Jan Tolsdorf*, Florian Dehling, Delphine Reinhardt, and Luigi Lo Iacono

Exploring mental models of the right to informational self-determination of office workers in Germany

Abstract: Applied privacy research has so far focused mainly on consumer relations in private life. Privacy in the context of employment relationships is less well studied, although it is subject to the same legal privacy framework in Europe. The European General Data Protection Regulation (GDPR) has strengthened employees' right to privacy by obliging that employers provide transparency and intervention mechanisms. For such mechanisms to be effective, employees must have a sound understanding of their functions and value. We explored possible boundaries by conducting a semi-structured interview study with 27 office workers in Germany and elicited mental models of the right to informational self-determination, which is the European proxy for the right to privacy. We provide insights into (1) perceptions of different categories of data, (2) familiarity with the legal framework regarding expectations for privacy controls, and (3) awareness of data processing, data flow, safeguards, and threat models. We found that legal terms often used in privacy policies used to describe categories of data are misleading. We further identified three groups of mental models that differ in their privacy control requirements and willingness to accept restrictions on their privacy rights. We also found ignorance about actual data flow, processing, and safeguard implementation. Participants' mindsets were shaped by their faith in organizational and technical measures to protect privacy. Employers and developers may benefit from our contributions by understanding the types of privacy controls desired by office workers and the challenges to be considered when conceptualizing and designing usable privacy protections in the workplace.

Keywords: informational self-determination, privacy at work, mental models, usable privacy controls

DOI 10.2478/popets-2021-0035
Received 2020-11-30; revised 2021-03-15; accepted 2021-03-16.

1 Introduction

During regular employment, employees disclose large amounts of personal data, much of which is known to be sensitive [39, 56]. The digitization of work processes results in the omnipresence of information systems and extends the disclosure and processing of personal data. The increasing vulnerability to privacy violations poses a challenge to the preservation and protection of the fundamental right to privacy [10, 30, 55]. Different to the definition of privacy as the right to freedom from intrusion, as used in the U.S. [30], privacy in Germany is tantamount to the right to informational self-determination. It guarantees individuals transparency and personal control over the collection, use, and disclosure of personal data in all aspects of life. With the GDPR coming into force in 2018, the foundations of informational self-determination were incorporated into national legislation of all member states of the European Union (EU). The difference in power between data processors (e.g. employers) and data subjects (e.g. employees) are balanced by making both jointly responsible for privacy protection. Employers have several obligations, including: making transparent which personal data are processed and for what purposes; providing information on risks and rights in a way that is comprehensible to employees; providing intervention options; ensuring that these rights are respected and can be exercised with the implementation of adequate organizational and technical measures; weighing up their interests against employee privacy and protection needs. For their part, employees are expected to exercise their rights.

We argue that the current situation poses a dilemma: Privacy controls, which employers have to provide and guarantee for but which are to be used by employees, can only protect privacy to the extent that em-

***Corresponding Author: Jan Tolsdorf:** Bonn-Rhein-Sieg University of Applied Sciences, E-mail: jan.tolsdorf@h-brs.de
Florian Dehling: Bonn-Rhein-Sieg University of Applied Sciences, E-mail: florian.dehling@h-brs.de
Delphine Reinhardt: University of Göttingen, E-mail: reinhardt@cs.uni-goettingen.de
Luigi Lo Iacono: Bonn-Rhein-Sieg University of Applied Sciences, E-mail: luigi.lo_iacono@h-brs.de

ployees' perceptions of their rights and obligations are sufficient. From Human Computer Interaction (HCI) research, it is well known that one's internal perceptions (i.e. mental models) of a system (i.e. informational self-determination) considerably influence behavior. If employees have false or significantly limited perceptions, simply providing privacy controls would reduce the principles of the GDPR to absurdity [24]. To shed light on this matter, we explored the boundaries of the perceptions of informational self-determination by conducting a mental model study with 27 office workers in Germany. The key insights are:

(1) We found that terminology rooted in legislation that is used in privacy statements and tools to define different categories of data are ambiguous, and perceptions diverge among individuals. However, the understanding may be aligned by making the attributes *relation to a person*, *sensitivity*, *access*, and *relation to work* explicit.

(2) We found high demands for control over the dissemination and use of data. We identified three groups with different views regarding the level of ex-ante and ex-post privacy control. The groups also differed in their desire for control over (1) the disclosure of data, or (2) the flow of data, or (3) unrestricted control. Only the third group recognized transparency as a key element for privacy. Yet, informational self-determination is seen as a burden in the face of current control options.

(3) We found low awareness about the entities involved in data processing, whether data existed, how data are transferred, where data are stored, and how data are protected. Nevertheless, we found confidence in organizational and technical measures to protect privacy, but also a tendency to over- or underestimate the level of protection. Ignorance is compensated for by high levels of trust in electronic data processing and in the conduct of employers. Also, hackers and internal attackers are believed to pose a great threat to privacy.

We consider our results a valuable contribution to the privacy debate by extending existing U.S.-biased views with insights from the most dominant privacy framework in Europe. By exposing misconceptions and limitations in employees' mental models, we provide insight into which privacy controls employees desire.

The rest of this paper is structured as follows: first, we present our research foundations, followed by related work on privacy, and mental models of privacy at work. We then provide details on our procedure and methods for designing and conducting our study, along with details on the analysis and limitations. We then present the results of our study for each topic. We finally summarize our findings and give an outlook to future work.

2 Research foundations

Our contributions are guided by the overall research question *"what are the mental models of the right to informational self-determination from office workers in Germany?"*. We focused on three key research topics:

(T1) Perceptions of categories of data: The right to informational self-determination stipulates different rules for the processing of different categories of data. Legal texts use different terms both to refer to such categories and to express rules for processing. In practice, office workers are often confronted with legal terms when interacting with data protection guidelines or software. However, the terms are used inconsistently and are attributed with different meanings in different contexts. For example, privacy policies use terms interchangeably or add non-privacy related terms. Also software often use the same terms to describe access rights without considering the exact legal meaning. Based on a review of the GDPR, the Federal Data Protection Act, and expert group discussions (cf. Sec 4), we describe below the most common (legal) terms in Germany:

Data *(ger.: Daten)*
Unspecific in the context of privacy legislation but often used in practice to refer to various categories of data.

Information *(ger.: Informationen)*
Like "data", often synonymous use.

Personally Identifiable Information (PII)
(ger.: Personenbezogene Daten)
Official legal term in German legislation that refers to "any information relating to an identified or identifiable natural person" (Art. 4 GDPR). It is widely used in privacy statements to inform about rights and processing activities. *Examples:* all data with personal reference incl. name, nationality, IP address, personnel number.

Individual-Related Information (IRI)
(ger.: Personenbeziehbare Daten)
A subcategory of PII solely referring to data with indirect personal reference but from which an individual can be identified. Today, referred to as PII in practice. *Examples:* IP address, personnel number.

Private data *(ger.: Private Daten)*
If employees are allowed to use work tools (e.g. IT devices) for private use, law forbids employers to access data marked as private by employees. In practice, the term is also inconsistently used in privacy statements and privacy settings of software to refer to data or access rules. *Examples:* private files, private emails.

Personal data *(ger.: Persönliche Daten)*
Unlike in English, the literal translation of "personal data" into German means such data with a strong "personal" reference and distinguishing characteristic of an individual (cf. GDPR). Personal data in the legal sense is referred to in German as PII. In practice, the term is inconsistently used in privacy statements and privacy settings of software to refer to data or access restrictions. *Examples:* personal preferences, interests, behavior.

To date, it is unknown how office workers perceive these terms and the implied legal meanings. Since legislation obliges employers to *"provide any information [..] in a concise, transparent, intelligible and easily accessible form, using clear and plain language"* (Art. 12, GDPR), identifying potential misconceptions is of high practical relevance. We provide first insights by examining office workers' perceptions and familiarity with these terms.

(T2) Concepts of informational self-determination: The employment context grants extensive information rights to employees, but only limited self-determination. Data processing is permitted without employees' formal consent if the processing is either indispensable, or permitted by the national laws or collective agreements. Compliance with legal obligations can be audited by employee representatives. Also, organizations that exceed a certain size or for which the processing of personal data constitutes a core activity must designate a Data Protection Officer (DPO), who verifies the lawfulness of processing operations. Employees may also turn to DPOs in case of privacy violations or questions. We reveal office workers' perceptions of the current organizational and legal frameworks, as well as their requirements for transparency and intervention, which they derive from their right to privacy at work.

(T3) Awareness of personal data processing: Past studies revealed that people have a poor understanding of the data flow and infrastructure of systems they use every day [27, 29]. However, adequate awareness is vital in drawing accurate conclusions regarding security and privacy. Law even mandates that people *"should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights"* (Recital 39, GDPR). Employees are known to expect their personal data to be protected [15]. It remains unknown however, what employees believe with respect to which precise safeguards are implemented and which threat models exist. We therefore investigated office workers' perceptions of (a) data storage and data flow as well as (b) safeguards and threat models.

3 Related work

We discuss related work with a focus on information privacy in the employment context and the use of mental models for privacy research. Given the contextual dependency of privacy, we focus on work related to the employment relationship.

3.1 Information privacy at work

Privacy is a multidimensional concept that is highly contextual with little agreement in the literature regarding its definition. For the purpose of our research, we focus on information privacy [60], of which vital elements are (1) the control over giving access to information [6, 68], (2) the appropriate flow of information [46], and (3) the uniqueness of privacy perceptions and demands in different contexts [45, 62]. Privacy at work is thus (at least) a tripartite concept comprising control over (1) the *gathering* of personal information (e.g. collection), (2) the *handling* of personal information (e.g. processing) as well as (3) the *perceived legitimacy* of the employer to process data (e.g. expected usage) [3, 16].

Concerning control and the handling of data, people willingly disclose personal information in an employment context, and do so in awareness of possible privacy invasions [9]. The factual knowledge of the data kept by employers is limited [69]. However, employees have been shown to express satisfaction with the granting of indirect consent by providing or withholding requested data on the basis of a "relevancy" criterion for determining their suitability [65, 69]. Data may be deliberately withheld when employees anticipate benefits or fear adverse consequences [9, 61]. To date, the influence of technology-supported control mechanisms has only been considered in connection with the protection of customer data [21].

Concerning the perceived legitimacy of data processing, employees deduce implicit privacy policies from legal regulations and develop certain data handling expectations for different data [61]. Employees may perceive an invasion of their privacy if employers' actual data processing do not meet their expectations. Whether or not the release of personal data by employers to others without the consent of employees constitutes an invasion of privacy remains a topic of academic debate [64, 65, 69].

