Achieving Usable Security and Privacy Through Human-Centered Design

Eduard C. Groen, Denis Feth, Svenja Polst, Jan Tolsdorf, Stephan Wiefling, Luigi Lo Iacono, and Hartmut Schmitt

1 Introduction

Scope and Motivation Numerous examples show that cybersecurity and data protection measures need to be designed in such a way that end users can interact safely with digital systems (e.g., [81, 100]). This user orientation is addressed by the field of *usable security and privacy* (USP). USP aims to support the design of security and data protection measures in a way that: (1) users, designers, and developers are supported in the best way possible in their security- or privacy-related projects and (2) the measures contribute to a continuously positive user experience. Because of our research background and projects, in this chapter, we will focus primarily on usable privacy. However, usable security and usable privacy usually go hand in hand, which makes it sensible to view them as a common research discipline. Thus, our recommendations should be equally applicable to security-related topics.

Problem and Idea In practice, the fields of requirements engineering (RE) and user experience (UX) design are tasked with translating data protection regulations into a system's implementation through requirements and design concepts. Although both disciplines have decades-long expertise with security and data protection requirements, the changes in international data protection regulations

E. C. Groen (✉) · D. Feth · S. Polst
Fraunhofer Institute for Experimental Software Engineering IESE, Kaiserslautern, Germany
e-mail: eduard.groen@iese.fraunhofer.de; denis.feth@iese.fraunhofer.de

J. Tolsdorf · S. Wiefling · L. Lo Iacono
Hochschule Bonn-Rhein-Sieg, Sankt Augustin, Germany
e-mail: jan.tolsdorf@h-brs.de; stephan.wiefling@h-brs.de; luigi.lo_iacono@h-brs.de

H. Schmitt
HK Business Solutions GmbH, Friedrichsthal, Germany
e-mail: hartmut.schmitt@hk-bs.de

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_5

and the digital transformation impose new challenges on these disciplines. A particularly challenging question is how to equip end users of systems—both data processors and data subjects[1]—with the appropriate decision support, transparency, empowerment, and other resources.

Proper design of USP requires new questions to be answered to make the right data protection design choices, such as: What understanding do stakeholders—particularly end users—have of privacy and data protection? What kind of privacy-specific needs do they have? And how can we categorize stakeholders into groups? The answers to these questions strongly affect the way a system is designed and its security and privacy properties are made usable, thereby achieving *usable security and privacy* (USP; see Sect. 2.2). Functionally, they influence what the system should do; quality-wise, they affect how well it is adapted to the stakeholders' characteristics and context. Unfortunately, existing security frameworks (e.g., BSIMM, SAMM, Common Criteria), models (e.g., MS SDL), and best practices (e.g., the OWASP guides) barely consider usability and user experience.

Our idea is to firmly cement security and privacy into the *human-centered design* (HCD) process. The HCD process includes the human perspective in a software system's design process and ensures that it is developed in a way that its interaction helps human actors make the "right" security and data protection decisions intuitively in the corresponding use cases, thereby minimizing potential errors by misconfiguration. Techniques for RE and UX that guide practitioners to obtain the correct privacy-related answers are still emerging. Including these techniques in the HCD process helps to ensure that the stakeholders are properly considered during the design of these security and privacy aspects.

Contribution and Structure In this chapter, we present three complimentary USP-oriented methods developed on the basis of good practices, which can be used in HCD, RE, and UX design processes. Together, these methods provide practitioners tasked with designing the USP for a system with a practical toolkit, helping them to assure that USP aspects are sufficiently considered in the HCD process:

1. Eliciting and modeling the **mental models** of end users with respect to security and privacy in order to understand the stakeholders' assumptions and expectations (Sect. 3)
2. Eliciting and analyzing the **privacy needs** of data subjects and the **data usage needs** of data processors in order to understand the stakeholders' privacy-related requirements (Sect. 4)
3. Collecting and structuring user characteristics along dimensions into **user group profiles** and **privacy personas** in order to understand typical stakeholder perspectives on the protection of their data (Sect. 5)

[1] According to the GDPR [27], *data subjects* are natural persons whose personal data are processed; *data processors* are legal entities or individuals that process personal data of others; *processing* includes gathering, storing, using, transferring, and deleting personal data.

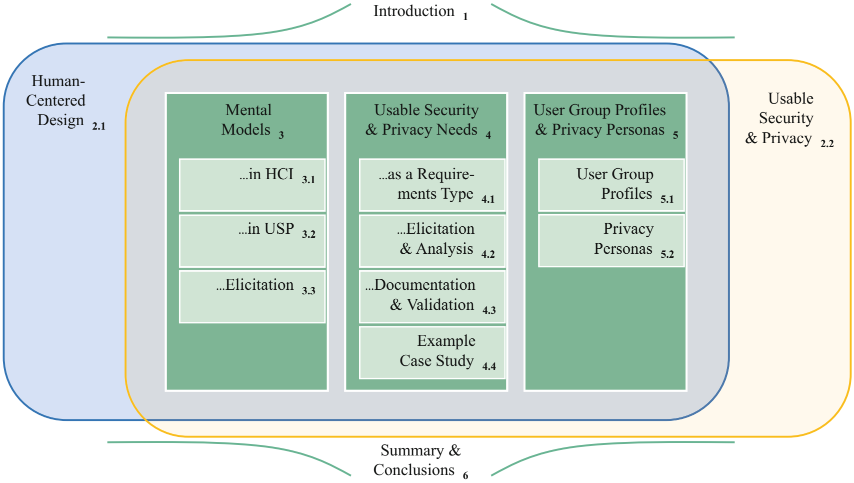

Introduction 1
Human-Centered Design 2.1
Usable Security & Privacy 2.2
Mental Models 3
...in HCI 3.1
...in USP 3.2
...Elicitation 3.3
Usable Security & Privacy Needs 4
...as a Requirements Type 4.1
...Elicitation & Analysis 4.2
...Documentation & Validation 4.3
Example Case Study 4.4
User Group Profiles & Privacy Personas 5
User Group Profiles 5.1
Privacy Personas 5.2
Summary & Conclusions 6

Fig. 1 Overview of this chapter's structure

Figure 1 presents the structure of this chapter. In Sect. 2, we first describe the two concepts underlying this chapter: HCD and USP. We then present the three aforementioned methods in Sects. 3–5. In Sect. 6, we conclude by outlining implications of the USP elicitation techniques. This structure enables readers interested in applying a particular technique to consult only its corresponding section, while we recommend that casual readers follow this chapter's sequential order.

2 Background

2.1 Human-Centered Design

HCD reflects the consideration of end users in the design of systems. The goal and main argument for using an HCD process is to increase the fit of the product to the requirements of end users by involving the stakeholders themselves in the design process. Stakeholder involvement is also intended to minimize the risk of erroneous design decisions. So far, however, the various requirements for security and user experience have mostly been elicited as an incidental by-product—if at all—in HCD. With regard to usable security and privacy (USP) requirements, no best practices exist for many application domains yet, let alone verified research experience. Feth, Maier and Polst [30] proposed a model for USP, using smart homes as an application example. They mapped different parts of their model to the activities in the HCD process. However, mental models and personas were not considered in the model, and USP needs were not addressed as detailed as in this chapter.

ISO 9241-210 [49] is the international standard for HCD for interactive systems. It is complementary to existing design methodologies and provides a human-centered perspective that can be integrated into different design and development processes. ISO 9241-210 provides the following principles for human-centered approaches that should be followed, regardless of the design process or the allocation of responsibilities and roles:

- The design is based upon an explicit understanding of end users, tasks, and environments.
- End users are involved throughout the design and development.
- The design is driven by and refined through user-centered evaluation.
- The process is iterative.
- The design addresses the whole user experience.
- The design team performing HCD includes multidisciplinary skills and perspectives; this does not require a team to be large, but it should be sufficiently diverse to collaboratively make trade-off decisions regarding design and implementation at appropriate times.

The HCD process consists of four activities for designing an interactive system, which in this chapter we relate to USP:

Activity 1: Understanding and Specifying the Context of Use According to ISO 9241-210, the context-of-use description shall include the following:

- *The end users and other stakeholder groups:* There can be a range of different user groups as well as other stakeholder groups whose needs are important, also regarding security and privacy.
- *The characteristics of the end users or groups of users:* End users have different needs and characteristics regarding privacy and security. Eliciting the end users' mental models promotes a better understanding of their subjective conception of technical processes (e.g., data processing) and tasks. The identified user groups can be described in the form of user group profiles or personas. Their relation to personal data helps determine whether they have privacy needs as data subjects and/or data usage needs as data processors.
- *The goals and tasks of the end users:* The types and frequency of tasks that end users typically perform can be part of the persona descriptions, while USP needs are intertwined with particular goals regarding the use or protection of personal data.
- *The environment(s) of the system:* Relevant questions concerning the technical, physical, or socio-cultural environment can be, e.g., Do the end users need to interact with the system when they are preoccupied with other activities? Are there presumably many bystanders? Can someone watch over a user's shoulder and read the screen? Is the data transferred via public or private Wi-Fi?

Activity 2: Specifying the User Requirements Identifying user needs and specifying the functional and other requirements for the system being designed are crucial activities. A specific subset of needs are USP needs, which can, among other things, be analyzed in order to derive further privacy requirements. The intended context of use includes the (personal) data used in and transferred by the system. A quality model can ensure that the goals of different stakeholders are taken into account and that all relevant quality aspects are considered: data quality, product quality, quality in use, process quality, and structural quality [82].

Activity 3: Producing Design Solutions Established best practices facilitate the design of solution prototypes and final designs. In the USP context, three different levels of best practices can be distinguished [92]: (1) *principles* as general fundamentals that should be considered during the development process; (2) *guidelines* as descriptions for adopting these principles, and (3) *patterns* as reusable and proven solutions to commonly occurring problems appearing in system development.

