



GEORG-AUGUST-UNIVERSITÄT  
GÖTTINGEN

## INVESTIGATION OF INFORMATION PRIVACY IN EMPLOYMENT

Fundamental Knowledge and Practical Solutions for the Human-Centered Design of Measures  
to Preserve the Right to Informational Self-Determination in Employment

Dissertation

for the award of the degree

DOCTOR RERUM NATURALIUM

of the Georg-August-Universität Göttingen

within the doctoral program

PhD Programme in Computer Science (PCS)

of the Georg-August University School of Science (GAUSS)

submitted by

JAN TOLSDORF

from Cologne, Germany

Göttingen, 2022



Institute of Computer Science  
Computer Security and Privacy

### **Thesis Committee**

---

Prof. Dr.-Ing. Delphine Reinhardt  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

Prof. Dr.-Ing. Luigi Lo Iacono  
Institute for Cyber Security & Privacy  
Hochschule Bonn-Rhein-Sieg, Germany

Prof. Dr. phil.-nat. Jens Grabowski  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

### **Members of the Examination Board**

---

Prof. Dr.-Ing. Delphine Reinhardt  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

Prof. Dr. rer. pol. Kai Rannenberg  
Chair of Mobile Business & Multilateral Security  
Goethe-Universität Frankfurt am Main, Germany

Prof. Dr.-Ing. Luigi Lo Iacono  
Institute for Cyber Security & Privacy  
Hochschule Bonn-Rhein-Sieg, Germany

### **Further Members of the Examination Board**

---

Prof. Dr. phil.-nat. Jens Grabowski  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

Prof. Dr.-Ing. Ramin Yahyapour  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

Prof. Dr. rer. nat. Bernhard Schmitzer  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

Prof. Dr. rer. nat. Dieter Hogrefe  
Institute of Computer Science  
Georg-August-Universität Göttingen, Germany

**Date of the oral examination:** 08 August 2022

## ABSTRACT

---

The processing of employee personal data is dramatically increasing. To protect employees' fundamental right to privacy, the law provides for the implementation of privacy controls, including transparency and intervention. At present, however, the stakeholders responsible for putting these obligations into action, such as employers and software engineers, simply lack the fundamental knowledge needed to design and implement the necessary controls. Indeed, privacy research has so far focused mainly on consumer relations in the private context. In contrast, privacy in the employment context is less well studied. However, since privacy is highly context-dependent, existing knowledge and privacy controls from other contexts cannot simply be adopted to the employment context. In particular, privacy in employment is subject to different legal and social norms, which require a different conceptualization of the right to privacy than is usual in other contexts. To adequately address these aspects, there is broad consensus that privacy must be regarded as a socio-technical concept in which human factors must be considered alongside technical-legal factors. Today, however, there is a particular lack of knowledge about human factors in employee privacy. Disregarding the needs and concerns of individuals or lack of usability, though, are common reasons for the failure of privacy and security measures in practice.

This dissertation addresses key knowledge gaps on human factors in employee privacy by presenting the results of a total of three in-depth studies with employees in Germany. The results provide insights into employees' perceptions of the right to privacy, as well as their perceptions and expectations regarding the processing of employee personal data. The insights gained provide a foundation for the human-centered design and implementation of employee-centric privacy controls, i.e., privacy controls that incorporate the views, expectations, and capabilities of employees.

Specifically, this dissertation presents the first mental models of employees on the right to informational self-determination, the German equivalent of the right to privacy. The results provide insights into employees' (1) perceptions of categories of data, (2) familiarity and expectations of the right to privacy, and (3) perceptions of data processing, data flow, safeguards, and threat models. In addition, three major types of mental models are presented, each with a different conceptualization of the right to privacy and a different desire for control.

Moreover, this dissertation provides multiple insights into employees' perceptions of data sensitivity and willingness to disclose personal data in employment. Specifically, it highlights the uniqueness of the employment context compared to other contexts and breaks down the multi-dimensionality of employees' perceptions of personal data. As a result, the dimensions in which employees perceive data are presented, and differences among employees are highlighted. This is complemented by identifying personal characteristics and attitudes toward employers, as well as toward the right to privacy, that influence these perceptions.