Previous research has focused on employee monitoring and workplace surveillance [8] as well as ac-

ceptance and impact of technology [10]. Studies have been largely based on quantitative methods using causal modeling [36]. In comparison, fewer qualitative studies have been conducted to explore privacy at work. Those studies that do exist are mainly rooted in academic frameworks of privacy, including Communication Privacy Management (CPM) theory [50] and privacy as contextual integrity [45]. CPM theory describes the tension between the desire to reveal and the desire to withhold information based on ownership, control, and turbulence. Ownership refers to the belief that one owns information, the disclosure of which would make one vulnerable. If information is disclosed, other entities become co-owners. Control refers to managing access to information. Access rules must be negotiated for co-owned information and are based upon boundary spheres. Privacy turbulence occurs when such rules are violated. Contextual integrity emphasizes on the appropriate flow of information. Different transmission principles apply to information, taking into account social norms for a particular context. Previous studies have made use of open-ended online surveys [61], semi-structured interviews [5] or mixed methods approaches based on standardized questionnaires [9].

Our work complements research on information privacy at work, by presenting holistic insights from office workers' privacy perceptions in relation to existing legislation. To the best of our knowledge, we are the first to examine employee requirements for privacy controls based on the right to informational self-determination. With this focus, we expect our results to be highly practical and to contribute towards a modern understanding of privacy in employment relationships in Europe.

3.2 Mental models of privacy at work

Research on mental models of privacy at work is thus far limited. Mental models are simplified internal representations of external reality that enable individuals to make sense of their environment, including but not limited to simple actions, systems, or even complex phenomena [26]. Mental models are generally considered to be incomplete, incorrect, and highly context-dependent, making them unstable or rather inconsistent [47]. Irrespective of their accuracy, mental models guide people's decision making process in both familiar and unfamiliar situations [17, 25]. In the context of HCI on topics of usable security and privacy, mental models are surveyed (1) to construct a system in which cognitive effort is optimised for usability [11, 58, 66], (2) to use them as a tool for effective communication between expert and ordinary users [31, 52, 67, 70], or (3) to capture and explore concerns, expectations, and understandings of technology [20, 23, 27, 38, 54, 71]. Previous research has elicited mental models of privacy in general [48] and in the context of specific technical solutions, with a particular emphasis on online services [13, 19, 33, 37, 51, 58]. From the results of these studies, it is already evident that the nature of privacy does not permit a mental model that is universally true. Instead, individuals use highly simplified models [2] and rely on several incomplete and poorly formed sub-models [51].

Mental models of wearables at work were found to be biased by anxiety of privacy intrusions and the fear of limited self-determination [41]. High levels of concern regarding the misuse of information by employers are reasons that hinder adoption of wearables. Simultaneously, some employees are generally willing to disclose data if they receive adequate gratification in return.

To the best of our knowledge, we are the first to capture and present office workers' perceptions of personal data in the employment context, and gain in-depth insights into their understandings of data processing, data flow, safeguards, and threat models.

4 Methodology

We conducted a mental model study based on semi-structured interviews with 27 office workers from Germany during the period July until September 2019, and in August 2020. In the following, we provide details on the applied methodology, the interview guidelines, the participants' recruitment and demographics, the evaluation, the study's limitations, and ethical considerations.

4.1 Method selection

The elicitation of mental models requires the extraction of subjects' internal representations and can be done either directly or indirectly [49]. Direct methods assume that respondents are able to articulate their trains of thought. Indirect methods are based on researchers' interpretations of a statement or observation. A common procedure is using open-ended semi-structured interviews [66]. They allow participants to express themselves freely and allow the interviewer to clearly work out relevant aspects by asking targeted follow-up questions. In contrast, focus groups may not allow for the

same insights, as participants may not share their personal opinions or may adapt them due to group dynamics [32]. We therefore decided to conduct individual interviews. For these interviews, different methodologies are available, including card-sorting tasks, verbal, and graphical methods. All of these methodologies present different advantages and limitations [7]. In order to overcome the limitations, a combination of at least two elicitation techniques is common [29, 52, 58]. Thus, we chose to conduct our interviews using both verbal and graphical elements, as given that informational self-determination is a highly abstract concept.

4.2 Interview guideline and procedure

Guideline design: The main challenge in creating interview guidelines is to ensure that they cover all topics of interest. To the best of our knowledge, there is no comprehensive model available that could be used to deduce questions on informational self-determination. Thus, to design an appropriate interview guideline, we adopted an expert model approach [42], as it has been proven to be valuable in eliciting mental models on computer security and privacy [13]. With this approach, we aimed to capture and sort relevant aspects of the subject area of interest. In order to ensure the quality of the expert model, we executed an iterative development process: First, we derived an initial version from selected themes on German and EU data protection laws. We then conducted two expert group sessions with researchers from law, psychology, ergonomics, IT systems engineering, as well as security and privacy (N=8). In the first session, the initial model was presented and discussed. We adjusted the model based on the feedback gathered, which involved adding aspects of general privacy literature, as well as technical and organizational circumstances of workplace environments. The revised model was discussed in a second session with the same group of experts. Subsequent changes were again individually reviewed. The final model was divided into four categories: (1) common privacy terminology and processes that are relevant at the moment of data collection; (2) steps of data processing; (3) negative and positive consequences for both employees and employers; (4) transparency aspects of interest to employees. The expert model is available in Appendix A. We derived interview guidelines from the model and revised them with three researchers experienced in conducting interviews. We also conducted three pilot interviews with office workers to fine-tune the questions and wording.

Procedure: In the interview, our participants were welcomed and briefed about the study procedure and conditions. We asked for their consent to elicit drawings, hand writings, voice recordings, and questionnaire answers. Each participant then summarized their job profile and the technical tools used for work. We then presented six different categories of data and asked for definitions and examples. Respondents were then asked to explain their abilities and liberties in disclosing data to employers. We encouraged them to discuss ways in which their privacy could be violated. We then asked for explanations of the concept of informational self-determination and its relevance to the employment relationship. Participants were then guided through a drawing task. We presented a sheet with different data and asked them to indicate (1) how and where the data are stored, (2) who has access to them, and (3) which attack vectors and safeguards exist. At the end of the survey, respondents filled out a demographic questionnaire and were asked if they wanted to add anything to the discussion. Not including time spent briefing and debriefing, the interviews lasted between 29 and 97 minutes. Our interview guidelines are available in Appendix B.

4.3 Participants

Recruitment and enrollment: Since demographic variables correlate to different privacy perceptions [35], we aimed to recruit a heterogeneous sample in terms of professional and socio-demographic backgrounds. The sample was thus recruited to balance gender, work experience, age, job profile, and organization size. We also took into account whether or not the processing of personal data was a core activity of the participants' job.

Initially, we contacted four organizations operating in various business areas and presented the content of the study to the respective management. After the organizations' internal approval audits were completed, one organization required us to involve the staff association before approving recruitment. When required, we also briefed the division managers to secure their agreement and support for the study. We asked the different managers not disclose the content of the study in advance to their employees. We carried out targeted recruitment via e-mail invitations sent to various organizational units (using internal mailing lists) and by asking office workers directly to participate in the study if their demographic details matched our recruitment target. To counteract demographic imbalance, we also contacted office workers outside these organizations. The

invitations asked recruits to participate in an interview on "general practices in dealing with data at the workplace", but did not reveal the exact purpose of the study. Interested employees contacted the interviewers directly. If possible, the interviews took place on the organizations' premises to prime participants to the work context (N=19), or in our laboratories (N=3), or via a web conferencing tool (N=5). Participants did not receive any compensation from the interviewers, but some were allowed to participate during their working hours and were exempted from normal duties.

Demographics and fields of activity: We recruited 27 employees in total (13 female, 14 male) from nine different organizations. Participant age ranged between 24 and 58 years (M=40.5, SD=10.4). Among these participants, 6 worked in micro companies (< 10 employees), 7 in medium companies (< 250 employees), and 14 in large organizations (≥ 250 employees). Typical for office workers, the level of education in our sample was relatively high: the minimal educational level was secondary school and 17 participants held an academic degree. For our analysis, we divided our participants into three groups of different professional backgrounds and experience with data processing:

The first group comprised administration employees (N=9), who were mainly concerned with the management of financial resources and project controlling. These participants mostly worked with central management software and processed personal data of other employees working for the same employer. Two participants held leadership positions with staff responsibility.

Computer scientists and software developers formed the second group (N=11). They were divided into areas of security engineering, requirements engineering, and B2B software for personnel management and stock control. Three participants worked in academia and two held a leadership or managerial position with staff responsibility.

The third group comprised employees with activities other than the processing of personal data and without a computer science background (N=7). This group included two participants who worked as technical engineers in the field of construction who performed mainly CAD-related tasks, two participants who worked as sales staff for B2B software, and three participants who worked in the field of communication and marketing, including media design and consulting (which involves exchanges with customers). One participant held a leadership position with staff responsibility.

A table compiling all participants' demographic information is available in Appendix C.

4.4 Evaluation and data analysis

We conducted a qualitative analysis of our interview data by carrying out inductive coding. We chose this approach because the themes are generated based on the content of the interview itself. For coding, we followed established guidelines and common practices for semi-structured interviews [14, 40]. First, we segmented the transcribed audio recordings into thematic sections based on our interview guidelines. Two coders (A, B) then reviewed the material several times in depth and discussed the topics and themes they encountered. Coder A (the principal investigator [14]) then carried out line by line coding using a mixture of open coding and in vivo coding on the sections of interest. Next, codes of the same topic were merged. The remaining codes were then grouped into related categories and organized into hierarchies by coder A. The set of codes that resulted therefrom was presented to coder B. Coder A and B then coded a randomly selected 30% subset of the interview sections related to each research topic. By doing so, they identified coding conflicts and resolved any differences in code comprehension. The codebook was reworked by reorganizing, adding, or removing codes in order to align to both coders' understandings. A final subsequent recoding of 100% of the material was carried out by the two coders. The coders reached an Inter-Rater Agreement (IRA) of 75% ($Kappa = 0.81$). However, relying solely on Kappa values is debatable due to our complex coding system (214 codes) and the non-equal probability of code occurrence [14]. Therefore, remaining differences were discussed and, if possible, resolved by negotiation. The final IRA is 91%. Full agreement was not reached due to remaining differences in the coders' interpretations of individual statements.

4.5 Limitations

Although the study design intends to capture general mental models of informational self-determination at work, generalization of results cannot be given due to the qualitative property of the study and the strong context dependence of privacy. While education does not significantly impact privacy perceptions [36], it may nevertheless affected the understanding of our questions and the resulting answers. Despite individual demographic differences in our small sample, our study also contains limitations which are well known in privacy research: our participants' perceptions are biased by macro-environmental factors, particularly with regard

to the cultural background and the existing strong governmental regulation framework [36]. Findings may vary for office workers from other organizations, because privacy perceptions correlate to the organization type [63]. Nevertheless, our results constitute an important step towards more complete views of privacy by complementing the results of prior studies that had U.S.-biased samples [12, 36]. Our results also contribute to the diversity of meanings, values, and attitudes about privacy with findings from an underrepresented context.

