would be that it provides a structured way for doing this. The lack of methods for identifying context-based threats was also noticed during the review of current PTM methods. A question was raised regarding expertise required for using the method and how easily could privacy or security consultants be trained to use it, is extensive background knowledge required and can the method be taught. These questions were noted down for further research.

## 6.5 The second pilot

A second pilot was arranged with a company developing smart office lighting solutions as a part of the Mad@Work programme. It was soon identified that the target was not rich enough for systemic exploration with Taiga method. Its goal was anonymity and the LINDDUN method was chosen to identify threats instead. A failed experiment has learning value (Poskela et al., 2015, p 15) and in this case it helped to clarify what kinds of targets should Taiga be applied to. The research question sets the scene as “complex systems”. Aspects that indicate complexity and define systems were explored in the section Systems thinking, complexity and Soft Systems Methodology. These could be developed into a quick pre-screening tool before applying Taiga. Recalling the idea of WAI and WAD, it should be kept in mind that a system described as orderly and simple may have hidden complexity to it.

## 6.6 Ending the innovation phase

Since there were no other pilots available at the time and the first pilot had been successful, it was decided to close to iterations and move onto analysing the results and drawing conclusions of the research project. Lukka (2001) notes that a construct reaching and passing the market testing phase is a positive signal of the construct's success. Although an open market test did not take place, the method nevertheless passed the first pilot with success. The final form of the Taiga method is shown in Figure 12.

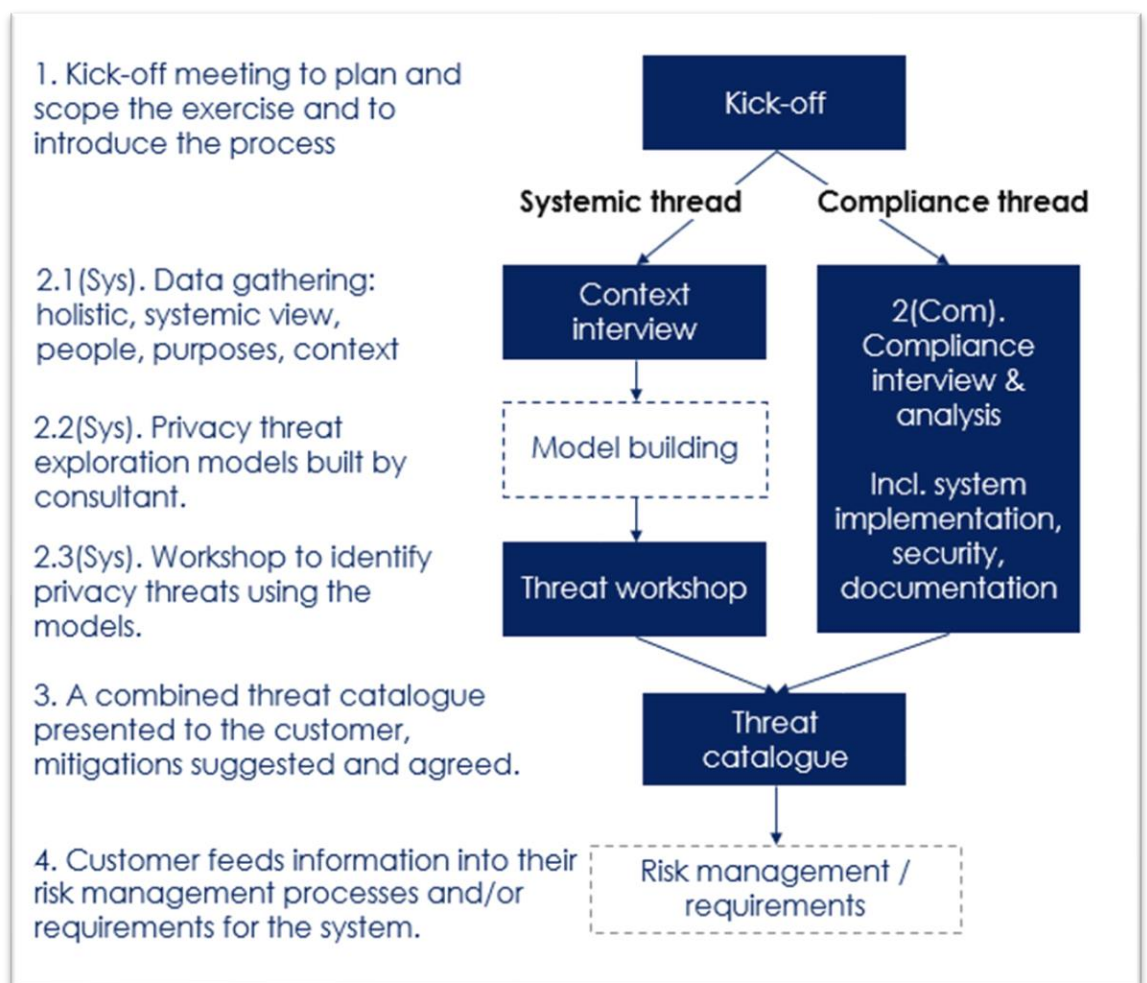


Figure 12: Overview of Taiga method

## 7 Results and discussion

This section lays out the results of the research and answers the research question: *How can privacy threat modelling (PTM) of complex systems be improved with the soft systems approach?* The sub-question a. concentrates on the method qualities, b. on the method in action and the quality of the research and development process, and question c. on the method's observed effects and output.

- a. What kind of a PTM method achieves this?
- b. How well was the PTM method implemented?
- c. What were the effects of using soft systems approach in PTM?

The research found that soft systems approach improved privacy threat modelling by helping to understand the target in its context and giving 'eye opening' insights into it from new viewpoints, a view that seemed to be missing from current methods. The current methods do not clearly differentiate between compliance threats and threats emerging from the functioning of target in its context. The usual approach is to examine the target through the already known things such as documentation, data, system designer' and owners' views, using already known frameworks such as compliance requirements or other lists. The main benefit of Taiga was that it recognises that both the known and unknown world exists, and they need to be approached differently. For the latter, Taiga provided a structured way for uncovering emergent privacy threats that would likely go unnoticed with other available privacy threat modelling methods. With the aid of SSM the target could be explored as a whole, without the constraint of externally set boundaries. The system could be explored as a system implementing different purposeful human activities, rather than only seeing its officially stated purpose. The resulting Taiga method arranges the exploration of compliance and systemic threats into one comprehensive method. The research results are analysed in detail through the sub-questions a-c under the following three subchapters.