Activity 4: Evaluating the Design User-centered evaluation is an essential element of HCD. Because user tests are usually time-consuming and costly, it is advisable to first conduct an expert-based heuristic evaluation for USP [29]. Another part of the evaluation is the assessment of compliance with legal standards, for which the USP needs provide a helpful basis. In the European Union, the GDPR has the greatest regulatory impact, especially as it defines the rights of the data subject, which include the right of access, the right to rectification, and the right to erasure.

2.2 Usable Security and Privacy

As mentioned earlier, USP refers to inter- and transdisciplinary methods for designing security- and privacy-enhancing measures in such a way that: (1) users and security engineers (e.g., designers and developers) are supported in the best way possible in their security- or privacy-related goals and projects and (2) the measures contribute to a continuously positive user experience (e.g., promoting intuitive decision-making on choices regarding data privacy) [39, 81].

USP gained attention and relevance in the mid-1990s when computers entered every household and the Internet became widespread. In 1996, Zurko and Simon [105] proposed three categories for a user-friendly security agenda: (1) usability testing for security systems; (2) security models and mechanisms for user-friendly systems, and (3) consideration of the end users' needs as the primary goal(s) for secure system development. This was a radically new perspective, as end users were often still regarded as a security threat at the time. Other works such as those by Whitten and Tygar [99], Adams and Sasse [3], and Blythe, Koppel and Smith [8] built upon this work.

In the 2000s, USP gained momentum in research. Several standard works dedicated to this topic were published—such as [7, 23, 46, 85]—and many studies were conducted [20, 35–37, 87]. 34 of those earliest works were collected in an anthology [21] focusing on realignment of usability and security, authentication mechanisms, secure systems, privacy and anonymity systems, and commercialization of usability. Garfinkel and Lipford [39] provide a good summary of the field up to 2014, while the work of Fischer-Hübner et al. [31] (in German) is also still up-to-date in many areas.

In recent years, the field of USP expanded to cover topics including ubiquitous computing, smart home, and online privacy. Current research trends also reflect trends in social challenges and themes. Two examples are inclusiveness and diversity, which are both increasingly getting attention in the USP community [59, 70]. Moreover, the surge in employees working from home during and after the COVID-19 pandemic has increased the need for USP [26]. For a more detailed summary of USP research, please refer to the chapter "Empirical Research Methods in Usable Privacy and Security".

3 Mental Models in Security and Privacy

Mental models are personal internal representations of the *external reality* that help people understand their surroundings and guide their actions [52]. On a more abstract level, the external reality can represent any kind of *target system* or problem space that people have to deal with: It can be simple and concrete, like finding our way to the kitchen, or complex and abstract, like dealing with climate change. Mental models essentially convey an individual's perception, imagination, knowledge, and comprehension of a particular target system. When people deal with security and privacy issues in cyberspace, their actions are inevitably the result of their concepts regarding technology, tools, or threats contained in their mental models. In case of misconceptions, people may bypass security measures or avoid using privacy settings because they do not understand how they work or what benefit they bring. It is therefore important to consider end users' mental models in the design of a system, as this helps designers and developers of security and privacy mechanisms to align those mechanisms with the end users' understanding and expectations. This can help increase end users' acceptance and enables them to make informed decisions regarding security and privacy. In Sect. 3.1, we will first define key properties of mental models that are specific to their application in human–computer interaction (HCI). In Sect. 3.2, we will detail for which purposes mental models are suitable in usable security and privacy (USP) and provide examples. In Sect. 3.3, we will conclude this section by outlining how mental models can be elicited in practice.

3.1 Mental Models in Human–Computer Interaction

In the field of HCI, mental models are commonly used to capture the various elements of an individual's awareness and perception of theoretical concepts or the specific information of systems they use [74, 93]. Human beings employ (predominantly simplistic) mental models to grasp complicated processes and systems in their daily lives, rather than spending a lot of time studying them in depth [19]. Nevertheless, irrespective of their accuracy, mental models guide people's decision-making process in both familiar and unfamiliar situations [19, 51]. An end user's mental model is created through interactions with the target system (e.g., the Internet), respectively its system image (e.g., an Internet browser) [71]. Individuals construct mental models of unknown systems by attempting to explain their observations and experiences using analogies from concepts they are familiar with [15]. Thus, the model is affected by an end user's experience and understanding. However, a mental model does not have to be technically correct; it only needs to be practical.

The elicitation of mental models can provide insights into the perceptions and sensations of individuals, which in turn helps to better understand the reasons for and the factors influencing their behavior [19]. If one then tries to elicit an end user's mental model, a conceptualization of this model emerges (i.e., a model of a model). The insights gained from this model can be used to align the target system with the end user's mental model by either supporting them in their understanding or adapting the design of the target system or system image. For example, conceptualized models can be used to design a system in such a way that the cognitive effort required to use it is minimized.

Mental models are generally considered to be vague and highly contextual representations [71]. Based on observations, the use of mental models is subject to the following restrictions [71], which have also been confirmed in related studies [10, 32, 58, 62, 77, 84, 88]: (1) Mental models are incomplete, unstable, and simplified. (2) Mental models have no sharp boundaries. (3) Mental models are "unscientific" and tend to be incorrect. (4) The ability of end users to use mental models is limited. Consequently, there cannot be one unambiguous mental model for a target system; rather—due to subjectivity—several models must always be considered. If the complexity of a target system exceeds the cognitive abilities of a human being, they depend on using a more or less suitable mental model to plan the actions they assume to be "correct" for achieving a goal.

3.2 Mental Models in Usable Security and Privacy

In the field of USP research, mental models are often studied regarding particular tools and technologies (e.g., password managers [12], Wi-Fi [55]), abstract systems

Table 1 Overview of mental model studies in USP

Topic	Context	Stakeholder	Publications
Risk communication	Privacy and security	Computer users	[10, 68]
Smart home	Privacy and security	End users	[103, 104]
Internet use, attacker models, threats, protection strategies	Online privacy and security	Online users, computer users, security experts	[24, 66, 67, 77, 80]
Computer security warnings	Computer security	Lay users vs. experts	[9]
Firewalls	Computer security	Computer users	[78]
Computer security threats	Computer security	Computer users	[54, 96]
Phishing	Online security	Online users	[25]
Influence of mass media	Online security	Online users	[34]
HTTPS, connection security	Online security	Lay users, experts	[33, 56]
Internet	Online security	Lay users, experts	[53]
(End-to-end) Secure communication	Secure communication	Online users	[1, 69, 79, 80]
Encryption mechanisms	Security	Online users	[101]
Passwords and password managers	Security	Online users	[12, 91, 98]
Mobile apps	Mobile privacy	Mobile users	[62]
Online behavioral advertising	Online privacy	Online users	[102]
Internet use and online privacy literacy	Online privacy	Online users, children	[16, 40, 58, 65]
Wi-Fi	Online privacy	Online users	[55]
K-anonymity, anonymous credentials	Privacy-enhancing tech.	Online users	[84, 94]
TOR network	Privacy-enhancing tech.	Lay users vs. experts	[38]
Privacy in employment	Privacy perceptions	Employees	[88]
Folk definitions of privacy	Privacy perceptions	Online users	[60, 72]
Home network maintenance	Technology	Computer users	[76]

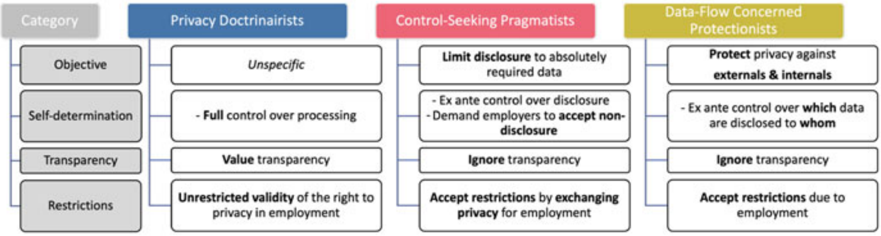
(e.g., the Internet [53], smart home [103, 104]), or other abstract concepts (e.g., privacy perceptions [60, 72, 88]). Table 1 presents a non-exhaustive overview of the body of literature on mental model studies in USP and maps these to the stakeholders they address. Numerous studies have sought to understand how end users—and laypeople in particular—envision networks and communication channels, what entities they assume are involved in them, and what threats they believe these entities pose to security and privacy. For example, lay users tend to underestimate the complexity and multi-layered nature of Internet communication, meaning that the actual (personal) data flow remains obscure to them [38, 53, 67].

At the same time, end users also underestimate the capabilities of secure protocols because their complexity exceeds the end users' knowledge and understanding [1, 56]. From previous studies, it is evident that the nature of security and privacy does not permit a mental model that is universally true. Instead, individuals use highly simplified models [2] and rely on various incomplete and poorly formed sub-models [77]. Because the complexity of information systems is often high, simplified mental models can cause end users to behave in unexpected ways, such as unintentionally disclosing private information [2]. Surveying mental models in USP can help mitigate such effects because they help researchers and developers understand why end users may or may not use certain tools or security and privacy mechanisms. Comprehensive summaries of the contents and applications of mental models in security and privacy can be found in [17, 93]. We can distinguish between three main purposes of using mental models in USP:

Purpose 1: Developing Systems in Which Cognitive Effort Is Optimized for Usability [9, 61, 84, 93] Mental models are frequently used to address the common difficulty in USP in order to ensure that the end users of a system accurately perceive the presented information [5, 9, 11] and to facilitate security- and privacy-preserving behavior [12, 84, 100]. For example, a study on security warnings revealed that novice end users and experienced end users seek out different cues when confronted with a warning and also perform different actions [9]. Likely due to their more limited knowledge and experience, novice end users tend to ignore potential security risks because they, for example, do not understand what "SSL certificate" means or because they believe that "saving" and "opening" a file is equivalent. As a result, novice end users may lower their device's overall security level or run unknown software and just wait to see what happens. So, instead of presenting end users with warnings that require them to engage in manual and complex security checks, better wording and automated security checks are ways to increase both usability and security. Many other mental model studies on information systems and security or privacy mechanisms in use contexts highlight similar issues [12, 56, 69, 104]. However, few researchers have used mental models in the development process to inform the design of metaphors and to ensure that security or privacy information is conveyed as intended [5].