As participation was voluntary, sampling may be affected by a self-selection bias and limited to the population of people employed at the organizations we contacted. Although we recruited our sample one year after the GDPR came into force, feedback we received during recruitment suggests a "data protection" and "privacy" fatigue. While our invitations did not mention these themes, the chosen wording of the invitations may still evoked unintended associations. The salience bias therefore probably intensified the self-selection bias with privacy fatigued individuals less likely to participate.

The results of studies with a mental model approach are limited by the study's setting, tasks, and analysis [27]. However, our participants may in fact had relatively advanced mental models of informational self-determination. Our sample was biased towards administrative and IT staff, suggesting familiarity with (personal) data processing. Therefore, our results likely represent the more advanced mental models, serving as a sound basis for future quantitative research.

4.6 Ethics

Although we do not have a formal IRB process at our university, we made sure to minimize potential harm by complying with the ethics code of the German Sociological Association as well as the standards of good scientific practice of the German Research Foundation. Our study complies with the strict national and European privacy regulations. We collected data anonymously when possible or when not possible, anonymized the data after the interview. Any contact information was stored separately. Participants were informed about withdrawing their personal data during or after the study. For this purpose, we supplied a deletion token at the beginning of the study. We particularly emphasized that aborting the interview would have no negative consequences and assured employees that neither their participation nor the interview's content were to be reported back to employers or management.

5 Results

The following subsections are organized around our research foundations in Sec. 2. More precisely, Sec. 5.1 is dedicated to T1, while Sec. 5.2 and 5.3 focus on T2 and T3, respectively. We translated relevant statements of our participants' from German into English applying a forward-backward translation procedure with native speakers. In relevant cases, we report how many participants stated specific themes to indicate the frequency and distribution. These counts may serve as indication and not as a basis for a quantitative analysis.

5.1 Perceptions of categories of data

We presented the six different terms for categories of data described in research topic **T1** in a random order to our participants, and asked them to provide definitions and examples with regards to their employment.

5.1.1 Participants' definitions of categories of data

Data and information: Our respondents tended to arrange the terms hierarchically, where *"first of all, everything is 'data'. 'Data' is at the top"* (P15). They emphasized that "data" is a *"generic concept [that describes] all kinds of things"* (P04) and whose composition generates information: *"data are different items out of all this information [..], the single items that you can divide these [other] categories into"* (P20). Our participants agreed that their everyday working life is full of data and information. Yet, we found different associations. While IT and administrative professionals linked mere factual knowledge without personal reference to these terms, other participants referred to data with a clear personal reference relevant to the job (e.g. customer data) when describing "information".

PII and IRI: Half of participants identified the implicit personal reference of IRI. Yet, all of our participants also identified a close relationship between IRI and PII or argued that there is no difference at all. A third of participants expressed difficulties describing these terms. Overall, we found the greatest confirmation that PII were perceived to directly relate to and uniquely identify an individual: *"[PII are] anything that only concerns me, that only I am, with which one could prove that this is my identity"* (P22). Most participants primarily assigned all types of master data (e.g. name)

to PII. IT-staff also linked biometrics and passwords to PII, and noticed PII's generation by tools and their omnipresence in log files. All participants were aware that PII become accessible to a variety of internal and external parties during employment. Very few participants expressed the need to protect PII from employers.

Private data: Participants described private data to be strongly non-work-related and as *"something that only [they] know, but the company does not know"* (P14). Participants stressed the high sensitivity of the data and expressed the urgent need to keep them confidential. Consequently, private data are disclosed reluctantly: *"I hate to give these out, so I'm very careful with them"* (P02). Participants believed that once private data are disclosed, access to them must be limited to a small group of people with special rights. Participants were aware that employers do access private data to at least a limited extent, whether due to socializing activities, business routines, or device usage. Participants located the data on work devices and in calendars, and insisted on having *"a right to expect [private data] to be specially protected"* (P01) by and from employers.

Personal data: We encountered the most non-uniform explanations for this term. Half of participants described personal data as a superset that either included, or was the same as private data. Some gave opposing explanations and declared that private data were the superset, whereas personal data were absolutely confidential. A third of participants claimed that "personal data" was a synonym for PII. The collected statements took fundamentally contradictory positions on a continuum between the extremes of personal reference: one quarter reported that personal data *"directly concern a person in their identity, which describe them, which clearly identify them, which make up their personality"*; in contrast, another quarter perceived personal data simply as *"information that is not personal at all"* and without reference to an individual, but *"which are subject to [their] personal access"*. Despite these differences, our participants agreed that personal data somehow belong to a person and that access may be restricted: *"personal data in the sense that they are not really public, or that I do not want them to be public"* (P17). Participants agreed that personal data serves business purposes and must be available to employers. Still, personal data must only be accessible by a small circle of people or an individual. Few participants indicated that personal data were worth protecting and should stay confidential.

Identified themes: We identified recurring themes in the coding of our participants' explanations which we arranged into four thematic groups (cf. Fig. 1):

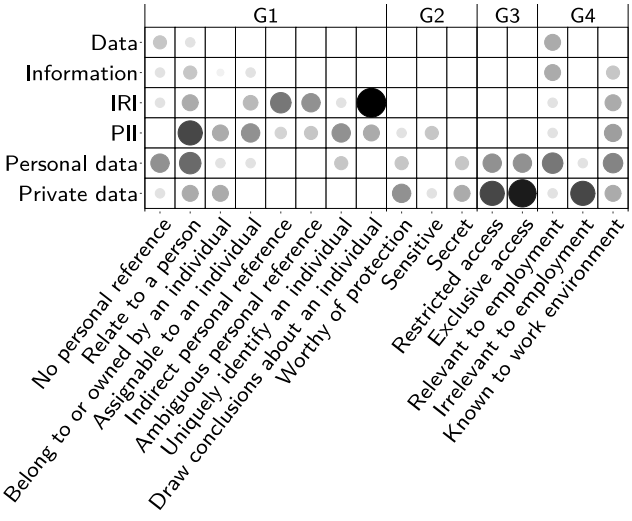

Fig. 1. Identified coding themes: (G1) relation to a person; (G2) data sensitivity; (G3) access to data; (G4) relation to work. Circle size and saturation are proportional to the number of mentions.

The first group (G1) describes the *relation to a person*. We found conflicting views on whether a personal reference exists, and how data relate to a person for five out of six terms. Also, colleagues working within the same organization or team held diverging views.

The second group (G2) concerns the *data sensitivity*. In line with contextual integrity, data marked as sensitive or secret were not perceived worthy protecting from employers if they fit into the context. Also, data considered secret or confidential were not necessarily expected to be sensitive and vice versa. We assume that participants recognized that some data served business purposes and therefore accepted the processing.

The third group (G3) relates to *access* of data. We found that it played a crucial role if participants located data in the private or personal sphere. In these cases participants believed that access to these data must be restricted to oneself and to small groups of entities.

The last group (G4) describes data's *relation to work*. Based on a code-co-occurrence analysis, we found that data with no business relevance were expected to be secret and protected by but also from employers.

5.1.2 Discussion

Our results are somewhat ambivalent. On the one hand, the answers we received indicate that the terms under question evoke adequate associations in a broader sense. Based on accumulated answers, our coding suggests that participants distinguished between three broader con-

cepts: (1) The first concept arises from data and information, and largely lacks privacy related attributes; (2) The second concept arises from PII and IRI, and symbolizes data with clear personal references; (3) The third concept is defined by private data and symbolizes data with no business relevance and strong access restrictions. On the other hand, however, the contradicting statements about personal data symbolize the numerous problems that our participants had with these terms. Half of participants explicitly asked for clarification or did not identify meaningful differences. One participant completely resigned: *"I do not understand these terms at all"*. We obtained similar answers from participants of different professions. Indeed, our results demonstrate that even employees who primarily process (personal) data or hold leadership positions have difficulties with legal terms found in practice. This coincides with previous findings that technical or legal jargon can be misinterpreted both by laypersons and experts [53].

Furthermore, we identified elements of CPM theory in our participants' answers. They intuitively referred to different privacy boundaries in their explanations of the different terms. Here, the assumed business relevance played a decisive role for whether data belong to the public or private sphere. This was associated with expectations of control, claims to ownership, but also rules for co-ownership: *"If I receive [sensitive personal data] from others [..] it can be data that are really confidential, and that I have to safeguard, and that I'm not allowed to disclose to the outside world"* (P22). However, participants made conflicting assumptions about spheres, (co-)ownership, and control for the same data concepts. Such conflicts also existed among participants from the same organization. In some cases, the participants themselves were also confused. Based on our results, office workers' associations of common terms seem to lack harmonized and clear boundaries. According to CPM theory, such *fuzzy boundaries* tend to lead to unintentional privacy intrusions because access rules also become fuzzy [50]. Also, lack of familiarity with the terms' legal meanings favors *boundary rule mistakes*, as employees either access data themselves without authorization or incorrectly assume no access because "they do not understand the privacy rules" [50].

Prior work showed that employees create "implicit rules [..] by implied meanings and understandings" for ownership and control [61]. Our results demonstrate this strategy's susceptibility to error. The use of common terms is likely to leave office workers in an uninformed state, since they are unaware of the rights and obligations that actually apply to, for example, "private data". The identified conflicting interpretations also strongly question the use of common terms for labeling data to express access rights in particular.

Since the use of legal terms will not disappear in practice, potential turbulences may be countered by making meaning and interpretations explicit. A possible approach is the explication of attributes based on the recurring themes that we found. In combination with the clear set of three broader concepts that we identified, we believe that the themes we captured may serve as a basis for more intuitive descriptions in the future.

5.2 Concepts of the right to informational self-determination at work

To address research topic **T2**, we discussed various topics of control over personal data with our participants and concluded with the question *"what is informational self-determination at work?"*. A quarter of participants expressed their lack of familiarity with the term, but their explanations did not differ from responses of participants who did not express this. Participants either discussed new topics or summarized previous topics of the interview which they considered essential for answering this question. One participant had very different associations: *"[It is the right to] freely choose what I want to allow to influence my formation of opinion. That means that I can choose the media I consume."*

We divided the aspects discussed by our participants into four thematic categories (cf. Fig. 2): (1) the *objectives* of informational self-determination; (2) the importance of *self-determination*; (3) the value of *transparency*; and (4) practical *restrictions* and *issues*.

5.2.1 Objectives of informational self-determination

We extracted two distinct objectives that our participants associated with the right to informational self-determination. First they believed it to limit disclosure to such data that are absolutely necessary for the employment relationship. This was accompanied by absolute claims for control: *"Whenever I decide that my employer is interested, that's what he needs, he gets the data, but everything else that goes beyond that, I refuse"* (P05). The second objective was to protect one's privacy from others, whereby participants distinguished between the protection from internals and externals (e.g. customers). A secondary goal was the increased overall control over non-personal data in work processes.