## 7.1 Success factors

The question of what kind of a method can improve PTM can be answered by analysing the factors that contributed to Taiga's success. The key idea driving its success was the division of privacy threat modelling into two threads, systemic and compliance threats, and appreciating that they need to be approached differently. As the other major success factor, Taiga included a method for the identification of systemic privacy threats, based on SSM. SSM's success may be attributed to the new perspectives it gives, its participatory and exploratory approach to identifying threats, its focus around humans and human activity and the way it presents the problem to the participants. Modelling human activity from a certain perspective helped to maintain the focus on people and to identify things that may harm them (such as the data subject view in the first pilot), but also to identify threats arising from the needs of people in the models (such as the needs of the employer, scientists and technical staff in the first pilot). This in turn led to the revelation of hidden personal data processing cases in the target system, also known as the WAD. The compliance thread, on the other hand, could be seen as the exploration of WAI.

The SSM models aided privacy threat identification well. With the models, the participants could concentrate on one coherent story at the time. Viewing the problem situation as a story of human activity that can be walked through was likely the main factor that helped the privacy threat identification. After all, the question regarding privacy threats stayed simple "Can you see what privacy issues might rise?". Therefore, the insights must have risen from how the context was laid out. The threats could not have been identified by the researcher alone. Insights were generated from the participants' existing knowledge and experiences enriched with the new viewpoints through open but structured debate. SSM did not seem suitable for identifying compliance flaws because compliance turned out to be a too straightforward subject for SSM, since SSM is for understanding situations where both the question and the answer are unclear. Compliance threat headlines are already known, and whether they exist in the target or not is the only thing that needs be ascertained. This solidified the division of Taiga into two threads.

## 7.2 Implementation

Both the implementation of Taiga and the implementation of the constructive research method are discussed under this subchapter. Taiga's positive reception by the pilot and the privacy specialists indicates that it was implemented well. Its output, the threats it produced, points to this as well. The requirements set for it in chapter 6.2 were fulfilled, although with a few reservations. The method approaches privacy threats as a multifaceted issue: personal data use that may harm the data subject, unethical use of personal data, privacy as a conflict and threats to informational self-determination. The method was fully piloted only once and not on a complex target. This means that its scalability was not tested. The second pilot showed that Taiga is not suitable for a target with very low complexity. The method was usable in a professional setting by a consultant familiar with the SSM. It appears that the method can uncover with a reasonable effort a good number of threats that would not otherwise be found. The method was shown to produce the kind of threats that it was designed for. The produced threats were comprehensible by the customer. The threats were presented to the customer in a format which they can use in their internal processes. The threats were relevant and such that the customer could act on them.

Originally SSM was to be used to address all aspects of privacy, including compliance. A lot of effort went into trying to incorporate compliance aspects in the SSM-based exploration, but at the end compliance was separated to its own thread and removed from the influence of SSM. One of the ideas was that the models could be inspected for GDPR compliance. Templates were produced for this purpose, but it came clear that the models existed in the systems thinking world, being mere epistemological devices, and the question of GDPR compliance was firmly fastened to the real world. Applying GDPR on the model would have confused matters and would not have produced any useful learning about the real-world situation.

Personas was another aspect that was brought in. Data subjects are important in PTM and ideas were sought from interaction design and persona-non-grata threat modelling to strengthen their presence in the method. At the end, a simple template was produced to capture personas. Because SSM already included humans through

modelling human activity, it was decided to use the template only for gathering extra enriching information, rather than giving personas a more leading role. Deeper reasoning for this was provided in chapter Drafting the method.

In Taiga, SSM was followed fairly prescriptively. Privacy was brought in through the choice of perspectives for the models: the data subject view and the data subject harming view. The debate centred around the question whether privacy issues may rise. A template for capturing personas was produced. No other privacy-modifications were made to the SSM approach. This appeared to be enough to produce relevant threats, since the idea was to identify threats emerging from the functioning of the system in its context, and SSM is designed for this kind of use.

The constructive research method was followed as planned. Research reliability, validity and objectivity was to be ensured through successful piloting in a real setting (Lukka, 2000), transparent research process open to scrutiny (Checkland, 2000; Seppänen-Järvelä, 2004) participatory learning process and dynamically adaptive goal-seeking, impartial involvement of various stakeholders' views in an open democratic dialogue, practical wisdom, and critical subjectivity (Lindhult, 2019). Effort has been made to document Taiga's innovation and testing process in detail, to allow it to be scrutinised. The learning journal fuelled adaptive goal-seeking and critical subjectivity throughout the project. It produced useful insights especially for the stage where the first draft of the method was produced. Towards the end of the project, the notes started to get more disorganised, which made reflecting on them more difficult. Diligently following the learning journal structure and keeping to the note taking practice through quieter, less innovative parts is crucial. The learning journal reveals the power of the learning process and this helped the project to stay on schedule the author motivated. For example, a note from 8<sup>th</sup> July 2020 read:

***Feelings:** I have been putting off touching the thesis. The interview drained me and lowered my self-belief. I started question this "silly idea". **Intuition:** Once I get on my thesis then I will discover that it is actually OK. **Post-script:** What happened was that by opening the thesis I immediately felt energised when I saw my learning and how it had developed.*



Further learning diary excerpts have been included in Appendix 6. SSM, and therefore also Taiga's systemic thread, relies on open participatory debate for raising insights. However, SSM lacks facilitation methods, which is recognised weakness of the SSM (Jackson, 2000). In the first pilot, although a good number of meaningful threats were produced, the debate mostly heard the project lead. Skilled facilitation could have increased the others' participation. The practical wisdom generated in the pilot, i.e. the threats and new perspectives into the work, was highly valued by the pilot participants. The overall evaluation was weakened by the fact that there was only one full pilot. True action research should be conducted through many learning cycles, but this was not realised as substantially as originally hoped for. There were smaller learning cycles throughout the project, and the learning journal helped to reflect learning to theory within these. This learning could have been strengthened even more by paying more attention to where in the cycle the researcher was at any point, e.g. planning, experiencing or reflecting.