Furthermore, this dissertation provides insights into practical aspects for the implementation of personal data management solutions to safeguard employee privacy. Specifically, it presents the results of a user-centered design study with employees who process

personal data of other employees as part of their job. Based on the results obtained, a privacy pattern is presented that harmonizes privacy obligations with personal data processing activities. The pattern is useful for designing privacy controls that help these employees handle employee personal data in a privacy-compliant manner, taking into account their skills and knowledge, thus helping to protect employee privacy.

The outcome of this dissertation benefits a wide range of stakeholders who are involved in the protection of employee privacy. For example, it highlights the challenges to be considered by employers and software engineers when conceptualizing and designing employee-centric privacy controls. Policymakers and researchers gain a better understanding of employees' perceptions of privacy and obtain fundamental knowledge for future research into theoretical and abstract concepts or practical issues of employee privacy. Employers, IT engineers, and researchers gain insights into ways to empower data processing employees to handle employee personal data in a privacy-compliant manner, enabling employers to improve and promote compliance. Since the basic principles underlying informational self-determination have been incorporated into European privacy legislation, we are confident that our results are also of relevance to stakeholders outside Germany.



## ZUSAMMENFASSUNG

---

Die Verarbeitung personenbezogener Daten von Beschäftigten nimmt erheblich zu. Um das Grundrecht auf Privatheit zu schützen, sieht der Gesetzgeber die Implementierung von Datenschutzmaßnahmen inklusive Transparenz und Intervention vor. Gegenwärtig mangelt es den für die Umsetzung verantwortlichen Akteuren, wie Arbeitgebenden und Software-Ingenieurinnen und -Ingenieuren, jedoch schlichtweg an Grundlagenwissen, um die notwendigen Maßnahmen zu konzipieren und zu implementieren. Tatsächlich hat sich die Privatheitsforschung bisher hauptsächlich auf Beziehungen im privaten Kontext von Verbraucherinnen und Verbrauchern konzentriert. Im Gegensatz dazu ist Privatheit im Beschäftigungskontext weniger gut untersucht. Da Privatheit in hohem Maße kontextabhängig ist, können vorhandene Kenntnisse und Datenschutzmaßnahmen aus anderen Kontexten jedoch nicht einfach auf den Beschäftigungskontext übertragen werden. Insbesondere unterliegt die Privatheit im Beschäftigtenkontext abweichenden rechtlichen und sozialen Normen, die eine andere Konzeptualisierung des Rechts auf Privatheit erfordern, als dies in anderen Kontexten üblich ist. Um diesen Besonderheiten gerecht zu werden, besteht ein breiter Konsens darüber, dass Privatheit als sozio-technisches Konzept betrachtet werden muss, bei dem neben den technisch-rechtlichen Faktoren immer auch menschliche Faktoren berücksichtigt werden müssen. Derzeit mangelt es jedoch insbesondere an Wissen über menschliche Faktoren zur Privatheit im Beschäftigtenkontext. Die Außerachtlassung der Bedürfnisse und Anliegen von Individuen oder mangelnde Benutzerfreundlichkeit sind jedoch häufige Gründe für das Scheitern von Datenschutz- und Sicherheitsmaßnahmen in der Praxis.

Diese Dissertation adressiert zentrale Wissenslücken zu menschlichen Faktoren im Beschäftigtendatenschutz, indem sie die Ergebnisse von insgesamt drei Studien mit Beschäftigten in Deutschland vorstellt. Die Ergebnisse geben Aufschluss über ihre Wahrnehmung des Rechts auf Privatheit sowie über ihre Wahrnehmungen und Erwartungen an die Verarbeitung personenbezogener Daten. Die gewonnenen Erkenntnisse bilden eine Grundlage für die menschenzentrierte Gestaltung und Umsetzung von Datenschutzmaßnahmen im Beschäftigtenkontext, d.h. von Datenschutzmaßnahmen, die die Sichtweisen, Erwartungen und Fähigkeiten von Beschäftigten einbeziehen.