Purpose 2: Effective Communication Between Researchers, Experts, Developers, and Laypeople [56, 78, 94, 96] Studies in USP have repeatedly found that lay users and developers or researchers do not speak the same language; for example, lay users talk about "encryption" but actually refer to concepts related to "authentication" [1, 80]. Also, mental models of actual encryption are limited to concepts of symmetric encryption because asymmetric encryption is beyond laypersons' understanding [101]. In such cases, the laypersons' mental models can serve as a tool or template onto which the knowledge of experts can be mapped, thereby making expert knowledge accessible to non-experts. At the same time, the aspects that laypersons consider to be pivotal to their decision-making can be identified and mapped to experts' mental models [11]. Effective communication may also refer to certain UI designs or support tools. These can be designed to correct misconceptions in laypersons' mental models, thereby facilitating security- and privacy-enhancing decisions [32]. This is especially relevant because people have been found to behave rationally in their decision-making, acting congruently with the framework of their mental models [11]. USP research has also suggested approaches that stimulate "false" mental models of end users, which can still lead to a secure use of tools [95].

Purpose 3: Capturing and Exploring Concerns, Expectations, and Understanding [34, 40, 53, 65, 79, 103] End users' mental models can be used, e.g., to get an overview of the variety of mental models that an information system should support [66, 75]. In particular, mental models can serve as an additional basis for dividing the potential target user group into smaller and more homogeneous subgroups of end users that share certain key characteristics related to privacy or security (see also Sect. 5.1 on user group profiles). In doing so, the designers in an HCD process can decide which subgroups to prioritize or give more attention to based on their mental models, for example, user groups with mental models that lead to potentially undesirable, non-privacy-compliant, or insecure behavior [75]. Figure 2 shows three mental models that were identified in a study on employees' understanding of their right to privacy in employment [88]. Each mental model is characterized by different objectives, desires for self-determination and transparency, and acceptance of restrictions. Naming the different mental models makes them more "tangible" and allows them to be used by researchers or developers when implementing privacy controls to take specific sets of properties into consideration. For example, based on the three models, when employers promote a new information system as privacy-friendly, although all employees expect greater control over their personal information, only "Privacy Doctrinairists" would also expect greater transparency. In contrast, a system that only provides transparency may not even be perceived as privacy-friendly by employees with the other two mental models.



Category	Privacy Doctrinairists	Control-Seeking Pragmatists	Data-Flow Concerned Protectionists
Objective	*Unspecific*	**Limit disclosure** to absolutely required data	**Protect** privacy against **externals & internals**
Self-determination	- **Full** control over processing	- Ex ante control over disclosure - Demand employers to **accept non-disclosure**	- Ex ante control over **which** data are disclosed to **whom**
Transparency	**Value** transparency	**Ignore** transparency	**Ignore** transparency
Restrictions	**Unrestricted validity** of the right to privacy in employment	**Accept restrictions** by **exchanging privacy** for employment	**Accept restrictions** due to employment

Fig. 2 Example mental models of the right to privacy in employment (adapted from [88])

3.3 Mental Model Elicitation

Eliciting mental models involves extracting an individual's internal representation of a target system. Common elicitation techniques can be divided into two categories according to their methodology [73]: (1) *direct methods*, which rely upon a stakeholder's ability to articulate and partially structure their knowledge and train of thoughts, and (2) *indirect methods*, which employ analyses of written or verbal recordings when stakeholders might be unaware of how they perceive the target system. In the latter case, an evaluator interprets the results of previously processed tasks and structures them, e.g., by frequency.

Open-ended semi-structured interviews are a frequently used instrument for eliciting mental models because the stakeholders can express themselves freely while allowing the interviewer to explore relevant aspects in greater depth by asking targeted follow-up questions [93]. Different support methodologies can be used during these interviews, such as card-sorting tasks or verbal and graphical methods. To ensure the mental models are elicited as completely as possible, purely verbal elicitation can be supplemented, e.g., by presenting the interviewees with illustrations depicting typical elements of the contextual topic and asking them to sort these according to relevance, draw them for themselves, or verbally explain and define certain terms [44, 68]. The interviewees can also be asked to solve practical tasks. During all activities, participants should be encouraged to describe their thought process aloud, which allows inferences to be made about their mental model [68].

Some researchers also use a combination of *focus groups* and individual interviews [84]. Focus groups are a special type of workshop that allows a larger number of subjects to be interviewed simultaneously [57]. Moreover, they help to uncover previously unidentified aspects through discussions between the participants when their opinions diverge. However, researchers should be aware that participants may adapt or even withhold their personal opinions due to group dynamics [57]. Other elicitation techniques are based on hypothetical scenarios that put stakeholders in a situation where they must make decisions according to their mental model [9, 25, 84, 95]. For example, participants may role-play a hypothetical end user who has to manage their privacy and security in everyday tasks [25]. All of these methodologies have their respective advantages and limitations [6]. In order to overcome these limitations, it is a common practice to employ two or more elicitation techniques [55, 78, 84].

When eliciting mental models by means of *surveys*, covering all topics of interest poses a challenge. A sound understanding of the target system is usually required. For this purpose, it can be helpful to first model the target system completely and then derive the survey from it. This is also referred to as an *expert model approach* [10, 68]. First, a model of the target system is created, which ideally contains a complete overview of influencing factors and their relationships. The modeling process may include literature reviews and expert involvement. The model may be revised and fine-tuned over several iterations [88]. Subsequently, questions are derived from the created model, which can be used in the context of an interview study, among other things. In this way, each aspect of the previously created model can be examined specifically. Initial conceptualizations of mental models can be based upon these results. The results can then be verified or validated using a survey for which questions are formulated that test the key points of the previously found conceptualizations. To assure that the outcomes have statistical power, measures must be taken to conduct such a survey with a sufficiently large number of participants. If the survey confirms the initial conceptualizations, the mental model can be further tested with experts, for example, through a practical evaluation in which the mental model is tested against several application scenarios.

In most cases, the interviews are analyzed by means of inductive coding. Here, an initial code list can be created either by coding a few transcripts [53, 58] or by using the available literature and expert knowledge of the research group [77]. To make the mental models more tangible, some researchers create word clouds of the codes to identify their relevance by frequency [84]. Other researchers use graphical approaches [16]. For example, they split the interviewees' responses into short phrases and identify connections between two objects within a statement. These are then represented by nodes in a diagram. The relationships between the nodes are visualized by paths, which are also taken from the analyzed statement (action, relationship). If the elicitation is based on an expert model, this can also serve as a code book for deductive coding. If a statement cannot be assigned to a code, the expert model is expanded to include it. During the evaluation, frequently occurring nodes or paths can be highlighted to visualize the frequency of keywords in the expert model. This visualization can furthermore be used to evaluate the accuracy of the statements [68].

4 Usable Security and Privacy Needs

In Sect. 3, we learned how end users think about usable security and privacy (USP) in the context of (software) systems. With this understanding, we can elicit the end-user needs that flow from these perceptions. Because we found that there is no widely used process for integrating USP into the design process of a secure system, we developed an approach based on the human-centered design (HCD) process that proves very helpful. In this section, we present the specific aspects of our approach to inspire design processes in other organizations. Although the focus here is on USP, keep in mind that aspects other than USP also need to be considered that pertain solely to user experience (UX; e.g., usage needs) and security (e.g., risk analysis).

The USP needs play well into the phases of the HCD process (see Sect. 2.1). Regarding *context of use*, stakeholders are assessed in terms of their role regarding personal data, which helps determine whether they have privacy needs and/or data usage needs. When *specifying the user requirements*, these needs are elicited and documented, and other types of requirements can be derived from them through analysis. The needs can be used as principles that guide the activities toward *producing design solutions*. Finally, they play a crucial role in uncovering and negotiating requirements conflicts when *evaluating the design*.

We will begin with an overview of the five types of requirements that are central to this approach (Sect. 4.1). We will then detail the activities for eliciting and analyzing them (Sect. 4.2) and then those for documenting and validating (Sect. 4.3) USP needs. Finally, we will apply them in a real-world example (Sect. 4.4).

4.1 USP Needs as a Requirements Type

In essence, a *user requirement* describes "a need perceived by a stakeholder" [43]. Typically, these needs are aimed at *what* a (software) system should do (functional requirement) and *how well* that system should do this (quality requirement) [42]. The requirements regarding data protection are somewhat different because the end users' concern is not so much with the system, but with what is (potentially) being done with personal data. These *needs* are therefore often more abstract than functional and quality requirements and cannot be translated directly into organizational measures or software properties. In this chapter, we consider a need to be a goal expressed by a data subject or data processor regarding the processing of personal data.

Various models and methods have been developed to transform abstract legal requirements into suitable measures and to evaluate these measures. The Standard Data Protection Model (SDM) [4] by the technology working group of the German Data Protection Conference standardizes the implementation of the GDPR requirements in concrete technical and organizational measures. One approach to defining privacy requirements is to consider "data privacy" a software product quality characteristic—much like "security"—and taking the seven protection goals from the SDM as subcharacteristics [82]. This helps to define and organize security and privacy requirements. To promote USP, the Usable Privacy Cube model [50] considers both objective and perceived usability criteria when evaluating data protection.