### 7.3 Effects and value to stakeholders

This subchapter discusses both the immediate and the wider effects of the Taiga method. Taiga produced relevant and interesting privacy threats, listed in Table 5, which was both surprising and expected. Surprising, as noted in the previous subchapter, there were not many privacy-specific additions to the SSM in Taiga. Expected, since SSM was designed to produce insights into complex situations and it worked as designed. The most valuable finding was that the threats produced through the compliance and systemic threads were clearly different – both threads had value and a unique approach. Taiga was efficient enough, based on the time spent on the interviews (systemic: 1 hour, compliance: 1.5 hours) and the debate workshop (1.5 hours). This produced five systemic privacy threats and eight compliance threats. Overall, the exercise took 4 working days. Out of this, preparing the models and refining and recording the identified threats on the threat table took 1-2 working days. These activities are likely to streamline through repetition, making the method swift to use. For example, Checkland (2000) suggests only about 20 minutes of preparation time per model. Moving to act in SSM Mode 2 should also help to smoothen the process. Compared to other available methods, Taiga can

pinpoint problem areas relatively efficiently and weighs up well against both unstructured brainstorming and detailed mapping style methods.

For the author, the project had immense learning value. Theoretical knowledge was deepened and widened, and many insights were gained regarding the nature of privacy and what privacy threat modelling means. As noted earlier, the learning journal was a priceless source of motivation and insight. Long term effects are likely to include cementing the use of a learning journal in personal professional practice and exploring oneself as a systems practitioner. Gaining skills for facilitation was recognised as a training need. In addition, the project has inspired the author to strive further academically.

For the pilot participants, the pilot generated understanding of the target and privacy threats in it as well as increased understanding of privacy issues in general. A widened perspective was the clearest effect. For the research sponsor, the effects are promising but not yet concrete. The method is not yet polished enough to be widely marketed, but the concept was proven, and the resulting method may be applied repeatedly to develop it further. Once Taiga becomes a marketable service it will show the project's final value to the sponsor. The wider business environment includes the method's future customers, and dissemination of the research results through blogs and other media can help to raise awareness of privacy threat modelling, its applications and different approaches to it. If future development produces a method which can be taught with relative ease, that may spark interest within the wider business environment too. The wider academic environment will enjoy a new field of application for SSM, as forecasted by Watson (2012), and hoped for by Warren et al. (2018). Warren sees the benefits of SSM studies as twofold: raising awareness and interest of SSM within academia, and increasing knowledge of field-specific problem situations, which here is privacy threats.

## **8 Conclusions**

This research project explored how current privacy threat modelling practice can be improved with the soft systems approach, namely Peter Checkland's Soft Systems Methodology. SSM is a systemic action research methodology designed for complex

targets that include the human element, to understand them and to instigate change in them. The research question was approached by developing and testing a new privacy threat modelling method, titled Taiga, that would use the SSM and answer today's privacy needs. Constructive research method was chosen as the framing method for the research, since it is meant for developing and testing a construct for the real world and also as it allowed the SSM cycle to be embedded within it, within its innovation and testing phases. This approach worked well. An innovative privacy threat modelling method was produced, which saw that compliance and systemic threats deserve a different approach. It proved to be successful in a pilot, producing threats on the system side that would have otherwise been unlikely to be uncovered, proving the concept of SSM improving privacy threat modelling. For uncovering systemic privacy threats that arise from the functioning of the target in its environment, the method harnessed SSM's capability of making sense of complex situations and gaining insights in them. In this case, the insights that were sought were privacy threats. Other strengths of SSM were its human activity focus and participatory nature.

## 8.1 Limitations and future research

The original research question specified 'complex system', but the complexity aspect remains unanswered. The method did not get to be tested against as complex system as originally hoped for. The target system had enough complexity to generate interesting threats, but for example, it only had one declared purpose for the personal data, a limited number of roles, and simple data types. This should be addressed in future pilots. Hopes are high as SSM was designed to make sense of highly complex situations.

Since Taiga went through one full pilot only, this appraisal does not include comparisons between pilots. Further pilots should be planned to include targets of high variety. Data gathering should be planned in more detail overall so that different pilots could be compared to each other effectively. In the first pilot, the collection of feedback from the customer was light and informal, and this should also be improved in future pilots. Further pilots should be arranged so that action learning is ensured.

Possible improvements to the Taiga method should be explored in the next pilots. Rich pictures and related techniques should be tested in the finding out stage, especially with highly complex targets. The question set for interviews should be revised so that the questions are easily understandable by participants or alternatively it should be tailored for each interview. The persona template's role in understanding the various stakeholders better and generating useful viewpoints to model should be inspected and clarified. The BATWOVE acronym should be tested in place of CATWOE, which would include the victim viewpoint in the models' root definitions (Midgley & Reynolds, 2001). The question of suitable mitigations to the found threats should be more formally addressed. Bringing in workshop facilitation techniques could increase participant engagement, addressing the lack of facilitation techniques, which is one recognised weakness of SSM (Mingers, 2000). Overall, more experimentation should be done in future pilots.

The method's usability by a consultant and how easily the method may be taught should also be investigated. This question was raised at the review with privacy specialists and would be an important future evaluation point for the research sponsor – referring to the “Can we make money with this?” evaluation need identified in 10. The method should be accompanied with a user guide that would state the method's purpose, its privacy definition, suitable targets etc.

## 8.2 Wider effects

Chapter Privacy threat modelling recognised three types of a privacy threat modelling method: compliance focused, tools for developers, and those that model context-based harms to a data subject. Taiga's biggest strengths lie in finding context-based threats. Thus, it may be used when privacy impact needs to be assessed, to complement a GDPR compliance assessment and improve impact assessment coverage. Neither the GDPR nor EU guidance give a method for identifying threats to data subjects arising from the functioning of the system in its context.

Out of the context-focused methods, Taiga's approach is not as resource heavy as PRIAM but is more structured than the Seattle method. Compared to PRIAM, Taiga's

main strength should be its scalability guaranteed by SSM, although it was not tested. The level of detail at the finding out stage can be easily adjusted to gather more information by complementing the interviews with the rich picture technique, and/or other relevant techniques such as the Systemigram. There is no limit to how many models are built and what viewpoints are used, which also helps scaling up.