Konkret werden in dieser Dissertation erstmals mentale Modelle von Beschäftigten zum Recht auf informationelle Selbstbestimmung, dem deutschen Pendant zum Recht auf Privatheit, vorgestellt. Die Ergebnisse geben Aufschluss über (1) die Wahrnehmung von Kategorien von Daten, (2) die Vertrautheit mit und die Erwartungen an das Recht auf Privatheit und (3) die Wahrnehmung von Datenverarbeitung, Datenfluss, Schutzmaßnahmen und Bedrohungsmodellen. Darüber hinaus werden drei Haupttypen von mentalen Modellen vorgestellt, die jeweils andere Konzeptualisierungen des Rechts auf Privatheit und unterschiedliche Bedürfnisse für Datenschutzmaßnahmen beinhalten.

Darüber hinaus bietet diese Dissertation vielfältige Einblicke in die Wahrnehmung der Datensensibilität und die Bereitschaft von Beschäftigten, personenbezogene Daten im Rahmen ihrer Beschäftigung preiszugeben. Insbesondere wird die Einzigartigkeit des Beschäftigungskontextes im Vergleich zu anderen Kontexten hervorgehoben und die Mehrdimensionalität der Wahrnehmung personenbezogener Daten aufgeschlüsselt. In-

folgedessen werden die Dimensionen, in denen Beschäftigte Daten wahrnehmen, dargestellt und die Unterschiede hervorgehoben. Ergänzend dazu werden persönliche Merkmale und Einstellungen gegenüber Arbeitgebenden sowie dem Recht auf Privatheit identifiziert, die diese Wahrnehmungen beeinflussen.

Des Weiteren gibt diese Dissertation Einblicke in die praktische Umsetzung von Datenmanagementlösungen die den Schutz der Privatheit von Beschäftigten fördern. Konkret werden die Ergebnisse einer nutzerzentrierten Designstudie mit Beschäftigten vorgestellt, die im Rahmen ihrer Tätigkeit personenbezogene Daten anderer Beschäftigter verarbeiten. Auf der Grundlage der gewonnenen Ergebnisse wird ein Datenschutzmuster vorgestellt, das die Datenschutzverpflichtungen mit den Aktivitäten zur Verarbeitung personenbezogener Daten in Einklang bringt. Das Datenschutzmuster ist nützlich für die Gestaltung von Datenschutzmaßnahmen, die die Fähigkeiten und Kenntnisse dieser Beschäftigten berücksichtigen, um sie in der datenschutzkonformen Verarbeitung zu unterstützen und so zum Beschäftigtendatenschutz beizutragen. Die Ergebnisse dieser Dissertation kommen einer Vielzahl von Akteuren zugute, die mit dem Beschäftigtendatenschutz befasst sind. Zum Beispiel werden die Herausforderungen aufgezeigt, die von Arbeitgebenden und Software-Ingenieurinnen und -Ingenieuren bei der Konzeption und Gestaltung von mitarbeiterzentrierten Datenschutzkontrollen zu berücksichtigen sind. Politische Entscheidungsträgerinnen und -träger sowie Forscherinnen und Forscher gewinnen ein besseres Verständnis für die Wahrnehmung der Privatheit durch die Beschäftigten und erhalten Grundlagenwissen für die künftige Erforschung theoretischer und abstrakter Konzepte oder praktischer Fragen des Beschäftigtendatenschutzes. Arbeitgebende, IT-Ingenieurinnen und -Ingenieure sowie Forscherinnen und Forscher erhalten Einblicke in die Möglichkeiten, wie datenverarbeitende Mitarbeitende befähigt werden können, mit personenbezogenen Daten von Arbeitnehmenden datenschutzkonform umzugehen, sodass Arbeitgebende die Einhaltung der Vorschriften verbessern und fördern können. Da die Grundprinzipien der informationellen Selbstbestimmung Eingang in die europäische Datenschutzgesetzgebung gefunden haben, sind wir zuversichtlich, dass unsere Ergebnisse auch für Akteure außerhalb Deutschlands von Bedeutung sind.