Still, documenting privacy aspects in the form of a traditional user requirement might cause them to either be too unspecific (e.g., "The system shall maintain the users' privacy.") or too much in the solution space (e.g., "When the user logs in, the system shall perform the following actions: . . . "), while other notations such as soft goal models do not differentiate between privacy aspects. Something appeared to be missing in between: a different type of need that must be elicited in order to understand what drives the stakeholders. This led us to propose *USP needs*, which we introduce as a novel concept in this chapter: a set of five needs organized into two logical groups as shown in Fig. 3. Each of these needs represents a desire expressed by a stakeholder regarding how personal data are handled [83]. It is paramount to distinguish the stakeholders into the two main user group profiles regarding data

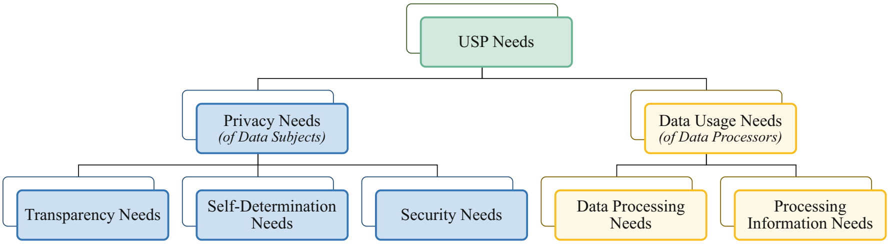


Fig. 3 The five usable security and privacy needs, grouped by type of end user

privacy—data subjects and data processors—because they have divergent needs that, as we will see, might contradict each other.

What sets USP needs apart from typical user requirements is that they are general purpose, i.e., not oriented toward a particular software implementation. They more strongly relate to the legal aspects of personal data. This way, when the needs of both user groups are fulfilled optimally, the effectiveness and the legal compliance of the developed system are inherently maximized, which helps to argue against needs that data protection regulations do not tolerate.

Let us start with *data subjects*. They are concerned with knowing how their data are protected and what their data are being used for, and they want to exert control over (what happens with) their data. This translates into three *privacy needs*:

- **Transparency need:** The data subjects' need or desire for understandable information and openness about the processing of their personal data.
- **Self-determination need:** The data subjects' need or desire for autonomous control over the processing of their personal data.
- **Security need:** The data subjects' desire for their personal data to be protected, particularly with regard to the privacy violations that should be prevented. These will often be phrased negatively, i.e., a need for something *not* to occur.

Data processors, on the other hand, want to use personal data for particular purposes and understand what is allowed. This translates into two *data usage needs*:

- **Data processing need:** The data processors' need to process certain personal data for a specific purpose, including the ability to access such data.
- **Processing information need:** The data processors' need for information about regulations regarding the processing of personal data in order to be legally compliant.

4.2 USP Needs Elicitation and Analysis

In this section, we will describe our recommended approach for embedding the needs into typical requirements engineering (RE) activities, with suggestions on how needs are elicited in workshops and interviews. The elicitation of needs should begin very early in the RE phase; this activity can be initiated as soon as the most important stakeholders have been identified during the initial stakeholder analysis. This is possible because USP needs describe a personal perception or desire that is largely independent of the system being developed. The needs analysis is performed in various stages depending on the status of other requirements artifacts and illustrates the useful contribution of USP needs within the RE activities:

- **Open needs analysis:** The basic needs are determined for the key stakeholders through workshops or interviews. This results in an initial set of basic needs that provide input for deriving user requirements, akin to soft-goal analysis.
- **Scenario-based needs analysis:** Once the project's topic, scope, and goals have crystallized and high-level scenarios have been formulated, the second type of needs analysis can be performed. This analysis associates basic needs with scenarios, while further needs are uncovered as the domain is understood better. In workshops and interviews, scenarios can be used to trigger the stakeholders to express previously uncovered needs. As this activity aims to enrich the understanding of a scenario with the needs that apply to it, scenarios do not have to be associated with all the needs nor vice versa.
- **Detailed needs analysis:** When the to-be (process) situation has been described and use cases have been formulated, it becomes possible to triangulate the use cases with the user requirements and needs associated with them. This ensures that the stakeholders' privacy-related needs have been considered and that the system will deliberately promote, ignore, or actively prevent these needs from getting fulfilled. At this stage, workshops and interviews are usually no longer performed; this is only recommended if the analysis reveals gaps in the elicitation.

The first two analyses, in particular, require active participation of the stakeholders. We recommend eliciting the needs through workshops, but if the project context demands it, semi-structured interviews can also be used. Below, we provide a general-purpose template for both elicitation techniques, which can be tailored to specific project contexts (e.g., a company for which a privacy solution is being designed, the analysis of a particular website, or the definition of a process in which personal data are processed). We also suggest holding at least two different workshops: one with stakeholders who are primarily data subjects to elicit their privacy needs and one with stakeholders who are predominantly data processors to elicit their data usage needs.

The *workshop for data subjects* should be held with at least six participants so that at least two groups can be formed. Ideally, a much larger workshop with a diverse sample of stakeholders is best, but with more than fifteen participants, the workshop becomes harder to manage. Moderation cards should be prepared in three colors, such as yellow, green, and blue. To write down their needs, the participants should use the following template, which is derived from user stories [14]: *"As a <data subject>, I would like* <**need**>, *so that* <rationale>"—see Sect. 4.3 for several examples. The workshop can be structured as follows:

- Form groups of three.
- Each person in the group selects one data class that is likely to contain personal data about them.
- For each data class, the group repeats the following steps:
  - Discuss what a company, individuals, or third parties do with this data class, and for what purpose. Optionally: describe typical security problems with protecting this data class.
  - As a data subject, which needs do you have (accordingly) regarding the protection of this data? Write each need on a yellow card using the sentence template. (This question elicits security needs.)
  - As a data subject, what would you like to know regarding the collection, processing, or use of this data? Write each need on a green card using the sentence template. (This question elicits transparency needs.)
  - As a data subject, what need do you have regarding self-determination? Write each need on a blue card using the sentence template. (This question elicits self-determination needs.)
- Each person in the group picks one data protection, transparency, and self-determination need that they find most important. If another person in the group already picked their most important need, they should choose their second most important one. It is also possible for the workshop organizers to use a prioritization technique (e.g., “buy-a-feature” [41]).
- Discuss as a group what use cases/overall features of a system should be available to fulfill the selected needs.

The *workshop for data processors* can be performed with fewer participants than the workshop with data subjects because this is a smaller stakeholder group whose goals are more homogeneous. Six or nine participants will therefore suffice. Prepare moderation cards in two colors, such as purple and orange. Their needs are also documented as a user story, but using this template instead: *“As a <data processor>, I would like* <**need**>, *so that* <rationale>.” The workshop can be structured as follows:

- Form groups of three.
- Each person in the group selects one class of personal data that they are likely to process.
- For each data class, the group repeats the following steps:
  - Discuss what you, your company, other individuals, or third parties do with this data class, and for what purpose. Optionally: describe typical problems regarding the processing of this data class.
  - As a data processor, which needs do you have (accordingly) regarding the processing of this data? Write each need on a purple card using the sentence template. (This question elicits data processing needs.)
  - As a data processor, what would you like to know regarding the collection, processing, or use of these data? Write each need on an orange card using the sentence template. (This question elicits processing information needs.)

- Each person in the group picks one data processing need and one processing information need that they find most important. If another person in the group already picked their most important need, they should choose their second most important one.
- Discuss as a group what use cases/overall features of a system should be available to fulfill the selected needs.

In case the above two workshops cannot be organized, or whenever there are key stakeholders who cannot participate in the workshops, we recommend including the following questions in an *elicitation interview* with the stakeholders:

1. Which of your personal data do you consider worth protecting in the context of the system under development?
2. What (potential) problems do you see in protecting your privacy?
3. In what way should a tool that allows you to set and monitor your privacy settings improve the protection of your privacy? (This question implicitly probes for self-determination needs.)
4. For a specific data category: Which actor or role has or should have access to these data, and what do they use it for?
5. Which need do you have regarding the protection (or, for data processors: processing) of these data? (This question elicits security or data processing needs.)
6. What would you want to know regarding the collection, processing, or use of these data? (This question elicits transparency or processing information needs.)
7. Which of each discussed need is most important to you, and why?

4.3 USP Needs Documentation and Validation

When needs have been elicited during the open or scenario-based needs analysis, they should be documented accordingly. In addition to guidelines on how to document them, in this section, we present a procedure for validating the needs by examining their legal basis.

Typically, documenting the needs begins with typing up the needs from the workshop's moderation cards. We recommend including every elicited need from the workshops or interviews, but differentiating between the needs that the participants identified as important as opposed to those they did not, for example, by prioritizing them according to the MoSCoW method into must-, should-, could-, and will-not-have needs [13]. At this stage, it is important to assure the quality of the contents by checking for wrongly attributed needs (written on the wrong color card) and verifying that the expressed need and the rationale make sense and are self-explanatory. The need should also be given a name, which can often be derived

Table 2 Examples of a security need and a data processing need, adapted from [89]

Attribute	Content
Name	**Business email communication**
Description	As a *social partner*, I would like *my email communication to not be disclosed to others*, so that *I can protect both the content and my contacts*.
Priority	Nice-to-have
Name	**View email contents of employees**
Description	As an *employer*, I would like *to be able to view the email content of my employees*, so that *I can detect misconduct in internal or external communication*.
Priority	Should-have

quite simply from the keywords in the *need* section of the template. Table 2 shows examples of a documented security need and a data processing need.[2]

The key difference in validating needs compared to typical requirements is that instead of verifying with the stakeholders that the documented needs are correct,[3] they are instead analyzed for their legal merit based on applicable regulations, legislature, and case law. The resulting *legal interpretations* form an important basis for assessing to what degree a particular need can be met in the intended context: Should it be allowed, limited, or forbidden? We recommend storing the legal interpretations as separate entities that are subsequently linked to one or more needs. For example, in the German-language documentation of the TrUSD project [89], the needs shown in Table 2 are linked to the two legal interpretations "Processing for purposes of the employment relationship" and "Processing of business emails/determination of private email use," while the data processing need is additionally linked to the legal interpretation "Communication control." These descriptions explain that the processing is permissible pursuant to the German Federal Data Protection Act (BDSG) under specific conditions (e.g., that business and private emails are clearly separated) and for specific purposes detailed in the BDSG and the GDPR.