Taiga method could also improve the spotting of issues early in a system development, as long as the developed system and its context forms a rich enough concept to build models and base debate around. In this kind of use case, the compliance thread could be left out. Since the systemic thread of Taiga gives a holistic view of the system, it can raise insights not limited to privacy. Taiga would be suitable to be incorporated in systems development to consider human issues, especially where systems development is itself viewed as action research (Rose, 2002). Compliance considerations could be brought in when the target is ready for it. However, Taiga is currently not refined enough to be usable by a non-trained person and so cannot replace for example the card deck based Elevation of privacy method. Since SSM is very good as an eye-opener, experiencing it once can motivate and remind users to consider various viewpoints in the future too, at best creating privacy-focused practice within the organisation. Finding out if Taiga could be polished into a straightforward method that could be used off-the-shelf by anyone could be a topic of further research. Checkland (2000) suggests that SSM in Mode 1 can be used for teaching purposes. Niu et al. (2011) showed that SSM is easy to understand by different stakeholders and it can be applied at low cost and by non-experts. On the other hand, Small and Wainright (2018) accounted some obstacles with SSM due to the unfamiliar nature of the approach when used in an organisation accustomed to hard methodologies. If persons in this kind of organisation experienced systemic modelling being used alongside a compliance assessment, and saw the difference in the produced threats, they could accept the approach more readily and start understanding privacy as a wider concept.

Overall, the project successfully proved the concept of SSM improving privacy threat modelling and showed that systemic and compliance privacy threats should be approached from different angles. This project could be viewed as yet another study where SSM has been applied to only find that it can give insights about its target, as

it is designed to do. In that sense, the results of the study were as expected. SSM can improve privacy threat modelling when the purpose and target of privacy threat modelling matches the intended application of SSM. This links to the other main revelation from this project, which is that uncovering privacy threats that arise from the functioning of the target in its context deserve a distinct approach. The Taiga method resulting from this research project may not be a polished method of its own as yet, but future development should focus in turning it into one, so that its practical value in addition to the research value can be fully realised.

## 9 References

- Ackoff, R. L. (1997). Systems, messes and interactive planning. *The Societal Engagement of Social Science*, 3(1997), 417-438.
- Ackoff, R. L. (1999). Transformational leadership. *Strategy & Leadership*, 27(1), 20-25. <https://doi.org/http://dx.doi.org/10.1108/eb054626>
- Armson, R. & Ison, R. (2004). Block 1 – Juggling with complexity: Searching for a system. *T306 Managing complexity: A systems approach*. The Open University.
- Article 29 Working Party. (2017). *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, wp248rev.01*. European Union, Article 29 Data Protection Working Party. [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=611236](https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236)
- awal street journal. (2015). *Systems Thinking Speech by Dr. Russell Ackoff*. <https://youtu.be/EbLh7rZ3rhU>
- Blitz, M. J. (2017). Comparing the Laws of Privacy. *Criminal Justice Ethics*, 36(2), 265-277. <https://doi.org/10.1080/0731129X.2017.1358922>
- Braithwaite, J., Braithwaite, J., Wears, R. L., & Hollnagel, E. (2016). *Resilient health care. volume 3, reconciling work-as-imagined and work-as-done*. CRC Press.
- Bultmann, J. (2017). *Introducing Threat Modeling for Seattlites*. <https://seattleprivacy.org/introducing-threat-modeling-for-seattlites/>
- Buttarelli, G. (n.d.). *Ethics*. [https://edps.europa.eu/data-protection/our-work/ethics\\_en](https://edps.europa.eu/data-protection/our-work/ethics_en)
- Checkland, P. (2000). Soft systems methodology: a thirty year retrospective. *Systems Research and Behavioral Science*, 17(S1), S11-S58. [https://doi.org/10.1002/1099-1743\(200011\)17:1+3.3.CO;2-F](https://doi.org/10.1002/1099-1743(200011)17:1+3.3.CO;2-F)
- De, S. J., & Le Métayer, D. (2016). *PRIAM: A Privacy Risk Analysis Methodology*. Springer International Publishing. [https://doi.org/10.1007/978-3-319-47072-6\\_15](https://doi.org/10.1007/978-3-319-47072-6_15)
- DistriNet Research Group. (n.d.). *About*. <https://www.linddun.org/about>
- European Union. (2012). *Charter of Fundamental Rights of the European Union, 26 October 2012, 2012/C 326/02*. <https://www.refworld.org/docid/3ae6b3b70.html>
- Council of Europe. (2010). *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14, 4 November 1950, ETS 5*. <https://www.refworld.org/docid/3ae6b3b04.html>

European Union Agency for Fundamental Rights. (n.d.). *Article 7 - Respect for private and family life*. <https://fra.europa.eu/en/eu-charter/article/7-respect-private-and-family-life>

Finnish Advisory Board on Research Integrity. (2013). *Responsible conduct of research and procedures for handling allegations of misconduct in Finland*. Finnish Advisory Board on Research Integrity.

F-Secure. (2018). *Elevation of Privacy, Privacy Cards for Software Developers*. <https://github.com/F-Secure/elevation-of-privacy>

Gartner. (2019). *Gartner Identifies the Top 10 Strategic Technology Trends for 2020*. <https://www.gartner.com/en/newsroom/press-releases/2019-10-21-gartner-identifies-the-top-10-strategic-technology-trends-for-2020>

High-Level Expert Group on Artificial Intelligence. (2019). *Ethics guidelines for trustworthy AI*. European Commission.

Information Commissioner's Office. (2018). *Sample DPIA template*. <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-impact-assessments/>

International Association of Privacy Professionals. (n.d.a). *Glossary of Privacy Terms*. <https://iapp.org/resources/glossary/>

International Association of Privacy Professionals. (n.d.b). *What does privacy mean?* <https://iapp.org/about/what-is-privacy/>

ITEA. (2020). *Mad@Work: Mental Wellbeing Management and Productivity Boosting in the Workplace*. <https://itea3.org/project/mad-work.html>

Jones, P., & Kijima, K. (2019). *Systemic Design*. Springer.

Kananen, J. (2013). *Design research (applied action research) as thesis research : a practical guide for thesis research*. Jyväskylän ammattikorkeakoulu.