*Not the lucky ones are grateful.  
It is the grateful ones who are happy.*  
— (loosely based on) Francis Bacon

## ACKNOWLEDGMENTS

---

First, I would like to thank the members of my thesis advisory committee, Prof. Dr.-Ing. Delphine Reinhardt, Prof. Dr.-Ing. Luigi Lo Iacono, and Prof. Dr. phil.-nat. Jens Grabowski for supervising my dissertation project and providing valuable feedback on my research. I am grateful to Prof. Dr.-Ing. Luigi Lo Iacono for offering me the opportunity to do a doctorate, and for always encouraging and pushing me with the greatest commitment. I thank you for your trust, your solution-oriented thinking, and your sense of responsibility towards your employees. I further thank Prof. Dr.-Ing. Delphine Reinhardt for the big leap of faith when she accepted me as an external PhD student in her research group. I thank you for the close and trustful collaboration, as well as for your constant guidance and support despite the distance. I strongly appreciated your structured way of working, and your eye for simplicity and details.

Moreover, I thank my co-workers of the Data and Application Security Group in Cologne and Sankt Augustin for their support, their input, and their feedback on my research. In particular, I would like to thank my long-time project colleague Florian Dehling for the trustful and reliable teamwork, his tireless commitment and support, and especially our great and yet sometimes tough discussions to always critically reflect our actions and conclusions. I also thank my fellow students of the Computer Security and Privacy Research Group in Göttingen for their input and feedback on my presentations and the many discussions and conversations about all sorts of things that broadened my mind. Furthermore, I thank my co-authors, co-researchers, and generally all supporters of my research for their contributions. Special thanks go to Svenja Polst and Hartmut Schmitt for helping to conduct interviews, and Graham Ashcroft, Ph.D., for helping translate participants' statements. A big thank you also to the research consortium of the project "TrUSD – Transparente und selbstbestimmte Gestaltung der Datennutzung im Unternehmen". Thank you for your valuable input in the form of reports, discussions, reviews, and assistance in conducting studies. In this regard, I also thank the taxpayers of Germany and the German Federal Ministry of Education and Research for funding my research.

Many thanks also to the study participants, especially to the staff of the participating organizations, for the many hours of valuable support they provided over such a long period of time next to their regular job. Furthermore, I would like to thank the many unknown reviewers of my submissions and publications for providing me with much valuable feedback to improve my research and presentation of results.

Last but not least, I would like to express my sincere thanks to my parents, my sisters, and my friends for supporting me on this journey. Thank you for your love, encouragement, and support in the times of celebration and joy, but especially in the times of stress and strain.