There is a constant tension between whether limiting one's personal privacy is justified for a specific processing purpose. The use of personal data to optimize work processes often sparks concerns regarding monitoring and performance evaluation,

[2] In chapters 4–8 in [89], we provide a catalog of 139 USP needs for organizational settings in German. It provides 46 transparency needs, 11 self-determination needs, 38 security needs, 39 data processing needs, and 5 processing information needs.

[3] Needs are subjective and do not describe an implementable aspect of a system, so there is no real need to validate them with stakeholders.

which shows that especially *data processing needs* and *security needs* may clash.[4] A key activity within RE is to analyze requirements during the requirements validation phase in order to identify conflicting requirements that need to be reconciled. This is important because failing to identify such conflicts might lead to an implemented system that does not satisfy the needs of at least one stakeholder. By specifying these needs, requirements reconciliation can be performed, and the decisions made to address conflicting needs are made explicit. In many cases, this will involve communicating the legal interpretation to the stakeholders involved (e.g., that privacy legislation does not permit a need to be fulfilled, or that higher value is assigned to a different need). The best solution approach depends on the context. For example, if potentially many data subjects have a concern, the explanation of why the system helps fulfill a particular data processing need could take the form of an information campaign explaining the necessity and benefits of processing the data and what security measures are being taken. Similarly, if a project reveals there is a great demand for transparency, this can be met through the development of solutions such as privacy dashboards in organizations [90] or privacy cockpits in digital ecosystems [22].

4.4 Example Case Study

In 2021, the regional public broadcaster *L1* of the Dutch province of Limburg got international media coverage due to a serious privacy-related incident. A quickly escalating dispute caused their newly appointed director to be suspended after nine months; a court ruling particularly blamed a disorganized works council.[5] Problems had arisen even before the director took up his post, with staff disputing the Supervisory Board's appointment procedure.[6] Dissatisfaction over his communication and leadership style caused employees to respond in a way the director described as a guerilla war waged against him.[7] But things really culminated when he presented a draft of the new privacy regulations that would infringe on the workers' privacy through the use of hidden cameras in the office, and—if there were compelling reasons—access to browsing histories and email accounts, including

[4] For example, an employee may not wish for their employer to know that they are ill (security need), but an employer has the right to know this. However, the employer may only use this knowledge for specific purposes such as resource planning and aggregated analyses (data processing needs). Using this information to send a collective get-well card is only allowed with the data subject's consent, and individual assessments based on this information are strictly prohibited.

[5] https://amp.nos.nl/artikel/2387272-bestuurder-peter-elbers-van-regionale-omroep-l1-op-non-actief.htm.

[6] https://www.limburger.nl/cnt/dmf20200922_00176921.

[7] https://www.limburger.nl/cnt/dmf20201105_93947605.

those of journalists, the company physician, and members of the works council.[8] The director had the sole power to determine what he considered compelling, and he would also be responsible for handling any complaints. The outrage among staff, Dutch journalists and lawyers, and in society as a whole resulted in the draft being retracted just three days later.

This case study shows that the director had several *data processing needs*, such as "View email contents of employees" (shown in Table 2) and "View browsing history of employees" for the purpose of assessing individual employees. Typically, professional correspondence may be reviewed if it is clearly distinct from private communications, but this assessment should then be performed by a superior, not by the director. This specific situation, however, uncovers a domain-specific type of *processing information need*: "Privacy rights of journalists." The fundamental principle that safeguards freedom of the press limits the ability to put journalists under surveillance to ensure that they can exert their duty of protecting their sources.[9] The director should have been aware that this kind of data processing contradicts the special rights of journalists that safeguard the *security needs* of "Business email communication" (shown in Table 2) and "Protect the identity of news sources from others" (including their employer), to which they are legally and ethically entitled. This demonstrates that these kinds of needs are not general purpose; while work emails may normally be monitored under certain conditions, these particular *security needs* are prioritized as "must-have" for journalists.

The director also had the *data processing need* "Video surveillance of employee activities." Under strict conditions, data protection legislation allows video surveillance for specific purposes (e.g., preventing illegal activities or industry espionage; improving work floor safety). However, monitoring employee activities in non-public spaces using CCTV cameras is only allowed if it is the mildest and most suitable measure, and should in that case be openly announced instead of through the use of hidden cameras. For the same reasons as above, this conflicts with and is overruled by journalists' *security needs*.

5 User Group Profiles and Privacy Personas

Section 4 described what needs the end users of a software system have with regard to usable security and privacy (USP). But who are these end users, and how can we typify them? The ISO 9241-210 standard [49] names two artifacts for describing user characteristics: user group profiles and personas. Although they are introduced as part of the *context of use*, they can also be used in other activities of the human-centered design (HCD) process, for example to specify the usage requirements of specific groups. These artifacts can accompany the development

[8] https://www.volkskrant.nl/cultuur-media/directeur-limburgse-omroep-11-wil-eigen-personeel-kunnen-volgen-met-camera-s~bba48bd7/.

[9] In this context, *sources* are professional contacts who provide journalists with newsworthy information.

team throughout the development process up to the evaluation, which can be carried out as a walkthrough from the perspective of a specific persona. We will discuss the concept of user group profiles in Sect. 5.1 and that of (privacy) personas in Sect. 5.2.

User characteristics strongly influence the context in which a system is used. It is therefore useful to gather and analyze relevant information about them in order to understand the current context and to specify the context for the future system. User group profiles summarize typical characteristics of end users, while personas are concrete examples of typical end users [86]. As examples of the characteristics of different user types, ISO 9241-210 cites end users with different levels of experience or physical capability.

5.1 User Group Profiles

Concerning data protection, the most essential user group profiles are the two main types of end users distinguished in the GDPR [27]: *data subjects*, whose personal data are processed, and *data processors*, who process personal data. Section 4.1 demonstrates one practical use of these profiles.

The consumer study “DsiN-Sicherheitsindex 2022” [63] distinguishes five different groups of end users of Internet services by their knowledge and behavior and provides suggestions on how to address security deficits for each (percentages according to DsiN):

1. **Fatalistic users** (17.7%) see dangers lurking everywhere but question the effectiveness of security measures. They often do not realize that their own behavior is an important component in the security concept.
2. **Outsiders** (5.3%) often feel overwhelmed by new digital offers but consider themselves to be primarily responsible for protecting their personal data.
3. **Thoughtless users** (37.1%) have a very high level of security knowledge but apply it too rarely. They are the least concerned about being at risk and have little interest in risk reduction measures.
4. **Driving users** (22.2%) are open to new things and try out more new digital services and offers than other end users. Due to their open-mindedness and curiosity, they are particularly suitable as multipliers to raise awareness.
5. **Considerate users** (17.8%) have the highest security knowledge and are also forerunners in the implementation processes. They are the most cautious and privacy-aware users when it comes to new digital offerings.

A similar approach is taken by Dupree et al. [97]. They divide end users of privacy and security tools into five categories according to their attitudes, beliefs, and behaviors: *marginally aware*, *fundamentalist*, *struggling amateur*, *technician*, and *lazy expert*. Some of these categories are compatible with the DsiN classification; for example, the lazy expert resembles the thoughtless users. Based on the rather abstract user group profiles, Dupree et al. also created personas (see Sect. 5.2) that cover the user space of privacy and security tools (e.g., “Henry—

The Lazy Expert"). With respect to end users' attitude and motivation toward giving feedback, Groen et al. [45] identified seven categories: *privacy-tolerant and socially ostentatious*, *privacy-fanatical but generous*, *passive and stingy*, *loyal & passionate*, *incentive seekers*, *perfectionists & complainers*, and *impact seekers*. Due to cultural differences, corresponding categorizations often only apply to the inhabitants of the country examined. For example, in a recent study, 65% of the participants in Cyprus were open to sharing their facial images with public administration for identity purposes, compared to 9% of the participants in Germany, Poland, and Romania [28]. For user group profiles that describe end users according to their use of particular security measures, it must be noted that corresponding security measures often become outdated after a few years, which may cause these user classifications to also become outdated over time.

User group profiles are a helpful means of painting a much more accurate picture of the key stakeholders that directly interact with the system. For example, the stakeholder group of *end users* can correspond to the five DsiN groups. By categorizing them accordingly, it is possible to analyze and document the needs and requirements of this stakeholder group in a much more differentiated way.

5.2 Privacy Personas

Personas are fictitious individuals representing typical user groups as archetypes [18]. Creating personas is not the same as defining user groups or creating user group profiles. Personas are descriptions of stereotypical individual end users that are derived from the identified user groups in order to emphasize the most important characteristics and details of the respective user group [47]. Usually, as many personas are created as are needed to cover all relevant user groups [64].

The intention behind creating personas is to get a more vivid description of the end users than with the more abstract user group profiles. The basis for the creation of personas can be quantitative or qualitative data collections, online surveys, interviews, or participatory observations of potential end users. Personas for the USP domain, or *privacy personas*, should emphasize the different ways in which personal data are handled and the different security needs of end users, among other things. Importantly, no discriminatory aspects should be highlighted nor associations made with real people [48]. Cooper, Reimann and Cronin [18] recommend that after the research with end users is complete, the distinct aspects of user behavior be listed as a set of behavioral variables. While demographic variables such as age or geographic location influence behavior, behavioral variables are much more useful in developing effective personas. The most important variables for distinguishing behavioral patterns according to Cooper et al. are *activities*, *attitudes*, *aptitudes* (e.g., education, training), *motivations*, and *skills* (related to the product domain and technology). In enterprise applications, behavioral variables are often closely related to job roles. Therefore, they recommend listing the variables separately for each role, i.e., creating a separate persona for each role.