Kokott, J., & Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4), 222-228. <https://doi.org/10.1093/idpl/ipt017>

Kurtz, C. F., & Snowden, D. J. (2003). The new dynamics of strategy: Sense-making in a complex and complicated world. *IBM Systems Journal*, 42(3), 462-483. <https://doi.org/10.1147/sj.423.0462>

Lukka, K. (2001). *Konstruktivinen tutkimusote*. <https://metodix.fi/2014/05/19/lukka-konstruktivinen-tutkimusote/>



Midgley, G., & Reynolds, M. (2001). *Operational Research and Environmental Management: A New Agenda*. Birmingham: The Operational Research Society. [https://www.researchgate.net/publication/315742111\\_OPERATIONAL\\_RESEARCH\\_AND\\_ENVIRONMENTAL\\_MANAGEMENT\\_A\\_NEW\\_AGENDA](https://www.researchgate.net/publication/315742111_OPERATIONAL_RESEARCH_AND_ENVIRONMENTAL_MANAGEMENT_A_NEW_AGENDA)

Miller, M. J. (2020). *Gartner's Top Strategic Technology Trends for 2021*. <https://uk.pcmag.com/news/129506/gartners-top-strategic-technology-trends-for-2021>

Mingers, J. (2000). An Idea Ahead of Its Time: The History and Development of Soft Systems Methodology. *Systemic Practice and Action Research*, 13(6), 733-755. <https://doi.org/10.1023/A:1026475428221>

MyData. (n.d.). *MyData*. <https://mydata.org/>

Niu, N., Lopez, A. Y., & Cheng, J. -. C. (2011). Using soft systems methodology to improve requirements practices: an exploratory case study. *IET Software*, 5(6), 487. <https://doi.org/10.1049/iet-sen.2010.0096>

Norman, D. (2005). Human-centered design considered harmful. *Interactions*, 12, 14-19. <https://doi.org/10.1145/1070960.1070976>

Organ, J., & Stapleton, L. (2016). Technologist engagement with risk management practices during systems development? Approaches, effectiveness and challenges. *AI & Society*, 31(3), 347-359. <https://doi.org/10.1007/s00146-015-0597-4>

Ottenheimer, D. (2020). *Advancing GDPR with privacy preserving tech*. <https://inrupt.com/Solid-GDPR>

Panetta, K. (2018). *Gartner Top 10 Strategic Technology Trends for 2019*. <https://www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2019/>

Petrides, L. A., McClelland, S. I., & Nodine, T. R. (2004). Costs and benefits of the workaround: inventive solution or costly alternative. *International Journal of Educational Management*, 18(2), 100-108. <https://doi.org/10.1108/09513540410522234>

Poskela, J., Kutinlahti, P., Hanhike, T., Martikainen, M. & Urjankangas, H. (2015). *Kokeileva kehittäminen*. <http://julkaisut.valtioneuvosto.fi/handle/10024/74944>

Regulation (EU) 2016/679. *General Data Protection Regulation (GDPR)*. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. European Parliament, Council of the European Union. <http://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32016R0679>

Reynolds, M., & Holwell, S. (2010). *Systems Approaches to Managing Change*. Springer London, Limited. <https://doi.org/10.1007/978-1-84882-809-4>

Reynolds, O. M. (1969). Review: Privacy and Freedom by Alan F. Westin. *Administrative Law Review*, 22(1), 101-106. <http://www.jstor.org/stable/40708684>

Rose, J. (2002). Interaction, transformation and information systems development - an extended application of Soft Systems Methodology. *Information Technology & People (West Linn, Or.)*, 15(3), 242-268. <https://doi.org/10.1108/09593840210444773>

Rubin, A. (2004). *Anita Rubin: Pehmeä systeemimetodologia tutkimusmenetelmänä*. <https://metodix.fi/2014/05/19/rubin-pehmea-systeemimetodologia/>

Selin, J. (2019). *Evaluation of Threat Modeling Methodologies* (Master's thesis). <http://urn.fi/URN:NBN:fi:amk-2019060615264>

Seppänen-Järvelä, R. (2004). *Prosessiarviointi kehittämissuoritusprojektissa Opas käytäntöihin*. Stakes.

Sharp, H., Rogers, Y., & Preece, J. (2007). *Interaction design: beyond human-computer interaction* (Second edition ed.). Wiley.

Shostack, A. (2017). *A privacy threat model for Seattle residents, white paper (draft)*. <https://seattleprivacy.org/threat-modeling-the-privacy-of-seattle-residents/>

Sion, L., Van Landuyt, D., Wuyts, K., & Joosen, W. (2019). Privacy Risk Assessment for Data Subject-Aware Threat Modeling. Paper presented at the *2019 IEEE Security and Privacy Workshops (SPW)*, 64-71. <https://doi.org/10.1109/SPW.2019.00023>

Small, A., & Wainwright, D. (2018). Privacy and Security of Electronic Patient Records – Tailoring multimethodology to explore the socio-political problems associated with Role Based Access Control systems. *European Journal of Operational Research*, 265(1), 344-360. <https://doi.org/https://doi.org/10.1016/j.ejor.2017.07.041>

Solove, D. J. (2006). A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3), 477-564. <https://doi.org/10.2307/40041279>

Spiekermann-Hoff, S., & Oetzel, M. C. (2014). A systematic methodology for privacy impact assessments: a design science approach. *European Journal of Information Systems*, 23(2), 126-150. <https://doi.org/10.1057/ejis.2013.18>

Stevens, J. E., & Crawford, S. L. (2020). *Project reporting instructions*. <https://oppimateriaalit.jamk.fi/projectreportinginstructions/>

The Financial Times. (2019). *FT sets the agenda with new brand platform*. <https://aboutus.ft.com/en-gb/announcements/ft-sets-the-agenda-with-new-brand-platform/>

The National Institute of Standards and Technology. (2020). *NIST Privacy Framework: A tool for improving privacy through enterprise risk management*. U.S. Department of Commerce.

The Open University. (2004). The Inquiring Process which is SSM. *T306\_4 Systems practice: managing sustainability* (pp. 169-189). The Open University.

The OR Society. (2018). *OR60 Peter Checkland - A Parthian shot (friendly)*.  
<https://youtu.be/DNsq7szZKvQ>

Toikko, T., & Rantanen, T. (2009). *Tutkimuksellinen kehittämistoiminta: näkökulmia kehittämisprosessiin, osallistamiseen ja tiedontuotantoon*. Tampere University Press.