5.2.2 Self-determination

Self-determination was recognized as the key aspect of the right to privacy, which was reflected in this topic filling over half of the discussions. It was defined as having choice and the right that others, including employers, respect decisions to withhold personal data. P06 explained it this way: *"[enquiry forms have] incredibly many fields, but not even half of them are necessary. Self-determination would be how many fields I fill out."* Our participants elaborated on the different facets of control they derived from the right to informational self-determination. We found demands for control over all kinds of manipulations and processing. Three quarters of participants put emphasis on ex-ante control options, asking for control over the receivers and purposes in the disclosure process. A quarter of participants expected to be asked for explicit consent every time their personal data got processed or transmitted: *"[self-determination] would mean nothing else to me than every time someone wants to pass on any personal data or whatever about me to a third party, be it the client, be it colleagues, be it anything, I will be the first party asked if it is okay and if I give my blessing for it to happen"* (P13). Unsurprisingly, self-determination was considered to be missing in practice. For some, it was important to explicitly accept and reject data requests, while others aimed for simplified options, stating that (not) responding to requests was sufficient to (decline) accept data processing. A third of participants pointed out that such control is often unavailable to employees and instead asked for ex-post control that would allow them to object to ongoing processing.

The strong desire for self-determination was also made evident by the fact that half of participants stated that they would conduct their own investigations in the event of misuse of personal data. Very few participants indicated that they would consult a DPO. In cases of intentional misdemeanor, they claimed legal action against their employer by filing a claim for damages.

5.2.3 Transparency

A quarter of participants discussed and recognized the value of transparency for privacy. They noted the complex dimensions of "being informed" and argued it would mean to become truly and deeply aware of purposes and consequences of data processing. They further pointed out that one often does not consider the linkage of data and also sought assurances of the legitimacy of data collection: *"That I can clearly distinguish between legal requirements, data that must be collected, and data that are collected beyond that or linked together for different purposes, so that I can clearly identify at this point what the actual objective is."* (P11).

5.2.4 Restrictions and issues

Participants held different attitudes about the validity of the right to privacy in employment relationships. A third of participants expressed the unrestricted validity of this right. However, most participants noted at least minor restrictions due to the legal and occupational framework. In weighing the advantages of employment against perfect privacy, we found traits of a privacy calculus [18]. Participants noted that the disclosure of personal data was indispensable, especially in service-oriented professions.

Furthermore, participants discussed issues of mental load. They noticed the high cognitive demand that was necessary to truly capture the complexity of self-determined privacy decisions: *"I think [privacy] is a desirable ideal, but never quite attainable, as it would mean that one is actually fully aware of [all the data processing] and that one can then actively take control"* (P03). Participant P18 pointed out the associated high time costs: *"Many people probably feel the need to say that they would like to have informational self-determination, but are not willing to invest time in it."*

Our participants also pointed out the limitations of current privacy controls in many situations. They felt powerless, either because there was *"no way of saying no, I don't want to"* (P05) or they were unsatisfied with the controls they have. On this note, P03 complained that *"you can shape your everyday life by using the appropriate buttons and allowing or rejecting things"*. P18 pointed out the insufficiency of privacy settings, stating that *"if I had to set 10,000 settings every day, no, of course I don't want that"* and explained that there was also the question of *"granularity - I don't want to release data in such a detailed way."*

5.2.5 Clusters of mental models

We conducted a clustering analysis of the coded interviews to examine correlations among our participants' responses. Since our coding was aimed at identifying the presence of themes, we calculated the Jaccard-distance between the binary coding vectors of each participant.

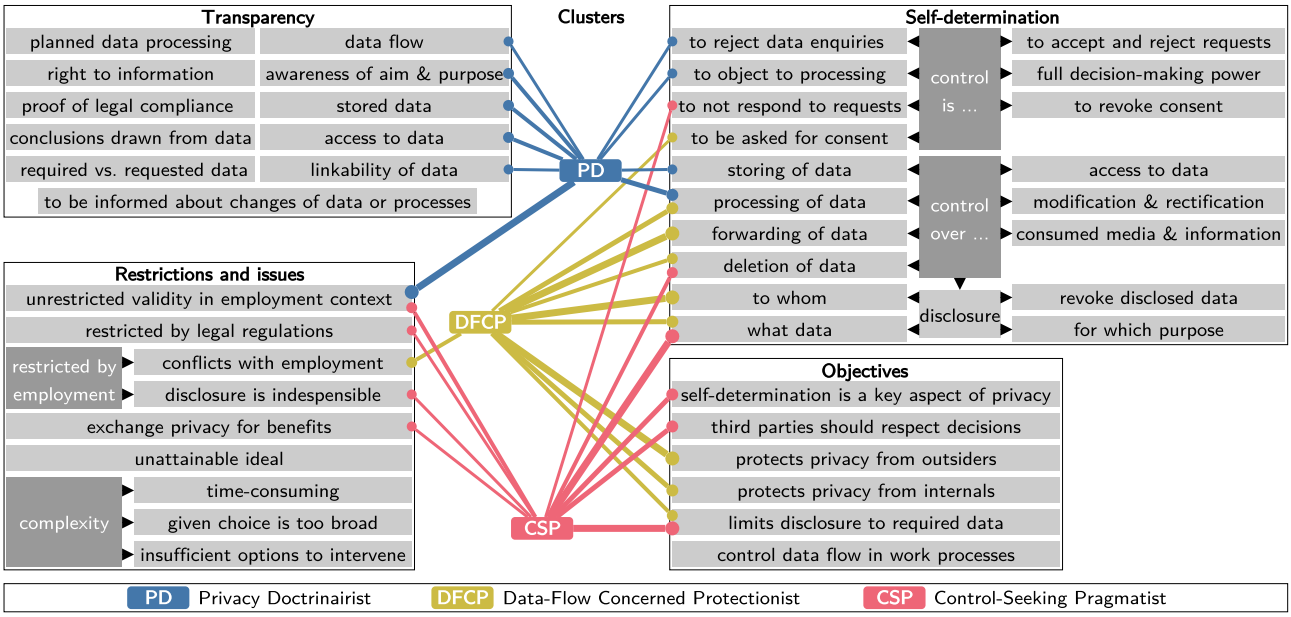

Fig. 2. Identified themes of informational self-determination at work arranged by code groups and hierarchies. For each identified cluster, the top ten codes are linked together. The line width symbolizes the code occurrence in a cluster (mentions / participants).

We used multidimensional-scaling to build a case map, followed by hierarchical clustering (Unweighted Average Linkage). We compared the resulting feature vectors for 2, 3, and 4 clusters by working out differences and similarities. We opted for the three-cluster solution due to meaningful differences in the views and emphasis on privacy objectives, transparency, and control (cf. Fig. 2).

Privacy Doctrinairist (PD): The first group (N=8; 5 IT, 2 others, 1 administrative) demanded the unrestricted validity of the right to informational self-determination at work, requiring full control over the processing of personal data. In addition, they partially recognized the value of ex-post control. Mental models in this cluster were the only ones that recognized transparency as an important key aspect of privacy, in order to become aware of aims and purposes of data processing. Emphasis was put on information about which personal data are stored and who has access to data.

Control-Seeking Pragmatist (CSP): For participants in this group (N=10; 5 administrative, 3 others, 2 IT), informational self-determination was tantamount to control over the disclosure of personal data. Mental models were characterized by the primary goal of limiting disclosure to absolutely necessary data. They defined self-determination as the key element of privacy and required employers to respect decisions to withhold data. Also, they showed traits of pragmatism, since they recognized the necessity of disclosure in employment relationships and tended to accept limitations to privacy.

Data-Flow Concerned Protectionist (DFCP): Participants in this group (N=9; 4 IT, 3 administrative, 2 other) had a strong desire to protect their privacy outside the organization and, to some extent, internally. We found strong claims towards an ability to gain control over both the forwarding of data by employers and the audience to whom personal data were disclosed. These demands were expressed in mental models either through expecting to be asked for explicit consent each time or expecting full control over the processing of data. Nevertheless, some mental models also showed traits of accepting restrictions.

5.2.6 Discussion

Our investigation of the right to informational self-determination reveals that privacy at work is associated with different meanings, objectives, and problems. Our cluster analysis further shows that although the mental models may overlap to some extent, there are different emphases. First, for mental models in the CSP and DFCP clusters, privacy appeared to be almost synonymous with control over the disclosure of data. The PD cluster, however, defined privacy in terms of both the demand for general control over data processing but also for transparency. Thus, while our findings are consistent with previous work highlighting the importance of control over the gathering and handling of data

for privacy at work [16], our results also indicate that transparency is another important dimension. Since legislation grants employees far-reaching rights for transparency but limits self-determination, the PDs belong to the profiteers of the current legal framework, despite their absolute claims to privacy. While no participants reported negative experiences with privacy at work, the somewhat limited view of the right to privacy as ex-ante control among the CSPs and DFCPs likely prevented them from becoming aware of issues that might conflict with their privacy objectives. For example, the right to transparency would allow CSPs to request proof from their employers or DPOs of what data they are required to disclose. The control goals of DFCPs also correlate with the transparency goals of understanding data flow. Here, control claims might reflect a lack of transparency of data flow at work, which is compensated for by considering the moment of disclosure as the most important control point for privacy protection. Participants' current mental models rather seem to simply make them accept conflicts they are aware of. Despite discussing aspects of transparency with all participants, our analysis does not provide an answer as to why CSPs and DFCPs ignored transparency as a key element of privacy.

Moreover, it is questionable whether ex-ante control would allow employees to manage their privacy in a reasonable way, given that our results, similar to findings from online privacy research [23, 54], suggest that privacy management is burdensome and that current intervention options are inadequate or complex. In fact, German legislation deliberately pursues a concept of privacy paternalism for employment relationships, limiting ex-ante control to relieve employees of the burden to protect their privacy. In particular, individual consensus is avoided because it is legally controversial and difficult for organizations to manage. An essential prerequisite for consent in a legal sense is that consent must be voluntary and can be revoked at any time without negative consequences. Due to the imbalance of power between employer and employee, however, true voluntariness is difficult to guarantee. Consent is therefore often unavailable to employees. Instead, legislation encourages collective agreements and makes works councils responsible for privacy protection. Indeed, the problem of true voluntariness appears to be intensified by an overall negativity bias regarding privacy management.

Nevertheless, our findings show that privacy paternalism conflicts with self-determination being deeply rooted in mental models. It is noteworthy that legislation generally enforces self-determination in non-work related contexts. We therefore assume that the legal framework itself does not appear to be problematic. Rather our findings coincide with other work, suggesting that people generally appear to be unaware of their rights towards ex-post control and transparency because of ignorance and false expectations about privacy legislation [4]. Since our sample includes office workers skilled in both security engineering and data processing, our results are likely to include more advanced mental models. We therefore assume that the identified bias towards ex-ante control is not unique to our sample.