Table 3 Example description of a privacy persona [89]

Attribute	Content
Name	**Ian Frederick** (sales employee)
Who am I?	37 years, male, single
Attitude toward digital work	Ian is aware of the importance of data protection in digitized work processes, especially as he handles customer data in sales work
Reasons for using the system	To see which consents have been given to the employer
Reasons for not using the system	Complicated handling; missing help options
Personality classification	Ian is extroverted, partly analytical and partly creative, neither particularly chaotic nor organized, is team-oriented, and has partial freedom in terms of time
Interests, motives, and goals	Well-established, simple processes for all sales and marketing activities; fast, centralized access to all required data
Problems and challenges	Both customer data and employee data must be kept up-to-date; this only works if all colleagues play their part
Personal environment and self-perception	Ian is appreciated by all colleagues as a team player and finds very good ways to approach different customer personalities
Typical working day	Everyday exposure to technology in the work environment, both as an end user (e.g., CRM and ERP system) and in sales (product demonstrations) for data protection
Qualifications and skills	IT specialist; Ian is involved in many of the company's projects

Personas can be used by a system's design and development team to imagine themselves in the role of current and future end users and better emphasize with them. This enables them to better understand their needs and play through different usage scenarios from the end users' point of view. By understanding the way the end user thinks and acts, it is easier to make the right design decisions—in overall product development, but also during the design of security features and data protection mechanisms to ensure they become as user-friendly as possible for specific user groups [64].

Various projects in the area of USP [22, 90] have developed templates and examples that support the creation of personas. Templates make it possible to evaluate research data and summarize the collected findings in a structured and clear way so that they can be referred to in the further course of development. Table 3 shows one of eight personas developed for a privacy dashboard that caters to the goals and needs of employees. Figure 4 shows a persona template for representing different user groups of digital ecosystems used to design and develop privacy cockpits. In both examples, some variables of "conventional" templates were adapted or further specified in order to collect and analyze USP needs in a structured way.

In addition to persona templates, workshop concepts for supporting the creation of personas have been proposed. Workshops for creating personas are particularly

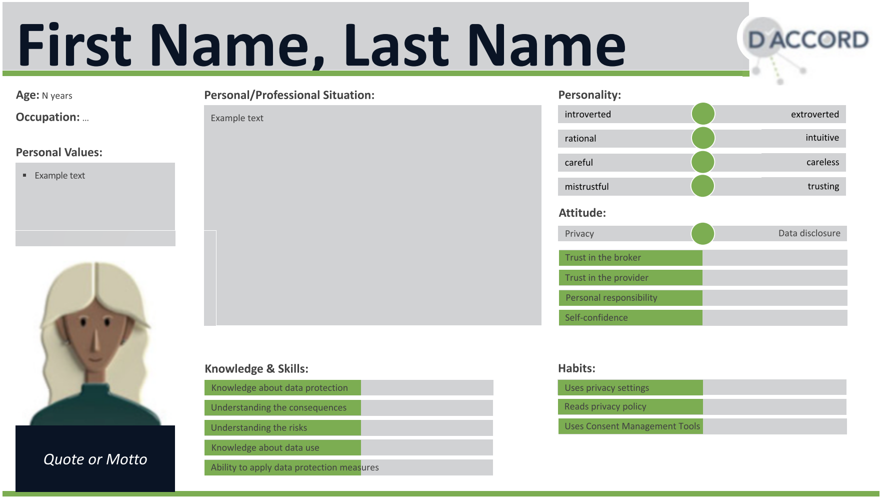


Fig. 4 Persona template for end users of digital ecosystems

useful if no comprehensive research material is available. For example, a workshop concept for elaborating personas in companies or organizations was developed that involves around 18 participants (including the moderator) and has a duration of two hours [48]. This workshop's schedule is as follows:

- Welcome and round of introductions.
- Presentation of the method.
- Formation of small groups.
- Each group works out an organization-specific persona using the persona template (e.g., on a Metaplan wall).
- Each group presents its persona in a group discussion.
- Summarization of the results in a feedback round.

6 Summary and Conclusion

In this chapter, we presented three methods regarding the interface between *human-centered design* (HCD) and *usable security and privacy* (USP): (1) mental models in security and privacy, (2) USP needs, and (3) stakeholder descriptions using user group profiles and privacy personas. These methods are complimentary in that they elicit or collect different types of information, with their own documentation formats and contributions to the design of a digital system.

The methods can play a constructive role throughout the HCD process. They can all be used to specify and understand the stakeholders' *characteristics* regarding USP: Mental models enable this by conceptually exploring their subjective perception and assumptions (implicit expectations); USP needs by inventorying their desires and requirements (explicit expectations), and profiles/personas by organizing them into logical groups. In other process steps, *goals and tasks* can be identified from the USP needs and included in the persona descriptions. Through analysis, *user requirements* can be derived from analyzing the USP needs. For the *design solutions*, mental models can inform patterns on end users' preconceptions, while USP needs provide possible principles. Finally, all methods help to *evaluate the design*: in terms of how well the system plays into the mental models, in terms of assuring that the USP needs are being fulfilled or overruled by other USP needs and comply with legal standards, and in terms of considering the usage scenarios of the system from the perspective of each persona.

Together, the three methods augment the HCD process with practical approaches to analyzing and assuring that USP is correctly implemented in a system by ensuring that the stakeholders are known, understood, and validated in the system's design. The additional work involved in applying these methods is manageable and can be justified by their contribution of employing good requirements engineering (RE) and user experience (UX) design practices, with which they integrate perfectly in our experience. Their use makes a positive contribution to a system's overall quality, not only in terms of constraints (e.g., improved assurance of compliance with data protection regulations), but also in terms of system quality (e.g., because security aspects have been analyzed in more depth) and quality in use (e.g., greater trust in the system). Specifically, we argue that these techniques will help the system to better achieve two core principles stipulated in Article 25 of the GDPR: (1) *Data Protection by Design* or *Security by Design*, which postulates the consideration of technical and organizational measures in the system design and development from the very beginning to ensure the best possible privacy and security as well as smooth human–machine interaction, and (2) *Data Protection by Default* or *Security by Default*, which postulates that the privacy and security of a system should not rely on end users making good settings, but rather that the default settings should already be as user-friendly, privacy-promoting, and secure as possible.

By presenting these methods, we hope to support the reader with practical knowledge and skills to help them achieve better USP in their systems. We do not claim that these are the only USP-related techniques that can be used in the HCD process, but in our context, we found these methods to be sufficient supplements to the tried and tested RE and UX techniques for achieving our goals. We do encourage the reader to try these approaches for themselves.

Acknowledgments This work is funded by the German Federal Ministry of Education and Research (BMBF) (grant numbers 16KIS1506K, 16KIS1507, and 16KIS1508). We thank Sonnhild Namingha for proofreading this chapter and Jannis von Albedyll for providing insightful comments.

References

1. Abu-Salma, R., Sasse, M. A., Bonneau, J., Danilova, A., Naiakshina, A., & Smith, M. (2017). Obstacles to the adoption of secure communication tools. In *Proc. of IEEE Symposium on Security and Privacy (SP)* (pp. 137–153). IEEE.
2. Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security & Privacy, 3*(1), 26–33.
3. Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40–46.
4. AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder. (2020). The standard data protection model. Technical report, UAG Standard Data Protection Model of the AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder.
5. Angulo, J., Fischer-Hübner, S., Pulls, T., & Wästlund, E. (2015). Usable transparency with the data track: A tool for visualizing data disclosures. In *Proc. of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems (CHI EA)* (pp. 1803–1808). ACM Press.
6. Asgharpour, F., Liu, D., & Camp, L. J. (2007). Mental models of security risks. In S. Dietrich, & R. Dhamija (Eds.), *Financial cryptography and data security*. Lecture notes in computer science (pp. 367–377). Springer.
7. Balfanz, D., Durfee, G., Smetters, D. K., & Grinter, R. E. (2004). In search of usable security: Five lessons from the field. *IEEE Security & Privacy, 2*(5), 19–24.
8. Blythe, J., Koppel, R., & Smith, S. W. (2013). Circumvention of security: Good users do bad things. *IEEE Security & Privacy, 11*(5), 80–83.
9. Bravo-Lillo, C., Cranor, L. F., Downs, J., & Komanduri, S. (2011). Bridging the gap in computer security warnings: A mental model approach. *IEEE Security & Privacy Magazine, 9*(2), 18–26.
10. Camp, L. J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine, 28*(3), 37–46.
11. Cassaigne, N. (2002). The dashboard: A knowledge conversion tool. In *IEEE International Engineering Management Conference* (Vol. 1, pp. 292–297). IEEE.
12. Chiasson, S., van Oorschot, P. C., & Biddle, R. (2006). A usability study and critique of two password managers. In *Proc. of the 15th Conference on USENIX Security Symposium* (pp. 1–16). USENIX Association.
13. Clegg, D., & Barker, R. (1994). *Case method fast-track: A RAD approach*. Addison-Wesley.
14. Cohn, M. (2004). *User stories applied: For agile software development*. Addison-Wesley Longman Publishing.
15. Collins, A., & Gentner, D. (1987). How people construct mental models. In *Cultural models in language and thought* (pp. 243–265). Cambridge University Press.
16. Coopamootoo, K. P., & Groß, T. (2014). Mental models of online privacy: Structural properties with cognitive maps. In *Proc. of the 28th International BCS Human Computer Interaction Conference (BCS-HCI)*, BCS-HCI '14 (pp. 287–292). BCS.
17. Coopamootoo, K. P. L., & Groß, T. (2014). Mental models for usable privacy: A position paper. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, A. Kobsa, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, D. Terzopoulos, D. Tygar, G. Weikum, T. Tryfonas, & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust* (Vol. 8533, pp. 410–421). Springer International Publishing.
18. Cooper, A., Reimann, R., & Cronin, D. (2012). *About Face 3: The essentials of interaction design*. Wiley.
19. Craik, K. J. W. (1943). *The nature of explanation*. University Press, Macmillan.
20. Cranor, L. F., & Garfinkel, S. (2004). Guest editors' introduction: Secure or usable? *IEEE Security & Privacy, 2*(5), 16–18.