## CONTENTS

---

1	INTRODUCTION	1
1.1	Motivation . . . . .	1
1.2	Objectives . . . . .	3
1.3	Methodology . . . . .	4
1.4	Contributions . . . . .	5
1.4.1	Employee mental models of privacy and the right to informational self-determination . . . . .	5
1.4.2	Empirical evidence of employee privacy perceptions . . . . .	6
1.4.3	Data Cart: A privacy pattern for the GDPR-compliant handling of personal data by employees . . . . .	7
1.5	Impact . . . . .	8
1.5.1	Generation of fundamental knowledge about human factors in employee privacy . . . . .	8
1.5.2	Design of practical and usable privacy controls for data processing employees . . . . .	9
1.5.3	Further impact . . . . .	9
1.6	Dissertation outline . . . . .	10
2	FOUNDATIONS	13
2.1	Information privacy . . . . .	13
2.2	Legal foundations and privacy definition . . . . .	15
2.2.1	Definition of the right to privacy as informational self-determination	17
2.2.2	Key stakeholders in employee privacy . . . . .	20
2.2.3	Definitions of data and information concerned . . . . .	23
2.2.4	Objectives, principles, and provisions of privacy legislation . . . . .	26
2.2.5	Rights of data subjects and employees . . . . .	28
2.3	Privacy engineering . . . . .	29
2.3.1	Privacy and data protection by design & by default . . . . .	30
2.3.2	Engineering processes, activities, and tasks . . . . .	31
2.3.3	Privacy and transparency enhancing technologies . . . . .	34
2.3.4	Privacy (design) patterns . . . . .	34
2.4	Human-centric privacy research . . . . .	35
2.4.1	Human-centered design . . . . .	36
2.4.2	Usable privacy . . . . .	37
2.4.3	Mental models . . . . .	38
2.4.4	Privacy macro models . . . . .	39
2.5	Summary . . . . .	41
3	INFORMATION PRIVACY IN EMPLOYMENT: A LITERATURE SURVEY	43
3.1	Literature review procedure . . . . .	43
3.2	Topics of employee information privacy . . . . .	44
3.2.1	Information system use . . . . .	44
3.2.2	Information privacy perceptions . . . . .	46
3.2.3	Job application . . . . .	47
3.2.4	Workplace monitoring and surveillance . . . . .	48

3.2.5	Privacy engineering . . . . .	48
3.3	Methodologies, sampling, and participants . . . . .	50
3.3.1	Methods . . . . .	51
3.3.2	Study samples . . . . .	51
3.3.3	Study participants . . . . .	53
3.4	Demarcation of this dissertation . . . . .	53
3.4.1	Privacy as a determinant to employee acceptance . . . . .	53
3.4.2	Conceptualizing privacy as an opt-out right . . . . .	53
3.4.3	Privacy implementation . . . . .	54
3.5	Summary . . . . .	55
4	PROBLEM STATEMENT AND RESEARCH QUESTIONS . . . . .	57
4.1	Employees' conceptualizations of modern and Eurocentric privacy . . . . .	57
4.1.1	Internal conceptualizations of informational self-determination . . . . .	58
4.1.2	Privacy perceptions of personal data . . . . .	59
4.2	Data processing employees as levers for employee privacy . . . . .	61
4.3	Summary . . . . .	62
5	STUDY I — EMPLOYEES' CONCEPTUALIZATIONS OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION . . . . .	63
5.1	Background and research model . . . . .	63
5.1.1	Perceptions of categories of data and terminology . . . . .	63
5.1.2	Concepts of informational self-determination . . . . .	64
5.1.3	Awareness and perception of personal data processing . . . . .	64
5.2	Methodology . . . . .	65
5.2.1	Ethical considerations of the study . . . . .	65
5.2.2	Method selection . . . . .	66
5.2.3	Interview guideline design . . . . .	66
5.2.4	Study procedure . . . . .	68
5.2.5	Participant recruitment and enrollment . . . . .	69
5.2.6	Participant demographics . . . . .	69
5.2.7	Evaluation and data analysis . . . . .	70
5.3	Perceptions of categories of data . . . . .	72
5.3.1	Employees' definitions of categories of data . . . . .	72
5.3.2	Identified themes of categories of data . . . . .	74
5.3.3	Discussion . . . . .	75
5.4	Conceptualizations of informational self-determination . . . . .	76
5.4.1	Objectives . . . . .	76
5.4.2	Self-determination . . . . .	77
5.4.3	Transparency . . . . .	77
5.4.4	Restrictions and issues . . . . .	77
5.4.5	Clusters of mental models . . . . .	79
5.4.6	Discussion . . . . .	80
5.5	Perceptions and awareness of personal data processing . . . . .	82
5.5.1	Self-disclosure . . . . .	82
5.5.2	Personal data flow . . . . .	83
5.5.3	Privacy safeguards . . . . .	84
5.5.4	Privacy threats . . . . .	85
5.5.5	Invasion of privacy . . . . .	86