Because mental models are formed by prior experience, we hypothesize that this bias results from the privacy controls available in practice, which appear to be characterized by ex-ante control outside of the work context. Likely, mental models of informational self-determination at work are derived to a large extent from mental models in other contexts. This would explain a lack of experience with ex-post controls and transparency, and also prevent mental models from linking these features to the right to privacy. Future challenges are to establish such a link. It should be in the best interests of employers to support their employees in building awareness of feasible control options, instead of leaving them in a mental state of unattainable privacy controls. Despite scientific and legal efforts to provide transparency-enhancing tools [44], their value to the right to privacy and their potential to reduce the burden of privacy management must also be promoted. The public discourse on data protection may have shaped mental models of privacy in an overly one-sided way. Employees should also become aware that DPOs and works councils are there to support them. Here, education is needed to familiarize employees with their rights and the entities involved in the right to privacy at work.

We compared the descriptive characteristics of our clusters with those of personas known from online privacy research and identified minor similarities with Morton's *information controller* and *organizational assurance seeker* [43], and with Schomaker's and Westin's *privacy pragmatist* [34, 57]. Different though, our clusters emphasize the various interpretations of the right to privacy at work instead of privacy concerns. In line with the criticism of online privacy personas not serving well in other than the original context [28], we expect our clusters to highlight privacy perceptions that are particular to the employment context. We would like to point out that our results do not indicate any unconcerned employees either, questioning the applicability of approaches like Westin's unconcerned persona to the work context. We consider this a consequence of the overall high value of the topic of data protection in Germany.

5.3 Awareness of data processing

Awareness of data processing is an essential component of informational self-determination, as it represents the prerequisite for all actions. To examine research topic **T3**, we presented a sheet with the different data types "bank details", "salary", "private address", and "telephone records" printed on it to our participants. We asked them to explain and sketch how and where that data are stored. We emphasized that there was no requirement to provide technically correct sketches. We then asked to include all parties in the drawing that are involved in preparing their payroll together with the corresponding data flow. We concluded by asking participants to spot and mark the places in the drawings which present the highest risk for data misuse, and to explain how the authorized access to the data is ensured. Referring to payroll preparation is a common choice to examine privacy related issues in employment relationships [59]. Employees are familiar with this processing, and it involves the sharing of sensitive personal data: Social security number, name, address, birth date, marital status, religious affiliation, child allowance, handicap allowance, and account number. Other data (e.g. own or children's birth certificates) are inaccessible to employers unless there are special regulations (e.g. civil servants). Also, in Germany, people seldom share information regarding their income level. This adds to the complexity of data flow and protection needs, and requires employers to protect the data by organizational and technical measures. Lastly, processing of payroll information serves as a good proxy for studying awareness, because it restricts the intervention, but not the transparency properties of informational self-determination.

5.3.1 Perceptions of the presence of data

Almost all participants believed that the master data (i.e. bank details, salary, private address) were available in both digital and analog (paper) format. Technical lay participants explained that such data simply flow into some form of program or system and remain there. IT professionals added technical aspects by describing the fine grained levels of detail on the multiple different data bases and backup storages they believed to exist. Participants pointed out that transmission media (e.g. emails) also contain a lot of personal data, but resided on an unmanageable amount of end-user devices inside and outside the organization: *"I can imagine that my private address is available in many local files: when I changed my bank account, I sent an email, which means that this email is in any case stored in our email system, which probably also ran into the backup. I don't know what the HR department did with it. In the worst-case scenario, they also printed out this email"* (P18). The term "personnel file" in particular was used as a synonym for the archiving of data in paper form.

The answers regarding the storage of phone records varied widely. Almost all respondents were uncertain as to whether and, if so, where this data would be stored. Two doubted the data were stored at all, concluding that employers had no interest in evaluating these data. Showing a "nothing to hide" mentality they claimed that they had nothing to fear as long as they did not abuse their tools: "*I'm pretty sure they won't follow up on it [unless] you call the same number maybe 100 times a day*" (P07) and "*I honestly don't know if there is any evidence anywhere, which I wouldn't care about anyway, because I'm actually only using it for business*" (P16). Non-IT staff further speculated that phone records were stored directly in the phone itself. They also reacted with surprise at their own ignorance and assumed that the data were stored together with the master data, or in unknown locations. Participants with a technical background or additional knowledge explained that all phone records were stored in the organization's phone software, and could often remember its actual name. They also included the ISP as the data owner in their drawings, who was supposed to store and have access to this data. Yet, most respondents, including managers, had no ideas about who could actually access these records within their organization, and which details were stored.

Concerning the processing of data in the course of payroll preparation, explanations by participants from the same organizations almost always differed or even contradicted each other. Three IT professionals assumed no intervention of human nor external entities, and explained the details of the payroll being prepared within the company network, while their colleagues and supervisors explained that the data were definitely sent to external authorities. Half of respondents had difficulties in clearly identifying the recipients of their data, mostly stated authorities or tax consultants, and further assumed that the data would be transferred to external parties via CDs, the mail, the internet, or unknown transmission channels: *"As you can see, I have no idea where my data flow to. What is becoming quite frighteningly clear to me right now, of course these are personal data, that you don't know exactly how they are processed, but I think this is also a bit of the banking phenomenon, you just assume that everything is good"* (P18).

5.3.2 Safeguards and threat models

In the following, we present the different safeguards and threat models that we identified in our participants' answers. A summary is provided in Fig 3.

Safeguards: We identified three different themes for safeguards that our participants referred to in their explanations: (1) the *organizational*, (2) the *technical*, and (3) the *physical* theme.

Irrespective of the professional background, nine participants explicitly stated that they were completely unaware of the extent to which safeguards existed for personal data, and also expressed displeasure in realizing their knowledge gaps: *"I have never thought about this before [...] it's also absurd that I don't know whether the data are encrypted"* (P12).

The vast majority identified a functioning authorization concept in the form of Role-Based Access Control (RBAC) within their organization as the most important safeguard. Technical laymen in particular associated strong security convictions with RBAC as the ultimate gatekeeper. Typical for mental models, they referred to their own experiences and claimed that unauthorized access within the enterprise software *"is very very difficult [...] if you don't have the role you can't get the data"* (P06). Yet, they also believed that IT administrators could still access data anytime, anywhere. IT experts, in turn, assumed that RBAC was applied at the file level and that unauthorized access was impossible. On a related note, participants also stressed the importance of authentication. However, merely non-administrative participants assumed that all entities must authenticate to the systems where data reside.

Administrative and IT staff also stressed the importance of appropriate procedural measures to clearly assign rights and responsibilities, or to use a four-eyes principle as a mediator for missing monitoring options. Four participants emphasized the importance of trusting others to handle sensitive data appropriately: *"I can't make sure that [a colleague] does something else with [my data]. So I trust that person to simply do their job"* (P20). Trust was also an important mediator when third parties such as tax consultants were involved in the payroll process: *"Service providers say to what extent they are secure or insecure and to what extent their processes are secure or insecure – I have to rely on them doing everything possible to ensure that the data are secure, which has something to do with trust"* (P17).

Some participants (mostly IT staff) assumed that all data storage and transmission channels were encrypted and ruled out the use of insecure channels: *"Email is an insecure communication medium, anyone can read it, potentially, so obviously [sensitive data] won't be transmitted over it"* (P14). Three participants claimed to delete or expect others to delete emails and data once the processing was finished. Non-IT staff also believed that data media and paper files were safely locked away.

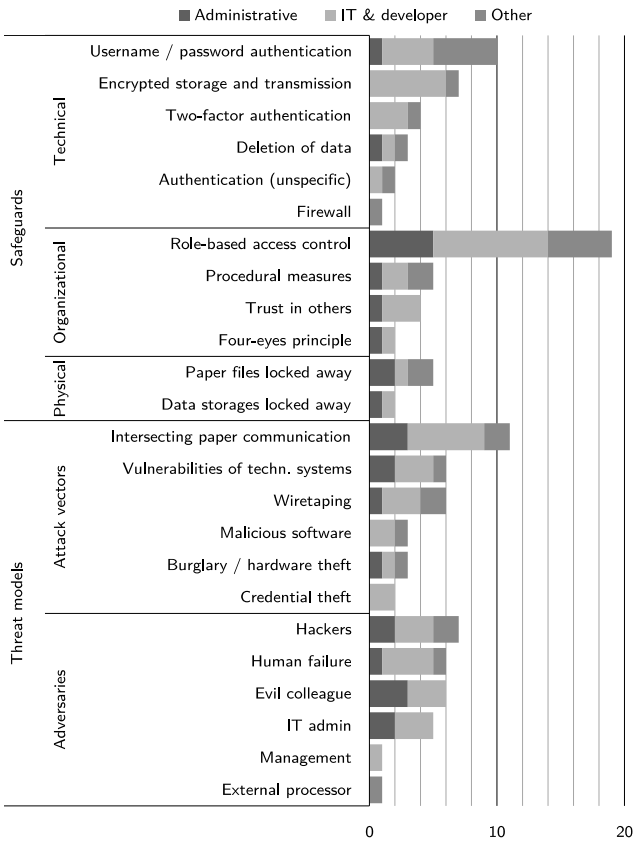

Fig. 3. Safeguards and threat models for privacy at work.

Threat models: Our participants identified hackers and their colleagues as the most likely adversaries, with similar high mentions. In fact, half of participants claimed that colleagues posed a great threat to privacy, since they were considered either vulnerable to socializing attacks, or inattentive and careless, or evil *"super administrators"* who could easily circumvent RBAC and access all data. Management was largely disregarded, but one manager explained the dangers of the role as often having full access to data although not carrying out any data-driven administrative tasks.

Seven participants (5 non-IT) pointed out that external adversaries would need to be highly powerful or skilled in order to retrieve any data. In such a case, however, adversaries could then simply "hack into systems" at will. Yet, IT professionals concluded that even powerful adversaries were very unlikely to get hold of

any raw personal data, and grounded their opinions in the multiple layers of safeguards they believed to exist: *"I have to gain access to the company's server system, I have to pass through a firewall, I have to know or be able to crack passwords to gain access to data of this kind. I think the physical way is the easier way"* (P21).

In this regard, the interception of paper communication was considered the easiest and most likely attack vector to obtain unauthorized access to data, especially in the payroll process. Most attack vectors were mentioned by IT professionals, though only credential theft was unique to this group. Next to vulnerabilities in systems, wiretapping of many unknown communication channels was also identified as attack vectors. Malicious software as well as burglary and hardware theft were sporadically identified as the most likely attack vectors.