21. Cranor, L. F., & Garfinkel, S. (2005). *Security and usability: Designing secure systems that people can use*. O'Reilly Media.
22. D'accord-Konsortium. (2022). D'accord—Adaptive Datenschutz-Cockpits in digitalen Ökosystemen (2022). https://daccord-projekt.de/
23. DeWitt, A. J., & Kuljis, J. (2006). Aligning usability and security: A usability study of Polaris. In *Proc. of the 2nd Symposium on Usable Privacy and Security* (pp. 1–7). ACM.
24. Dourish, P., de la Flor, J. D., & Joseph, M. (2003). Security as a practical problem: Some preliminary observations of everyday mental models. In *Proc. of CHI 2003 Workshop on HCI and Security Systems* (p. 3). ACM.
25. Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2006). Decision strategies and susceptibility to phishing. In *Proc. of the 2nd Symposium on Usable Privacy and Security*, SOUPS '06 (pp. 79–90). ACM.
26. Emami-Naeini, P., Francisco, T., Kohno, T., & Roesner, F. (2021). Understanding privacy attitudes and concerns towards remote communications during the COVID-19 pandemic. In *Proc. of the 17th Symposium on Usable Privacy and Security,* SOUPS'21 (pp. 695–714). USENIX Association.
27. European Union. (2016). General Data Protection Regulation. (2016). https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04. Regulation (EU) 2016/679.
28. European Union Agency for Fundamental Rights. (2020). *Your rights matter: Data protection and privacy: Fundamental rights survey*. Publications Office of the European Union.
29. Feth, D., & Polst, S. (2022). Benutzerfreundliche Umsetzung von Datensouveränität in Digitalen Ökosystemen. Whitepaper, Fraunhofer IESE.
30. Feth, D., Maier, A., & Polst, S. (2017). A user-centered model for usable security and privacy. In T. Tryfonas (Ed.), *Human aspects of information security, privacy and trust* (pp. 74–89). Springer.
31. Fischer-Hübner, S., Grimm, R., Lo Iacono, L., Möller, S., Müller, G., & Volkamer, M. (2011). Gebrauchstaugliche Informationssicherheit. *Die Zeitschrift für Informationssicherheit Jg, 4*, 14–19.
32. Fischer-Hübner, S., Pettersson, J. S., & Angulo, J. (2015). HCI requirements for transparency and accountability tools for cloud service chains. In M. Felici & C. Fernández-Gago (Eds.), *Accountability and security in the cloud: First summer school, cloud accountability project, A4Cloud, Malaga, Spain, June 2–6, 2014, Revised Selected Papers and Lectures* (pp. 81–113). Springer.
33. Friedman, B., Hurley, D., Howe, D. C., Felten, E., & Nissenbaum, H. (2002). Users' conceptions of web security: A comparative study. In *CHI '02 Extended Abstracts on Human Factors in Computing Systems*, CHI EA '02 (pp. 746–747). ACM.
34. Fulton, K. R., Gelles, R., McKay, A., Roberts, R., Abdi, Y., & Mazurek, M. L. (2019). The effect of entertainment media on mental models of computer security. In *Proc. of the 15th USENIX Conference on Usable Privacy and Security*, SOUPS'19 (pp. 79–95). USENIX Association.
35. Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security, 25*(1), 27–35.
36. Furnell, S. (2005). Why users cannot use security. *Computers & Security, 24*(4), 274–279.
37. Furnell, S. (2007). Making security usable: Are things improving? *Computers & Security, 26*(6), 434–443.
38. Gallagher, K., Patil, S., & Memon, N. (2017). New me: Understanding expert and non-expert perceptions and usage of the Tor anonymity network. In *Proc. of the 13th USENIX Conference on Usable Privacy and Security*, SOUPS '17 (pp. 385–398). USENIX Association.
39. Garfinkel, S., & Lipford, H. R. (2014). Usable security: History, themes, and challenges. *Synthesis Lectures on Information Security, Privacy, and Trust, 5*(2), 1–124.
40. Gerber, N., Zimmermann, V., & Volkamer, M. (2019). Why Johnny fails to protect his privacy. In *2019 European Symposium on Security and Privacy Workshops (EuroS PW)* (pp. 109–118). IEEE.

41. Gkatzidou, V., Giacomin, J., & Skrypchuk, L. (2021). *Automotive human centred design methods*. De Gruyter.
42. Glinz, M. (2007). On non-functional requirements. In *Proc. of the 15th IEEE International Requirements Engineering Conference,* RE'07 (pp. 21–26). IEEE.
43. Glinz, M. (2017). A glossary of requirements engineering terminology. https://www.ireb.org/en/cpre/cpre-glossary/
44. Grenier, R. S., & Dudzinska-Przesmitzki, D. (2015). A conceptual model for eliciting mental models using a composite methodology. *Human Resource Development Review, 14*(2), 163–184.
45. Groen, E. C., Seyff, N., Ali, R., Dalpiaz, F., Doerr, J., Guzmán, E., Hosseini, M., Marco, J., Oriol, M., Perini, A., & Stade, M. (2017). The crowd in requirements engineering: The landscape and challenges. *IEEE Software, 34*(2), 44–52.
46. Gutmann, P., & Grigg, I. (2005). Security usability. *IEEE Security & Privacy, 3*(4), 56–58.
47. Harley, A. (2015). Personas make users memorable for product team members. https://www.nngroup.com/articles/persona/
48. Institut für Technologie und Arbeit (ITA). (2021). Entwicklung eines Privacy Dashboard-Modellierungsrahmenwerks: D2.3 Dokumentation des Vorgehensmodells. Version 6. https://www.trusd-projekt.de/wp/wp-content/uploads/2022/06/TrUSD-D2.3-Partizipatives-Vorgehensmodell.pdf
49. ISO. (2019). *Ergonomics of human-system interaction—part 210: Human-centred design for interactive systems*. Standard.
50. Johansen, J., & Fischer-Hübner, S. (2020). Making GDPR usable: A model to support usability evaluations of privacy. In M. Friedewald, M. Önen, E. Lievens, S. Krenn, & S. Fricker (Eds.), *Privacy and identity management. Data for better living: AI and privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2.2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers* (pp. 275–291). Springer International Publishing.
51. Johnson-Laird, P. N. (1986). *Mental models: Towards a cognitive science of language, inference, and consciousness*. Cognitive Science Series. Harvard University Press.
52. Jones, N., Ross, H., Lynam, T., Perez, P., & Leitch, A. (2011). Mental models: An interdisciplinary synthesis of theory and methods. *Ecology and Society, 16*(1), article 46.
53. Kang, R., Dabbish, L., Fruchter, N., & Kiesler, S. (2015). "My data just goes everywhere:" User mental models of the Internet and implications for privacy and security. In *Proc. of the 11th Symposium on Usable Privacy and Security*, SOUPS'15 (pp. 39–52). USENIX Association.
54. Kauer, M., Günther, S., Storck, D., & Volkamer, M. (2013). A comparison of American and German folk models of home computer security. In L. Marinos & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust*. Lecture Notes in Computer Science 8030 (pp. 100–109). Springer.
55. Klasnja, P., Consolvo, S., Jung, J., Greenstein, B. M., LeGrand, L., Powledge, P., & Wetherall, D. (2009). "When I am on Wi-Fi, I am fearless": Privacy concerns & practices in everyday Wi-Fi use. In *Proc. of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '09 (pp. 1993–2002). ACM.
56. Krombholz, K., Busse, K., Pfeffer, K., Smith, M., & von Zezschwitz, E. (2019). "If HTTPS were secure, I wouldn't need 2FA" - end user and administrator mental models of TTPS. In *Proc. of the 2019 Symposium on Security and Privacy (SP)* (pp. 246–263). IEEE.
57. Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). SAGE.
58. Kumar, P., Naik, S. M., Devkar, U. R., Chetty, M., Clegg, T. L., & Vitak, J. (2017). 'No telling passcodes out because they're private': Understanding children's mental models of privacy and security online. In *Proc. of the ACM on Human-Computer Interaction, 1*(CSCW), 64:1–64:21.
59. Kumar, D., Kelley, P. G., Consolvo, S., Mason, J., Bursztein, E., Durumeric, Z., Thomas, K., & Bailey, M. (2021). Designing toxic content classification for a diversity of perspectives.

In *Proc. of the 17th Symposium on Usable Privacy and Security*, SOUPS'21 (pp. 299–318). USENIX Association.