United Nations General Assembly. (1948). *Universal Declaration of Human Rights*.  
<https://www.un.org/en/universal-declaration-human-rights/>

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, 4(5), 193-220. <https://doi.org/10.2307/1321160>

Warren, S., Sauser, B., & Nowicki, D. (2019). A Bibliographic and Visual Exploration of the Historic Impact of Soft Systems Methodology on Academic Research and Theory. *Systems (Basel)*, 7(1), 10. <https://doi.org/10.3390/systems7010010>

Watson, R. B. (2012). Suggestions for New Application Areas for Soft Systems Methodology in the Information Age. *Systemic Practice and Action Research*, 25(5), 441-456. <https://doi.org/10.1007/s11213-012-9233-0>

Which?. (2018). *Control, alt or delete? The future of consumer data*. London: Which?.  
<https://www.which.co.uk/policy/digital/2659/control-alt-or-delete-the-future-of-consumer-data-main-report>

White, S. M. (2015). Systems theory, systems thinking. Paper presented at the *2015 Annual IEEE Systems Conference (SysCon) Proceedings*, 420-425.  
<https://doi.org/10.1109/SYSCON.2015.7116787>

Wuyts, K. (2015). *Privacy Threats in Software Architectures* (Dissertation presented in partial fulfillment of the requirements for the degree of Doctor in Engineering).  
[https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1656390&context=L&vid=Lirias&search\\_scope=Liria s&tab=default\\_tab&lang=en\\_US](https://limo.libis.be/primo-explore/fulldisplay?docid=LIRIAS1656390&context=L&vid=Lirias&search_scope=Liria s&tab=default_tab&lang=en_US)

Wuyts, K. & Joosen, W. (2015). *LINDDUN privacy threat modeling: a tutorial* (Technical Report (CW Reports), volume C685 ed.). Department of Computer Science, KU Leuven.

Yleisradio. (2020). *Psychotherapy centre initially understated number of data breach victims*. [https://yle.fi/uutiset/osasto/news/psychotherapy\\_centre\\_initially\\_understated\\_number\\_of\\_data\\_breach\\_victims/11643235](https://yle.fi/uutiset/osasto/news/psychotherapy_centre_initially_understated_number_of_data_breach_victims/11643235)

## 10 Appendices

### Appendix 1. Stakeholder evaluation needs

Stakeholder	Potential evaluation needs and motivation	Stage of project	Potential evaluation criteria and methods
<b>Researcher (student, employee)</b>	Is my research topic interesting and motivating to me for the duration of the project? Have I chosen the right research method? How is my research design? How well am I achieving my research objectives? What have I learned from this iteration of the learning system? How am I meeting other stakeholders' needs (below)? <b>Evaluation for accountability / for development</b>	Before, during and after. Continuously and iteratively. <b>Formative / Summative</b>	Critically analysing and making justifications for my decisions in writing. Supervisor feedback. Regular observation and comparison.
<b>Sponsor (employer)</b>	Can we make money with this? Does this fit the company mission? Making money and strengthening brand. <b>Evaluation for accountability</b>	Before, during and after (short, medium and long term). <b>Summative</b>	Cost-effectiveness. Sales targets. Marketing and brand targets.
<b>University</b>	How good is this student's thesis? University needs students to graduate. <b>Evaluation for accountability</b>	During and immediately at the end. <b>Summative</b>	Efficacy of the thesis against the Master's assessment criteria. Review of thesis.
<b>Pilot organizations</b>	Was this worth the resources? Did we find privacy threats? Organisations want their products to be privacy safe and trusted. <b>Evaluation for accountability / for development</b>	During <b>Summative</b> (formative for the researcher)	Researcher: Efficiency, effectiveness and efficacy of threat modelling. Feedback from participants. Observation. Threat data collection.
<b>Wider business environment</b>	Is this useful or interesting? Can we use this or make money with this? Understanding, using and exploiting the method. <b>Evaluation for information generation</b>	Soon after (medium term). <b>Summative</b>	Utility and practical relevance of the developed method. Observation.
<b>Wider academic environment</b>	How does this contribute to the theory of ...? Good quality academic research and publications. <b>Evaluation for information generation</b>	After (long term). <b>Summative</b>	Relevance to theory base. Responsible conduct of research criteria. Citation quantity and analysis.

## Appendix 2. Summary table of privacy threat modelling methods

	What is privacy?	What kind of threats may be identified?	Threat elicitation method	Strengths	Weaknesses
<b>4.1.1 PRIAM</b>	The GDPR definition for data protection, but subjects can also include groups of individuals and the society as whole.	Threats that harm people in some way. Various threat sources.	The target is mapped and diagrammed from privacy perspective. Threats arise from interactions/linkages between the mapped privacy elements. Harm trees are constructed, and a risk assessment is performed using them.	A wide understanding of harms and privacy, strong focus on data subjects, recognition that combinations of elements generate threats.	Detailed mapping and extensive diagramming of the system is required, stakeholder involvement not described.
<b>4.1.2 Design science approach</b>	A combination of Solove's privacy taxonomy & requirements from data protection legislation.	Things that threaten privacy targets (compliance).	The system is documented from four angles. Data flow diagram is suggested as a simpler solution. Privacy targets are identified, and threats are anything that hinders the achievement of those. Stakeholder involvement is required for context-based threats.	A wide understanding of privacy.	Relies on privacy target identification, threats concern privacy requirements, no method for context-based threats or stakeholder involvement.
<b>4.1.3 DPIA, UK Information Commissioner's Office</b>	The GDPR definition for data protection.	Threats that harm people in some way. GDPR compliance, people's fundamental rights and freedoms.	Several exploratory questions from different angles, including personal data processing aims, practical implementation, context, data subjects' expectations and concerns, compliance, necessity and proportionality measures. Optional use of a data flow diagram is suggested. Stakeholder consultation, if deemed necessary.	Simple, easy to understand approach, flexible and scalable.	Requires some expertise, can end up superficial, since text boxes are small.

<b>4.1.4 Elevation of privacy</b>	The GDPR definition for data protection.	Threats which the deck has cards for, and potentially other ones through the discussion the cards generate among players. The cards partially cover GDPR compliance threats.	Practical approach with the aid of a data flow diagram and example scenarios/prompt cards. Free discussion.	Simple, easy to understand approach, flexible and scalable.	Requires some expertise, can end up superficial, no full coverage.
<b>4.1.5 LINDDUN</b>	Largely confidentiality of identity, achieved through data minimisation. Lighter on unawareness and non-compliance aspects.	Threats corresponding to the LINDDUN categories and found in LINDDUN threat trees.	Data flow diagram, threat trees.	Well-developed approach for ensuring confidentiality of identity by technical means.	Does not match well today's privacy needs, narrow privacy definition.
<b>4.1.6 Seattle residents' privacy threat model</b>	Aligns with Alan Westin's definition: self-determination of when, how and to what extent information is communicated to others.	Instances where someone is subject to data gathering, arising from the context.	Built around three questions: what are we working on, what can go wrong and what can be done. Use of brainstorming, listing of activities and data gathering, analysis of the lists and privacy trade-offs.	Participatory, simple, easy to understand approach, gives raise to insights.	Can result in too much data to handle, requires some expertise, no final version available.