5.3.3 Discussion

In the beginning of the interview we asked participants for which purposes their employers process their personal data: the vast majority mentioned the payroll. However, our results suggest that awareness is characterized only by superficial knowledge. In fact, we found only little to moderate factual knowledge on data processing. Participants were surprised by their own ignorance when we confronted them with questions. Thus, it is probably fair to conclude that our sample's overall awareness of data processing was rather low.

Our participants' mental models appear to be biased by their job-specific experiences in their respective work environments. However, advanced technical knowledge is not necessarily beneficial in this context. That is to say that IT professionals made heavily biased assumptions regarding safeguards and threat models, assuming that their employers' IT systems have very extensive and comprehensive security mechanisms. In practice, they ran the risk of overestimating the safeguards. Also, their technical view let them overlook entities in the data processing that they should have been aware of if they had known the business process. Other participants' mental models were rather simple and reflected their "user" experience with information systems. In particular, access to systems was tantamount with access to data, as this was how they perceived interactions themselves. Still, they also put great trust in their employers' infrastructures. Unlike in the U.S., there were no reports on leaked payroll data in the German media, which may explain such strong trust beliefs. However, mass media frequently reports on ransomware or phishing attacks against companies in Germany, yet these do not seem to be reflected in our findings either, apart from few IT professionals referring to them. Instead, internal attackers were considered a major threat to privacy, reflecting the desire to control data flow inside the organization (cf. Sec. 5.2).

Mental models of non-IT professionals were distorted by the belief in data "living" in certain systems or devices. In the case of phone records, some even expected the source to be the only sink. This suggests that participants did not consider data potentially becoming available to entities or systems other than the expected sink. While many participants were clueless with regard to the storing of telephone records, some did not even consider such information being sensitive or privacy-invasive. Also, very few participants raised concerns about the collecting and sharing of metadata by the software and devices they use at work. Such observations are surprising given the prominent discussion on the sensitivity of metadata on media. We would have expected our participants to be more sensitized to this topic, especially with regards to the prominent debate on data retention in the EU and the introduction of the GDPR over the past few years. In fact, Germany suspended data retention in 2017 due to massive concerns about privacy issues related to metadata. Yet, there seems to be little consciousness among non-IT staff.

Lastly, the many implicit assumptions about data processing made by our participants are problematic, because it indicates that they act under uncertainty in practice. Uncertainty is an important factor influencing human behavior and can have a negative impact on privacy [1]. For example, research attributes actions under uncertainty a significant contribution to the privacy paradox [22]. Our results show that ignorance poses a serious risk to fall into a (dis)illusion about personal data processing in employment relationships.

6 Conclusion and future work

The right to informational self-determination guarantees employees transparency and control over the collection, use, and disclosure of personal data. The law mandates employers to provide privacy controls that enable employees to exercise this right. However, our examination of 27 office workers' mental models reveals a variety of issues of the perceptions, concepts, and awareness of this right that could hinder employees from exercising it in practice. The most obvious boundaries are the one-

dimensional views of this right as mere ex-ante control, and the lack of awareness of personal data processing. The latter appears reasonable with regards to the ignorance of transparency. The identified gap between the mental models of informational self-determination and the fundamental objectives of this right [55] has several implications for the design and implementation of effective privacy controls, and for future work.

Implications for informing on data processing: We found overall awareness that many different personal data, including less conspicuous data (e.g. usage data), are collected and processed in the work context. However, office workers seem to struggle to identify the presence of such data in their work environments. We further found that no processing is expected for data with no assumed business relevance, but employees may draw wrong conclusions because they are unaware of purposes and recipients. Especially for data that are not disclosed actively, specific notices about recipients and processing operations are required. Our results indicate, however, that the use of common terms to describe data categories or access is unsuitable for this purpose due to ambiguity and contradicting perceptions. Even employees with leadership or administrative responsibilities cannot provide clear and consistent definitions of common terms. One way to improve this may be to provide explicit descriptions along with the use of concepts based on our identified themes: (1) relation to a person; (2) sensitivity; (3) access; and (4) relation to work. Mitigation efforts should also aim to counteract any inconsistent use of the terms in software, in privacy statements, or by employees and employers.

Implications for risk awareness: As far as the protection of personal data is concerned, our investigation shows that employers appear to enjoy the trust of their employees. In the event of a data protection incident, this trust relationship runs the risk of being severely disrupted. Also, overestimating safeguards hinders office workers from drawing reasoned conclusions about risks to their privacy, what conflicts with legal requirements to provide adequate information about risks. To prevent disillusionment and counteract uncertainty, it should be in employers' best interests to enhance the mental models of office workers and further strengthen the trust culture. Since employers already maintain details about personal data processing within the scope of a legally required processing directory, its careful preparation could, in part, provide the missing link for rising employees' awareness and consciousness.

Implications for control: There appears to be a disparity between the high demands for ex-ante control that we found, and the degree of control that the legal framework and the work context allow. Only *Privacy Doctrinairists* are likely to associate an increase of informational self-determination if privacy controls strictly meet legal requirements. However, since "self-determination" is considered central to the right to privacy but lamented to be lacking in the employment context, it is probably fair to assume that office workers perceive control to be limited in practice. Still, it is questionable whether the provision of ex-ante control would be helpful, because controls to which people are accustomed do not seem to meet their expectations. Even worse, the current design of controls prevents employees from exercising their rights, because the controls are burdensome or even illusory: too complicated, too time-consuming, too many options, or no freedom of choice. This suggests that employees' privacy actually benefits from current practice of dispensing with consent in the work context, because free consent is too burdensome. To compensate for control requirements, our results suggest that a reduced set of distinct controls would likely already accommodate many objectives related to ex-ante control: Involvement in sharing personal data with outsiders (e.g. business partners); and serious efforts by employers to educate their employees on how to reduce disclosure to the absolute minimum. However, we argue that employers and future work must also strive to educate and provide tools for ex-post control. Since it lies at the heart of the legal framework, employees require a solid understanding of and confidence in this form of control. Once they have familiarized themselves with it, employees may possibly even perceive it to be less burdensome in comparison to ex-ante control.

Implications for future research: Previous studies on privacy at work often consider the employers and cyber criminals to be the only intruders that impact employees' privacy perceptions [15, 41]. Our results suggest, however, that employees consider their coworkers and IT staff to be the more likely invaders to their privacy, but barely regard management as adversaries. This observation adds more depth to previous assumptions on adversaries, and shifts perspective. Assumptions about implemented protection mechanisms also varied among participants from the same organization and relied on the concept of trust when it comes to transmitting data to third parties. We recommend that future research should take (1) trust in affiliated parties, (2) trust in internal IT staff, and (3) assumptions on implemented safeguards into consideration and include them as control variables or antecedents in studies to explore their impact on privacy at work.

Acknowledgement

We thank our study participants and the participating organizations for supporting our work. We would also like to express our sincere thanks to: Hartmut Schmitt and Svenja Polst for helping us conducting the interviews; Graham Ashcroft for helping us translate the participants' statements; and Rehana Omardeen for helping us improve the final editing of this paper. Last but not least, we thank the anonymous reviewers for their guidance and insightful comments. This research is supported by the German Federal Ministry of Education and Research (BMBF) under the contract number 16KIS0899.

References

[1] A. Acquisti, L. Brandimarte, and G. Loewenstein. Privacy and Human Behavior in the Age of Information. *Science*, 347(6221):509–514, 2015.

[2] A. Acquisti and J. Grossklags. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy Magazine*, 3(1):26–33, 2005.

[3] B. J. Alge, G. A. Ballinger, S. Tangirala, and J. L. Oakley. Information Privacy in Organizations: Empowering Creative and Extrarole Performance. *Journal of Applied Psychology*, 91(1):221–232, 2006.

[4] F. Alizadeh, T. Jakobi, A. Boden, G. Stevens, and J. Boldt. GDPR Reality Check - Claiming and Investigating Personally Identifiable Data from Companies. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 120–129, 2020.

[5] M. Watkins Allen, S. J. Coopman, J. L. Hart, and K. L. Walker. Workplace Surveillance and Managing Privacy Boundaries. *Management Communication Quarterly*, 21(2):172–200, 2007.

[6] I. Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Pub. Co, 1975.

[7] F. Asgharpour, D. Liu, and L. Jean Camp. Mental Models of Security Risks. In *Proceedings of the 11th International Conference on Financial Cryptography and 1st International Conference on Usable Security (FC, USEC)*, pages 367–377, 2007.

[8] N. Backhaus. Context Sensitive Technologies and Electronic Employee Monitoring: A Meta-Analytic Review. In *Proceedings of the 11th IEEE/SICE International Symposium on System Integration (SII)*, pages 548–553, 2019.

[9] K. Ball, E. M. Daniel, and C. Stride. Dimensions of Employee Privacy: An Empirical Study. *Information Technology & People*, 25(4):376–394, 2012.

[10] D. P. Bhave, L. H. Teo, and R. S. Dalal. Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management*, 46(1):127–164, 2020.

[11] C. Bravo-Lillo, L. F. Cranor, J. Downs, and S. Komanduri. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security & Privacy Magazine*, 9(2):18–26, 2011.

[12] F. Bélanger and R. E. Crossler. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4):1017–1042, 2011.

[13] L. J. Camp. Mental Models of Privacy and Security. *IEEE Technology and Society Magazine*, 28(3):37–46, 2009.

[14] J. L. Campbell, C. Quincy, J. Osserman, and O. K. Pedersen. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research*, 42(3):294–320, 2013.

[15] D. Carpenter, A. McLeod, C. Hicks, and M. Maasberg. Privacy and Biometrics: An Empirical Examination of Employee Concerns. *Information Systems Frontiers*, 20(1):91–110, 2018.

[16] X. Chen, J. Ma, J. Jin, and P. Fosh. Information Privacy, Gender Differences, and Intrinsic Motivation in the Workplace. *International Journal of Information Management*, 33(6):917–926, 2013.

[17] K. J. W. Craik. *The Nature of Explanation*. Cambridge: Cambridge University Press, 1943.

[18] T. Dinev and P. Hart. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1):61–80, 2006.

[19] S. Fischer-Hübner, J. S. Pettersson, and J. Angulo. HCI Requirements for Transparency and Accountability Tools for Cloud Service Chains. In *Accountability and Security in the Cloud: First Summer School, Cloud Accountability Project, A4Cloud, Malaga, Spain, June 2-6, 2014, Revised Selected Papers and Lectures*, Lecture Notes in Computer Science, pages 81–113. 2015.

[20] K. R. Fulton, R. Gelles, A. McKay, Y. Abdi, R. Roberts, and M. L. Mazurek. The Effect of Entertainment Media on Mental Models of Computer Security. In *Proceedings of the 15th USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 79–95, 2019.

[21] M. F. Gan, H. N. Chua, and S. F. Wong. Privacy Enhancing Technologies Implementation: An Investigation of its Impact on Work Processes and Employee Perception. *Telematics and Informatics*, 38(1):13–29, 2019.