60. Kwasny, M., Caine, K., Rogers, W. A., & Fisk, A. D. (2008). Privacy and technology: Folk definitions and perspectives. In *Extended abstracts on human factors in computing systems*, CHI EA '08 (pp. 3291–3296). ACM.
61. Lederer, S., Hong, J. I., Dey, A. K., & Landay, J. A. (2004). Personal privacy through understanding and action: Five pitfalls for designers. *Personal and Ubiquitous Computing, 8*(6), 440–454.
62. Lin, J., Sadeh, N., Amini, S., Lindqvist, J., Hong, J. I., & Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proc. of the 2012 ACM Conference on Ubiquitous Computing (UbiComp)* (pp. 501–510). ACM Press.
63. Littger, M. (2022). Studie von Deutschland sicher im Netz e.V. zur digitalen Sicherheitslage von Verbraucher:innen in Deutschland. https://www.sicher-im-netz.de/dsin-sicherheitsindex-2022
64. Lo Iacono, L., Schmitt, H., Feth, D., Jakobi, T., Gorski, P. L., Dölle, M., Nehren, P., Kropp, E., Hausmann, S., Hofmeister, A., Frydyada de Piotrowski, A., & Balthasar, M. (2019). Arbeitskreis Usable Security & Privacy: Nutzerzentrierter Schutz sensibler Daten. Fachschrift. 3., aktualisierte Ausgabe. Technical report, German UPA e.V.
65. Maceli, M. (2019). Librarians' mental models and use of privacy-protection technologies. *Journal of Intellectual Freedom & Privacy, 4*(1), 18–32.
66. Maier, J., Padmos, A., S. Bargh, M., & Wörndl, W. (2017). Influence of mental models on the design of cyber security dashboards. In *Proc. of the 12th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications* (pp. 128–139). SCITEPRESS - Science and Technology Publications.
67. Mbewe, E. S., & Chavula, J. (2022). Security mental models and personal security practices of Internet users in Africa. In Y. H. Sheikh, I. A. Rai, & A. D. Bakar (Eds.), *E-infrastructure and e-services for developing countries*. Lecture Notes of the Institute for Computer Sciences. Social Informatics and Telecommunications Engineering (pp. 47–68). Springer International Publishing.
68. Morgan, M. G., Fischhoff, B., Bostrom, A., & Atman, C. J. (Eds.) (2002). *Risk communication: A mental models approach*. Cambridge University Press.
69. Naiakshina, A., Danilova, A., Dechand, S., Krol, K., Sasse, M. A., & Smith, M. (2016). Poster: Mental models – User understanding of messaging and encryption. In *Proc. of the 1st IEEE European Symposium on Security and Privacy* (article 18). IEEE.
70. Napoli, D., Baig, K., Maqsood, S., & Chiasson, S. (2021). "I'm literally just hoping this will work:" Obstacles blocking the online security and privacy of users with visual disabilities. In *Proc. of the 17th Symposium on Usable Privacy and Security*, SOUPS'21 (pp. 263–280). USENIX Association.
71. Norman, D. A. (1983). Some observations on mental models. In D. Gentner & A. L. Stevens (Eds.), *Mental models* (pp. 7–14). Lawrence Erlbaum Associates.
72. Oates, M., Ahmadullah, Y., Marsh, A., Swoopes, C., Zhang, S., Balebako, R., & Cranor, L. F. (2018). Turtles, locks, and bathrooms: Understanding Mental models of privacy through illustration. *Proceedings on Privacy Enhancing Technologies, 2018*(4), 5–32.
73. Olson, J. R., & Rueter, H. H. (1987). Extracting expertise from experts: Methods for knowledge acquisition. *Expert Systems, 4*(3), 152–168.
74. Payne, S. J. (2007). Mental models in human-computer interaction. In A. Sears & J. A. Jacko (Eds.), *The human-computer interaction handbook: Fundamentals, evolving technologies and emerging applications*, Human Factors and Ergonomics Ser. (2nd ed., p. 14). CRC Press.
75. Piekarska, M., Zhou, Y., Strohmeier, D., & Raake, A. (2015). Because we care: Privacy dashboard on Firefox OS. In *Proc. of the 9th Workshop on Web 2.0 Security and Privacy (W2SP)* (article 1). IEEE.

76. Poole, E. S., Chetty, M., Grinter, R. E., & Edwards, W. K. (2008). More than meets the eye: Transforming the user experience of home network management. In *Proc. of the 7th ACM Conference on Designing Interactive Systems*, DIS ’08 (pp. 455–464). ACM.
77. Prettyman, S. S., Furman, S., Theofanos, M., & Stanton, B. (2015). Privacy and security in the brave new world: The use of multiple mental models. In T. Tryfonas & I. Askoxylakis (Eds.), *Human aspects of information security, privacy, and trust*. Lecture Notes in Computer Science 8030 (pp. 260–270). Springer International Publishing.
78. Raja, F., Hawkey, K., & Beznosov, K. (2009). Revealing hidden context: Improving mental models of personal firewall users. In *Proc. of the 5th Symposium on Usable Privacy and Security*, SOUPS’09 (article 1). ACM Press.
79. Renaud, K., Volkamer, M., & Renkema-Padmos, A. (2014). Why doesn’t Jane protect her privacy? In E. De Cristofaro & S. J. Murdoch (Eds.), *14th International Symposium on Privacy Enhancing Technologies (PETS)*. Lecture Notes in Computer Science 8555 (pp. 244–262). Springer International Publishing.
80. Ruoti, S., Monson, T., Wu, J., Zappala, D., & Seamons, K. E. (2017). Weighing context and trade-offs: How suburban adults selected their online security posture. In *Proc. of the 13th Symposium On Usable Privacy and Security*, SOUPS’17 (pp. 211–228). USENIX Association.
81. Sasse, M. A., Smith, M., Herley, C., Lipford, H., & Vaniea, K. (2016). Debunking security–usability tradeoff myths. *IEEE Security & Privacy, 14*(5), 33–39.
82. Schmitt, H., & Groen, E. C. (2021). Qualitätsmodell zur Förderung des Beschäftigtendatenschutzes. *Datenschutz und Datensicherheit - DuD, 45*(1), 28–32.
83. Schmitt, H., & Polst, S. (2020). Anforderungen und Rahmenwerk für den betrieblichen Datenschutz. *Softwaretechnik-Trends, 40*(1), 9–10.
84. Schomakers, E.-M., Lidynia, C., & Ziefle, M. (2018). Hidden within a group of people – mental models of privacy protection. In *Proc. of the 3rd International Conference on Internet of Things, Big Data and Security* (pp. 85–94). SCITEPRESS - Science and Technology Publications.
85. Schultz, E. E., Proctor, R. W., Lien, M.-C., & Salvendy, G. (2001). Usability and security an appraisal of usability issues in information security methods. *Computers & Security, 20*(7), 620–634.
86. Shirogane, J. (2014). Support method to elicit accessibility requirements. In D. Zowghi & Z. Jin (Eds.), *Requirements Engineering* (pp. 210–223). Springer.
87. Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24*(2), 124–133.
88. Tolsdorf, J., Dehling, F., Reinhardt, D., & Lo Iacono, L. (2021). Exploring mental models of the right to informational self-determination of office workers in Germany. *Proc. on Privacy Enhancing Technologies (PoPETs), 2021*(3), 5–27.
89. TrUSD-Konsortium. (2021). Deliverables 1.1 & 1.2: Anforderungen und Anwendungsszenarien (Version 6.0). https://www.trusd-projekt.de/wp/wp-content/uploads/2021/09/TrUSD-D1.1_1.2-Anforderungen.pdf
90. TrUSD-Konsortium. (2022). TrUSD – Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen. https://www.trusd-projekt.de/
91. Ur, B., Bees, J., Segreti, S. M., Bauer, L., Christin, N., & Cranor, L. F. (2016). Do users’ perceptions of password security match reality? In *Proc. of the 2016 CHI Conference on Human Factors in Computing Systems*, CHI ’16 (pp. 3748–3760). ACM.
92. USecureD-Konsortium. (2022). USecureD Tools – Werkzeuge für Usable Security. https://das.h-brs.de/usecured
93. Volkamer, M., & Renaud, K. (2013). Mental models: General introduction and review of their application to human-centred security. In M. Fischlin & S. Katzenbeisser (Eds.), *Number theory and cryptography: Papers in honor of Johannes Buchmann on the occasion of his 60th birthday*. Lecture Notes in Computer Science 8260 (pp. 255–280). Springer.

94. Wästlund, E., Angulo, J., & Fischer-Hübner, S. (2011). Evoking comprehensive mental models of anonymous credentials. In *Proc. of the 2011 IFIP WG 11.4 International Conference on Open Problems in Network Security*, iNetSec'11 (pp. 1–14). Springer.
95. Wash, R., & Rader, E. (2011). Influencing mental models of security: A research agenda. In *Proc. of the 2011 New Security Paradigms Workshop*, NSPW '11 (pp. 57–66). ACM.
96. Wash, R. (2010). Folk models of home computer security. In *Proc. of the 6th Symposium on Usable Privacy and Security*, SOUPS'10 (article 11). ACM Press.
97. (Weber) Dupree, J.-L., Lank, E., & Berry, D. M. (2018). A case study of using grounded analysis as a requirement engineering method. *Science of Computer Programming, 152*(C), 1–37.
98. Weirich, D., & Sasse, M. A. (2001). Pretty good persuasion: A first step towards effective password security in the real world. In *Proc. of the 2001 Workshop on New Security Paradigms*, NSPW '01 (pp. 137–143). Association for Computing Machinery.
99. Whitten, A., & Tygar, J. D. (1998). Usability of security: A case study. Technical report, Carnegie-Mellon Univ Pittsburgh, PA, Dept of Computer Science.
100. Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *USENIX security symposium* (Vol. 348, pp. 679–702). USENIX Association.
101. Wu, J., & Zappala, D. (2018). When is a tree really a truck? exploring mental models of encryption. In *Proc. of the Fourteenth USENIX Conference on Usable Privacy and Security*, SOUPS '18 (pp. 395–409). USENIX Association.
102. Yao, Y., Lo Re, D., & Wang, Y. (2017). Folk models of online behavioral advertising. In *Proc. of the 2017 ACM Conference on Computer Supported Cooperative Work and Social Computing*, CSCW '17 (pp. 1957–1969). ACM.
103. Zeng, E., Mare, S., & Roesner, F. (2017). End user security and privacy concerns with smart homes. In *Proc. of the 13th Symposium on Usable Privacy and Security*, SOUPS'17 (pp. 65–80). USENIX Association.
104. Zimmermann, V., Bennighof, M., Edel, M., Hofmann, O., Jung, J., & von Wick, M. (2018). 'Home, smart home'—exploring end users' mental models of smart homes. In R. Dachselt & G. Weber (Eds.), *Mensch und Computer 2018—workshopband* (article 122). Gesellschaft Für Informatik e.V.
105. Zurko, M. E., & Simon, R. T. (1996). User-centered security. In *Proc. of the 1996 Workshop on New Security Paradigms* (pp. 27–33). ACM.