5.5.6	Discussion . . . . .	87
5.6	Implications . . . . .	88
5.6.1	Notice and transparency . . . . .	89
5.6.2	Control and intervention abilities . . . . .	90
5.6.3	Awareness . . . . .	90
5.6.4	Implications for research . . . . .	91
5.7	Study limitations . . . . .	91
5.8	Summary . . . . .	92
6	STUDY II — DETERMINANTS AND DIFFERENCES OF EMPLOYEES' PERCEPTIONS OF PERSONAL DATA . . . . .	93
6.1	Background and research model . . . . .	93
6.1.1	Differences in the perception of personal data . . . . .	93
6.1.2	Antecedents and causal model . . . . .	95
6.1.3	Employee groups and clusters . . . . .	98
6.2	Methodology . . . . .	98
6.2.1	Ethical considerations of the study . . . . .	99
6.2.2	Measurement instrument . . . . .	99
6.2.3	Study procedure . . . . .	100
6.2.4	Participant recruitment and enrollment . . . . .	100
6.2.5	Participant demographics . . . . .	101
6.2.6	Evaluation and data analysis . . . . .	101
6.3	Employees' perceived data sensitivity and willingness to disclose . . . . .	105
6.3.1	Descriptive results . . . . .	105
6.3.2	Contextual differences . . . . .	106
6.3.3	Discussion . . . . .	109
6.4	Groups of personal data . . . . .	110
6.4.1	Identification of latent groups of personal data . . . . .	110
6.4.2	Differences in sensitivity and willingness to disclose . . . . .	112
6.4.3	Discussion . . . . .	115
6.5	Antecedents and causal model . . . . .	116
6.5.1	Determinants of data sensitivity and willingness to disclose . . . . .	116
6.5.2	Effects of employee disposition to privacy . . . . .	122
6.5.3	Discussion . . . . .	124
6.6	Differences in employees' perceptions of personal data . . . . .	126
6.6.1	Clusters of employees . . . . .	126
6.6.2	Discussion . . . . .	128
6.7	Implications . . . . .	129
6.7.1	Consideration of contextual factors . . . . .	130
6.7.2	Classification of personal data . . . . .	130
6.7.3	Implementation of privacy controls . . . . .	131
6.7.4	Studying employee privacy perceptions . . . . .	132
6.8	Study limitations . . . . .	132
6.9	Summary . . . . .	133
7	STUDY III — DATA CART: A PRIVACY PATTERN FOR THE GDPR-COMPLIANT HANDLING OF EMPLOYEE PERSONAL DATA . . . . .	135
7.1	Background and research model . . . . .	135
7.2	Methodology . . . . .	136