[22] N. Gerber, P. Gerber, and M. Volkamer. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security*, 77(8):226–261, 2018.

[23] N. Gerber, V. Zimmermann, and M. Volkamer. Why Johnny Fails to Protect his Privacy. In *2019 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 109–118, 2019.

[24] J. Johansen and S. Fischer-Hübner. Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. In *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*, pages 275–291. Springer International Publishing, 2020.

[25] P. N. Johnson-Laird. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press, 1986.

[26] N. Jones, H. Ross, T. Lynam, P. Perez, and A. Leitch. Mental Models: An Interdisciplinary Synthesis of Theory and Methods. *Ecology and Society*, 16(1):1–13, 2011.

[27] R. Kang, L. Dabbish, N. Fruchter, and S. Kiesler. "My Data Just Goes Everywhere:" User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the 11th USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 39–52, 2015.

[28] J. King. Taken Out of Context: An Empirical Analysis of Westin's Privacy Scale. In *Proceedings of the 1st Workshop on Privacy Personas and Segmentation (PPS)*, pages 1–8, 2014.

[29] P. Klasnja, S. Consolvo, J. Jung, B. M. Greenstein, L. LeGrand, P. Powledge, and D. Wetherall. "When I am on Wi-Fi, I am fearless": Privacy Concerns & Practices in Everyday Wi-Fi Use. In *Proceedings of the ACM Conference on Human Factors in Computing Systems (SIGCHI)*, pages 1993–2002, 2009.

[30] D. Krebs and J. Doctor. "Privacy by Design": Nice-to-have or a Necessary Principle of Data Protection Law? *Journal of Intellectual Property, Information Technology and E-Commerce Law*, 4(1):2–20, 2013.

[31] K. Krombholz, K. Busse, K. Pfeffer, M. Smith, and E. von Zezschwitz. "If HTTPS Were Secure, I Wouldn't Need 2fa" - End User and Administrator Mental Models of HTTPS. In *Proceedings of the 40th IEEE Symposium on Security and Privacy (S&P)*, pages 246–263, 2019.

[32] R. A. Krueger and M. A. Casey. *Focus Groups: A Practical Guide for Applied Research*. SAGE, 2015.

[33] P. Kumar, S. Milind Naik, U. R. Devkar, M. Chetty, T. L. Clegg, and J. Vitak. 'no telling passcodes out because they're private': Understanding children's mental models of privacy and security online. *Proceedings of the ACM on Human-Computer Interaction*, 1(CSCW):1–21, 2017.

[34] P. Kumaraguru and L. F. Cranor. Privacy Indexes: A Survey of Westin's Studies. Technical report, Institute for Software Research, International School of Computer Science Carnegie Mellon University Pittsburgh, 2005.

[35] M. Kwasny, K. Caine, W. A. Rogers, and A. D. Fisk. Privacy and Technology: Folk Definitions and Perspectives. Technical report, Atlanta, GA: Georgia Institute of Technology School of Psychology – Human Factors and Aging Laboratory, 2008.

[36] Y. Li. Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28(1):453–496, 2011.

[37] J. Lin, N. Sadeh, S. Amini, J. Lindqvist, J. I. Hong, and J. Zhang. Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing. In *Proceedings of the 14th ACM Conference on Ubiquitous Computing (UbiComp)*, pages 501–510, 2012.

[38] M. Maceli. Librarians' Mental Models and Use of Privacy-Protection Technologies. *Journal of Intellectual Freedom & Privacy*, 4(1):18–32, 2019.

[39] E. Markos, G. R. Milne, and J. W. Peltier. Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *Journal of Public Policy & Marketing*, 36(1):79–96, 2017.

[40] P. Mayring. Qualitative Content Analysis. *Forum Qualitative Sozialforschung / Forum: Qualitative Social Research*, 1(2):1–10, 2000.

[41] T. Mettler and J. Wulf. Physiolytics at the Workplace: Affordances and Constraints of Wearables Use from an Employee's Perspective. *Information Systems Journal*, 29(1):245–273, 2019.

[42] M. G. Morgan. *Risk Communication: A Mental Models Approach*. Cambridge University Press, 2002.

[43] A. Morton and M. A. Sasse. Desperately Seeking Assurances: Segmenting Users by Their Information-seeking Preferences. In *Proceedings of the 12th IEEE Annual International Conference on Privacy, Security and Trust (PST)*, pages 102–111, 2014.

[44] P. Murmann and S. Fischer-Hübner. Tools for Achieving Usable Ex Post Transparency: A Survey. *IEEE Access*, 5:22965–22991, 2017.

[45] H. Nissenbaum. Privacy as Contextual Integrity. *Washington Law Review*, 79(1):1119–157, 2004.

[46] H. Nissenbaum. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford University Press, 2010.

[47] D. A. Norman. Some Observations on Mental Models. In *Mental Models*, pages 7–14. Lawrence Erlbaum Associates Inc., 1983.

[48] M. Oates, Y. Ahmadullah, A. Marsh, C. Swoopes, S. Zhang, R. Balebako, and L. F. Cranor. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. *Proceedings on Privacy Enhancing Technologies*, 2018(4):5–32, 2018.

[49] J. Reitman Olson and H. H. Rueter. Extracting Expertise from Experts: Methods for Knowledge Acquisition. *Expert Systems*, 4(3):152–168, 1987.

[50] S. Petronio. *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press, 2002.

[51] S. Spickard Prettyman, S. Furman, M. Theofanos, and B. Stanton. Privacy and Security in the Brave New World: The Use of Multiple Mental Models. In *Proceedings of the 3rd International Conference on Human Aspects of Information Security, Privacy, and Trust (HAS)*, pages 260–270, 2015.

[52] F. Raja, K. Hawkey, and K. Beznosov. Revealing Hidden Context: Improving Mental Models of Personal Firewall Users. In *Proceedings of the 5th ACM Symposium on Usable Privacy and Security (SOUPS)*, pages 1–12, 2009.

[53] J. R. Reidenberg, T. Breaux, L. F. Cranor, B. French, A. Grannis, J. T. Graves, F. Liu, A. McDonald, T. B. Norton, R. Ramanath, N C. Russell, N. Sadeh, and F. Schaub. Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Technology Law Journal*, 30(1):39–88, 2015.

[54] K. Renaud, M. Volkamer, and A. Renkema-Padmos. Why Doesn't Jane Protect Her Privacy? In *Proceedings of the 14th Privacy Enhancing Technologies Symposium (PETS)*, pages 244–262, 2014.

[55] A. Rouvroy and Y. Poullet. The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy. In *Reinventing Data Protection?*, pages 45–76. Springer, Dordrecht, 2009.

[56] E.-M. Schomakers, C. Lidynia, D. Müllmann, and M. Ziefle. Internet Users' Perceptions of Information Sensitivity – In-

sights from Germany. *International Journal of Information Management*, 46(1):142–150, 2019.

[57] E.-M. Schomakers, C. Lidynia, L. Vervier, and M. Ziefle. Of Guardians, Cynics, and Pragmatists - A Typology of Privacy Concerns and Behavior:. In *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS)*, pages 153–163, 2018.

[58] E.-M. Schomakers, C. Lidynia, and M. Ziefle. Hidden within a Group of People - Mental Models of Privacy Protection:. In *Proceedings of the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS)*, pages 85–94, 2018.

[59] J. Šišková and E. Lőrinczová. Implementation of GDPR into Payroll Accounting in the Czech Republic. In *Proceedings of the 10th Hradec Economic Days (HED)*, pages 1–8, 2020.

[60] H. J. Smith, T. Dinev, and H. Xu. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4):989–1016, 2011.

[61] S. A. Smith and S. R. Brunner. To Reveal or Conceal: Using Communication Privacy Management Theory to Understand Disclosures in the Workplace. *Management Communication Quarterly*, 31(3):429–446, 2017.

[62] D. J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477–560, 2006.

[63] E. F. Stone, H. G. Gueutal, D. G. Gardner, and S. McClure. A Field Experiment Comparing Information-privacy Values, Beliefs, and Attitudes Across Several Types of Organizations. *Journal of Applied Psychology*, 68(3):459–468, 1983.

[64] P. D. Tolchinsky, M. K. McCuddy, J. Adams, D. C. Ganster, R. W. Woodman, and H. L. Fromkin. Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment. *Journal of Applied Psychology*, 66(3):308–313, 1981.

[65] J. Tolsdorf and F. Dehling. In Our Employer We Trust: Mental Models of Office Worker's Privacy Perceptions. In *Proceedings of the 1st Asian Workshop on Usable Security (AsiaUSEC, FC workshop)*, pages 122–136, 2020.

[66] M. Volkamer and K. Renaud. Mental Models – General Introduction and Review of Their Application to Human-Centred Security. In *Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*, pages 255–280. Springer Berlin Heidelberg, 2013.

[67] R. Wash. Folk Models of Home Computer Security. In *Proceedings of the 6th ACM Symposium on Usable Privacy and Security (SOUPS)*, pages 1–16, 2010.

[68] A. F. Westin. *Privacy and Freedom*. Athenum Press, 1967.

[69] R. W. Woodman, D. C. Ganster, J. Adams, M. K. McCuddy, P. D. Tolchinsky, and H. Fromkin. A Survey of Employee Perceptions of Information Privacy in Organizations. *Academy of Management Journal*, 25(3):647–663, 1982.

[70] E. Wästlund, J. Angulo, and S. Fischer-Hübner. Evoking Comprehensive Mental Models of Anonymous Credentials. In *Proceedings of the 2011 IFIP WG 11.4 international conference on Open Problems in Network Security (iNetSEc)*, pages 1–14, 2011.

[71] E. Zeng, S. Mare, and F. Roesner. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th USENIX Symposium on Usable Privacy and Security (SOUPS)*, pages 65–80, 2017.