# Privacy threat modeling

As part of Nixu's involvement in the Mad@Work -project, we are developing a method to **threat model complex human-centric systems** from the **privacy** angle. This furthers the privacy goals of Mad@Work and its partners' achievement of their own project goals – as Nixu is offering to threat model the pilots and solutions.

## Benefits

### For you:

- You gain understanding of relevant privacy threats to your system, so that you can mitigate them.

### For us:

- Nixu will get to test and develop the method iteratively through using it on various solutions and pilots at their different development stages.

## Why Privacy threat modeling?

A key goal of Mad@Work is to develop unobtrusive, privacy-safe and ethical systems for furthering employee wellbeing at work.

From our experience, **identifying relevant threats is the most challenging step** for companies when assessing privacy risk. Risks to 'rights and freedoms' are tricky to grasp and the DPIA framework does not guide how to elicit threats in practice.

## Our approach

Nixu's approach is participative and user-centric and utilises techniques from Systems Thinking, such as different diagramming methods and building different human viewpoints into the solution, which are then used to explore it.

### Knowing your threats is essential for...

- Mad@Work aim
- privacy-safe solutions
- GDPR compliance
- DPIA (mandatory)
- Privacy by Design

Let's get started!

To find out more and to arrange an exercise, email or phone: Tuisku Sarrala, Senior Privacy Consultant  
[tuisku.sarrala@nixu.com](mailto:tuisku.sarrala@nixu.com) +358 40 672 8727

**nixu**

## Appendix 4. First draft of Taiga

**Question set for interviews:**

Question	Feeds to
What is this system for you? (Capture its essence in one sentence)	Root definition
Whether a tech solution existed or not, what is it that you want to do/need to do/achieve?	Root definition
Who does it serve? Who is it for?	CATWOE – C
Who does it? Who are part of the delivery?	CATWOE – A
What does this activity really do? What would you like it to do?	CATWOE – T, P - What
How do you do your activity? What activities make up your activity?	CATWOE – T, Q - How
What is needed for this activity? Materials, data, money etc.	Input
What comes out? What are you trying to make?	P - What, Output
Where in the wider/bigger picture you see this activity?	CATWOE – W, P/C
Are you (company, team, people) a typical one?	CATWOE – W, P/C
Does it matter to you? Care about it? Who does?	P/C
Who or what has power over this?	P/C
In relation to your other activities, where is this?	P/C
Why do you do the activity?	CATWOE – O, Q - Why
What are the expectations placed on you? Who places them?	CATWOE – O
Are you bound by some rules, laws, money, particular technology, or other constraints placed from the outside?	CATWOE – E

### Profile / persona

Question	Fill in
Description	
Goals	
Tasks	
Vulnerabilities	
Likes / dislikes / attitudes	
Worldview*	
Motivations for being a data subject	
Political placement**	
Cultural**	
Environment	

Click icon to add picture

(profile name/title here)

**Role**

Customer / Actor / Owner

Optional step: drawing of a rich picture (not piloted)



## System definition – Step 1a

<b>This is a system to:</b> (input, transformation, output)			
C - Customers			
A - Actors			
T - Transformation			
W - Worldview			
O - Owner			
E - Environmental constraints			
efficiency		What to do (P)	
effectiveness		How to do it (Q)	
efficacy		Why do it (R)	
ethicality			

## System privacy compliance – Step 1b

How GDPR requirements appear in the model.

Fairness	
Lawfulness	
Transparency	
Purpose Limitation	
Storage Limitation	
Accuracy	
Data minimisation	
Security	

Removed from the final version

## System privacy definitions – Step 1c

How privacy is defined in the model

Who are the boundaries defined by?	
What/where are the boundaries of privacy in this system?	
What are the negative impacts the boundary setter perceives?	

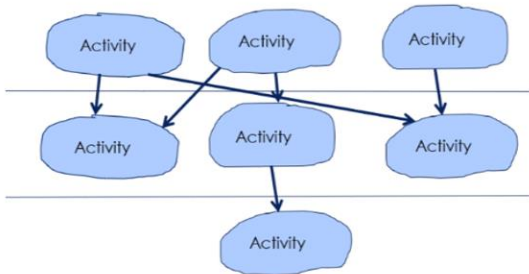
Removed from the final version

## System activities – Step 2

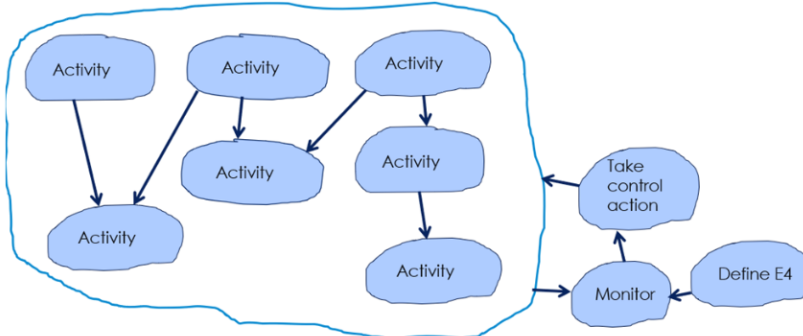
This is a system to:  
(input, transformation,  
output)

	Activities needed to be carried out	At once?
1		
2		
3		
4		
5		
6		
7		
8		
9		

## Activity sequence model – Step 3



## Built inquiry device – Step 4



## Inquiry & debate



Activity no.	Does it exist in real world? How? Could it? How?	What privacy issues it might rise?
1		
2		
3		

## Appendix 5. Hard aspects

### What can be observed in the real world?

- Guidance documents and system manuals
- Inventories
- Interview answers to direct questions
- Observed GDPR principles
- System functionalities, data fields etc.
- Security assessment results

### Interviews – real world

Question	
Do you have lists/records/inventories for GDPR?	
Do you have plans/drawings/diagrams?	
Do you have guides/policies/literature?	
What data processing constraints the planned technologies involve?	
Do you have constraints regarding lawfulness, fairness, transparency... etc.?	

GDPR compliance assessment method not included: any suitable method can be used.