A Expert model

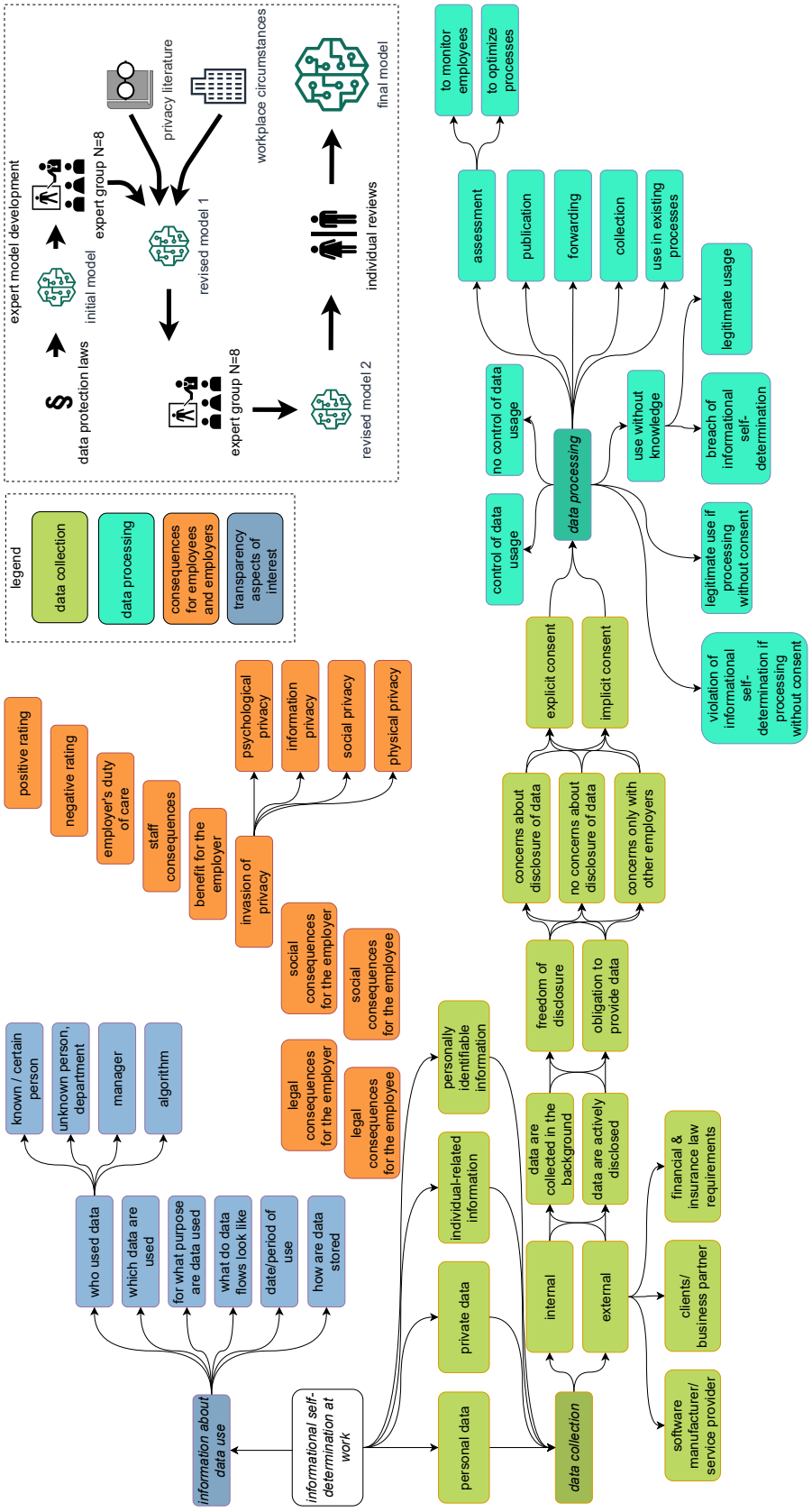

Fig. 4. Expert model of the right to informational self-determination at work.

B Interview outline (translated)

Welcome the participant and brief about the study procedure and the study conditions. Then ask for their consent to elicit data (drawings, hand writings, answers to questionnaire, voice recording) and handout the deletion token.

Before we start with the interview I would like to point out that I am only interested in your personal opinion or view on the respective question. For all questions that I will ask you always applies that: there are no wrong answers; and this is not a quiz and it is not about you giving a technically correct answer.
If I phrase a question in an unclear or imprecise way, or if you are not sure how I mean a question, or if you yourself have a question for me, please feel free to interrupt me. Do you feel comfortable starting the interview now?

To begin with, I would like to know a little more about your daily work routine:
- Please describe to me what tasks you mainly deal with in your everyday working life.

Have moderation cards and pen ready

- Which technical aids or tools do you use in your daily work? Write each tool on a (moderation) card.
- What specific tasks do you perform with these tools?
- Which applications do you use on a daily basis?

All cards with data categories on the table / screen.

Try to explain the following terms in relation to your everyday work. Provide examples of each term.
- Information
- Data
- Private data
- Personal data
- Personally identifiable information
- Individual-related information

- What data or information about you, are known to your employer?
- Can you think of other data or information when you think of the terms laid out and the tools you use?
- What data are collected in your work environment?
- How does your employer obtain such data from you and about you?

- For what purposes can this data be used?

- How do you consent to the use of this data?
- What liberties do you have when it comes to data about you that are available to your employer?

We have now already talked about some examples of data and information that you disclose in the course of your employment. In the private context, there are situations in which you have to provide data, for example, in order to be able to use an online service, but you may feel uneasy about the data you are asked for. In the following questions, I would like to know how you feel about this in the work context.
- Do you think your colleagues disclose personal data in the work context that they would prefer to withhold?
- Do you think there are any data that your colleagues (consciously) withhold from their employer?
- Can you provide examples of what kind of data this might be?
- Have you already been in a situation where you had to disclose data to your employer that you would have preferred to keep secret?

So far, we have talked about interactions between employees and their employers.
- Are there any third parties besides your employer who use, or collect, such data about you in the context of your job?

IF YES: provide blank, white DIN A4; skip otherwise

- Through which channel do these organizations or service providers receive your data? Please describe this data flow as accurately as possible by making a sketch.
- Will the data be passed on to external companies via the employer, or will they access the data directly from the employee?

We have mainly talked about how you, as an employee, handle your data. Now I would like to talk a little bit about the party that collects and uses such data, i.e. the employers.
- Do you think it is possible that your employer uses data from you or data about you without your knowledge?

- **IF NO:** Do you think it is possible in other companies that employers use such data from their employees without them being aware of it?
- What types of data are involved?
- What is the employer's purpose in doing so?

- Assuming an employer collects or uses data without the consent of its employees, what consequences could the misuse of data have for employees?
- How can employees respond to the misuse of their data?
- Assuming you were in such a situation, what would you do?

Let us assume that employers behave the way you want them to behave. Now suppose that you could ask your employer everything about your personal data that you are interested in.
- What would you like to know about the data that your employer uses about you?
- Who uses your data?

Finally, can you please explain to me the following concept:
- What do you understand by informational self-determination?
- What does informational self-determination in the workplace mean to you?

I would like you now to answer some questions by making sketches on this sheet. Also, please explain to me what you are drawing! Please keep in mind that it is not about drawing a technically correct picture! There is no right and wrong in this task!
On the left side of the sheet, you find some examples of personal data that are collected by your employer ("bank details", "salary", "private address", and "telephone records"). Your employer needs some of this data to prepare your monthly payroll.
- First, I would like you to describe how the data on the left are stored at your employer's site. To do this, use the space in the middle of the sheet and include the four boxes on the left in your sketch.
- Some of the data mentioned here are required to prepare your payroll. Please sketch how the payroll is generated using the example data.
- By whom will the payroll be prepared?
- How does the responsible office get access to the data?

You have now illustrated how your data will be used for payroll. In this sketch, how do you ensure that only the people responsible for payroll have access to this data.
- At what point in your sketch do you check to see if access is allowed?
- Suppose a non-authorized person wants to gain access to your data. Where in your sketch could they access the data?

Questionnaire on demographics (online):
- Age [years, no answer]
- Gender [f, m, d, no answer]
- Marital Status [Single, Married, Registered civil partnership, Divorced, Widowed, no answer]
- Highest Education [Secondary (elementary) school certificate, secondary school or equivalent qualification, advanced technical college or university entrance qualification, apprenticeship/vocational training, Academic degree, no educational attainment, no answer]
- Employment Total [years, no answer]
- Employment Current Employer [years, no answer]
- Industry [text, no answer]
- Professional Title [text, no answer]

Ask the participant whether they want to add anything to the previous discussion. Answer their questions if any. Ask the participant not disclose the contents of the study to their colleagues.

C Participants

Table 1. Participants Demographics

ID	Age	Sex	Education	Profession	Employment (years)		Org. Size	Industry (OECD)
					Total	Employer		
Administrative Activities (i.e. the processing of personal data is the core job activity)								
P01	46-55	m	Academic Degree	Third Party Fund Manager	16-20	6-10	L	Education
P02	56-65	f	Academic Degree	Administrative Employee	26-30	0-5	L	Education
P03	46-55	m	Academic Degree	Team Leader	16-20	6-10	L	Education
P04	46-55	f	University Entrance Qualification	Administrative Employee	26-30	6-10	L	Education
P05	46-55	f	Secondary School or Higher	Administrative Employee	31-35	31-35	L	Education
P06	56-65	f	Academic Degree	Team Leader Accounting	26-30	0-5	L	Education
P07	46-55	m	Academic Degree	Project Controller	20-25	6-10	L	Education
P08	46-55	m	Academic Degree	Purchasing Employee	20-25	6-10	L	Education
P09	26-35	f	Secondary School or Higher	Clerk	16-20	16-20	L	Education
IT & Software Development (i.e. the job requires overall familiarity with the processing of data)								
P10	26-35	m	Apprenticeship	Software Developer	6-10	0-5	S	IT-services
P11	36-45	m	University Entrance Qualification	IT Administrator	20-25	11-15	S	IT-services
P12	26-35	m	Apprenticeship	Application Developer	6-10	0-5	S	IT-services
P13	18-25	m	Academic Degree	Software Developer	0-5	0-5	M	IT-services
P14	26-35	f	Academic Degree	Software Developer	11-15	11-15	M	IT-services
P15	26-35	m	Academic Degree	Software Engineer	6-10	6-10	M	IT-services
P16	36-45	f	Academic Degree	Software Developer	20-25	11-15	M	IT-services
P17	46-55	m	Academic Degree	Management Software Development	16-20	0-5	M	IT-services
P18	36-45	m	Academic Degree	Researcher Software Development	11-15	6-10	L	Research
P19	18-25	m	Academic Degree	Research Assistant Software Development	0-5	0-5	L	Research
P20	36-45	f	Academic Degree	Researcher Software Development	20-25	11-15	L	Research
Other (i.e. the processing of personal data is not a core activity)								
P21	46-55	m	Apprenticeship	Supporter	26-30	11-15	S	IT-services
P22	46-55	f	Apprenticeship	Sales Employee	31-35	11-15	S	IT-services
P23	46-55	f	Academic Degree	Architect	20-25	6-10	S	Construction
P24	18-25	f	University Entrance Qualification	Civil Engineer	0-5	0-5	M	Construction
P25	26-35	f	Apprenticeship	Media Designer	11-15	6-10	M	Marketing
P26	26-35	f	Academic Degree	Teamlead Owned and Paid Media	11-15	0-5	L	Non-profit
P27	26-35	m	Academic Degree	Media Consultant	6-10	0-5	L	Marketing

Org. Size: S: micro (< 10) employees, M: medium (< 250) employees, L: large (≥ 250) employees