## Appendix 6. Excerpts from the Learning journal

Date	Selected excerpts from learning journal
19.2.2020	<p><b>Factual:</b> So many things to research. Spent a lot of time reading about what systemic methods are, trying to find one that sounds applicable to my study.</p> <p><b>Emotions:</b> Overwhelmed, so many options and threads! Exited by the systems world. Reality weighs... is this realistic?</p>
7.3.2020	<p><b>Idea:</b> Should I record separately “about research method” and “about threat eliciting method” so that I know which one I am thinking about?</p>
24.4.2020	<p><b>Factual:</b> Read about SSM. Es – effectiveness, efficiency, efficacy... <b>Idea:</b> Could measuring performance of the logical machine be changed to measuring its privacy effectiveness? Could ethicality be the 4<sup>th</sup> E?</p>
2.5.2020	<p><b>Factual:</b> Have documented the SSM method, Shostack style modelling and own experience of modelling, and done comparison. Interesting that Shostack notes that threat elicitation is the trickiest phase.</p> <p><b>Intuitions:</b> Do businesses want huge things modelled? Maybe businesses want waterfall process? (side note 11.5. choosing to ignore this hunch). I think I have gone astray with the thesis. Can I use SSM to research whether SSM is good for threat modelling? (side note: found the answer – various meta-level learning – learning system produces learning about the learning, about the target and about method)</p>
4.5.2020	<p><b>Factual:</b> Planning evaluation and writing an evaluation essay. Analysed a real life privacy consulting case on paper.</p> <p><b>Problems:</b> How do I bring GDPR in the method? Built into tools? Knowledge of consultant? How about building ‘good’ models to compare to ‘bad’ real world? (side note: not a good idea – but good questioning of the models’ purpose!)</p> <p><b>Insight:</b> (from going through notes later) In consulting, when doing GDPR assessments, we compare what people tell us to the documentation they supply us, and find discrepancies. Kind of real world vs imaginary world.</p>
5.5.2020	<p><b>Insight:</b> Privacy is kind of a conflict... so bringing up everyone’s interests could help finding solutions. Need to get a “clean” (verbal) view of the system, not a corrupted one with system plans. Example: manager shows official plan, a worker tells a completely different story.</p> <p>I should divide the threat modelling in exploration of real / hard stuff and exploration through systems models.</p> <p>Threat modelling is not what IS wrong but what CAN go wrong. Not audit. Not gap assessment. (side note: Good point.)</p>

	<p>Is system GDPR compliant -&gt; cannot be ascertained if purposes are not clear, BUT can highlight potential issues? (side note: Through inquiry devices!) GDPR check in stage 2 once models have been used?</p> <p><b>Problem:</b> Why bother with SSM? (side note 8.7.: Encouragement to self: It can reveal stuff that you would not otherwise see or think to look. Otherwise we'd assess FICTION, documented FICTION. When stuff goes WRONG is not when it is all used exactly as IMAGINED!</p>
11.5.2020	<p><b>Learnings:</b> Be more conscious about PDCA. Fact/fiction divide seems to be the most important point learned. Method feels robust enough, now I have question set and method mapped.</p> <p><b>Insight:</b> Can SSM be applied to simple targets, like one IoT device? First I thought SSM would be not suited, but the device could be imagined as a part of a complex situation (drawing of people with lots of use cases for it) (side note: Here is a simple device in a rich context – rich context is important)</p>
9.6.2020	<p><b>Factual:</b> The method is ready but not tested. Should I mock test it? How to add privacy in it? How about user personas? Read about Interaction design. Read about interviewing styles, structured and unstructured. Questionnaires. Contextual interviews.</p> <p><b>Ideas:</b> What to get out of threat modelling? Capturing purposes -&gt; systems models. Capturing connections/hidden things/emergence? How to identify emergence? Read about the law of unintended consequences, technological assessment, Collingridge dilemma, the precautionary principle. Too much to go for...!</p>
15.6.2020	<p><b>Factual:</b> First interview done. Received a comment “What’s this got to do with privacy?” Need better intro. Scoping questions was difficult. Whose perspective should they be answered from?</p>
8.7.2020	<p><b>Feelings:</b> I have been putting off touching the thesis. The interview drained me and lowered my self-belief. I started question this “silly idea”. <b>Intuition:</b> Once I get on my thesis then I will discover that it is actually OK. <b>Post-script:</b> What happened was that by opening the thesis I immediately felt energised when I saw my learning and how it had developed.</p>
5.8.2020	<p><b>Feelings:</b> Hard to sit down even I love the work! How can I motivate myself to sit down?</p> <p><b>Ideas:</b> Privacy definition... I thought my method was about MyData style privacy but it seems to be about data protection...? Maybe it boils down to purposes anyway since people cannot make informed choices without knowing the purposes. (drawing about the relationship between purposes, legal basis, personal choice, transparency) (drawing about purposes for the debate, with linked issues of ethical, legal, cultural and political). How about threats? Are the purposes that may be harmful? Once purposes are known, we can question if it's OK, necessary, fair etc... Hmm... who</p>

	<p>wants to just model purposes... don't they want to model overseas transfers and whatever compliance things, or are those revealed too? The method is essentially about exploration of purposes and secondarily trying to accommodate conflict between people and data user.</p> <p><b>Factual:</b> Explored meanings of privacy</p>
<b>18.9.2020</b>	<p><b>Factual:</b> Have achieved a lot of clarity. Only testing the method showed what it brings. The project leads comment was very telling: "eye-opening" referring to the kind of insights that systemic inquiry brought.</p> <p><b>Problems:</b> How does compliance analysis and systemic inquiry work together? What place does each one take? Targets are small but the method is aimed at huge projects.</p> <p><b>Ideas:</b> Move from Mode 1 to Mode 2. Think what models would be useful.</p>
<b>18.10.2020</b>	<p><b>Insights:</b> I did not have to mash privacy into this, this is more about exploring a complex situation. Looking at the target from various perspectives. Seeing things that are not said (WAD/WAI). Gaining the lost data subject view. This is good since there is no method for people+threats. Tried modelling pilot two. It is too simple. We do not have a problem situation. Would have needed more concept.</p>
<b>8.11.2020</b>	<p><b>Thoughts:</b> Leave out the element of complexity? Need to get this finished. Mode 2... can I suggest moving to Mode 2 when the method is meant to be easy to use?</p>
<b>22.11.2020</b>	<p><b>Factual:</b> Going through thesis, filling gaps. Analysing science articles. Looking for insights in diary.</p>
<b>10.1.2021</b>	<p><b>Reflection:</b> Difficult to know was something in this project just too difficult to understand or impossible/stupid to follow (i.e. GDPR for models). Perhaps if something feels too hard, there is probably something fundamentally wrong with the idea?</p>