7.2.1	Ethical considerations of the study . . . . .	137
7.2.2	Study procedure . . . . .	137
7.2.3	Participant recruitment and enrollment . . . . .	140
7.2.4	Participant demographics . . . . .	140
7.2.5	Evaluation and data analysis . . . . .	141
7.3	Privacy requirements for the handling of employee personal data . . . . .	142
7.3.1	Legal considerations . . . . .	143
7.3.2	Stakeholder needs for personal data processing . . . . .	144
7.3.3	Stakeholder needs for data protection . . . . .	145
7.3.4	Requirements for employee-centric (re)design of privacy controls . . . . .	145
7.4	Solution design . . . . .	148
7.4.1	Data cart metaphor . . . . .	148
7.4.2	Privacy pattern proposal . . . . .	149
7.4.3	Process flow model . . . . .	150
7.4.4	Interaction concept . . . . .	153
7.5	Prototype development . . . . .	155
7.6	Usability properties . . . . .	156
7.6.1	Metaphor and concept understanding . . . . .	156
7.6.2	Participant feedback and usability rating . . . . .	156
7.6.3	Identified problems . . . . .	158
7.7	Employee perceptions of Data Cart . . . . .	158
7.7.1	Digitalization and efficiency gains . . . . .	158
7.7.2	Data protection . . . . .	160
7.7.3	General concerns . . . . .	162
7.8	Discussion . . . . .	162
7.9	Study limitations . . . . .	164
7.10	Summary . . . . .	166
8	CONCLUSION . . . . .	167
8.1	Summary . . . . .	167
8.2	Limitations and outlook . . . . .	168
	BIBLIOGRAPHY . . . . .	171
A	APPENDIX LITERATURE SURVEY . . . . .	203
B	APPENDIX STUDY I . . . . .	225
B.1	Study I — Interview outline (translated) . . . . .	225
C	APPENDIX STUDY II . . . . .	229
C.1	Study II — Items and questions (translated) . . . . .	229
C.2	Study II — Analysis environment . . . . .	234
C.3	Study II — Participant demographics . . . . .	235
C.4	Study II — Personal data elements and groups of personal data . . . . .	239
C.5	Study II — Demographic differences privacy antecedents . . . . .	242
C.6	Study II — Covariates SEM analysis . . . . .	244
D	APPENDIX STUDY III . . . . .	247
D.1	Study III — Protocol Study 2: User goals and requirements (translated) . . . . .	247
D.2	Study III — Protocol Study 3: Usability walkthrough (translated) . . . . .	249
D.3	Study III — Protocol Study 4: Formative usability study (translated) . . . . .	252
D.4	Study III — Non-functional requirements . . . . .	255



D.5 Study III — Screenshots Data Cart prototype (translated) . . . . .	256
--	-----

## LIST OF FIGURES

Figure 1.1	Simplified schematic representation of the processing of employee personal data, as well as the implementation of the right to privacy in the employment context . . . . .	2
Figure 2.1	Basic legal framework and complementary laws for employee privacy . . . . .	17
Figure 2.2	Stakeholder map of the GDPR with a mapping to entities in the employment context . . . . .	21
Figure 3.1	Quantification of identified methods, samples, and participants in employee privacy research . . . . .	51
Figure 3.2	Cross table of method and analysis used in related work . . . . .	52
Figure 3.3	Cross table of sample and topic in employee privacy research . . . . .	52
Figure 5.1	Expert model of the right to informational self-determination in employment . . . . .	67
Figure 5.2	Identified coding themes of categories of data . . . . .	75
Figure 5.3	Identified themes of informational self-determination in employment . . . . .	78
Figure 5.4	Conceptualizations of identified safeguards for employee privacy . . . . .	84
Figure 5.5	Conceptualizations of identified threat models for employee privacy . . . . .	86
Figure 6.1	Summary research objectives and research questions in Study II . . . . .	94
Figure 6.2	Anticipated causal model of antecedents for perceived data sensitivity and willingness to disclose in the employment context . . . . .	96
Figure 6.3	Model for examining effects of employees' dispositions to a right to privacy on privacy antecedents . . . . .	98
Figure 6.4	Descriptive results perceived data sensitivity and willingness to disclose . . . . .	107
Figure 6.5	Changes in the rank order of personal data . . . . .	108
Figure 6.6	Pairwise rank correlations of perceived data sensitivity of the same set of personal data items investigated in different studies with varying contexts and cultural backgrounds . . . . .	109
Figure 6.7	Robust LMM's fixed effects for different groups of personal data . . . . .	114
Figure 6.8	SEM models summarizing privacy antecedents' inter-effects and effects on perceived data sensitivity and willingness to disclose . . . . .	119
Figure 6.9	Effects of employees' disposition to privacy as a right . . . . .	123
Figure 6.10	Employee clusters differences for various groups of personal data . . . . .	127
Figure 7.1	User-centered design approach and development process. . . . .	138
Figure 7.2	Summary stakeholder job profiles, job tasks, and (personal) data processed . . . . .	141
Figure 7.3	Flow of the concept developed using the metaphor of a data cart . . . . .	151
Figure 7.4	Process flow diagram of the concept developed using the metaphor of a data cart . . . . .	152
Figure 7.5	Basic interaction concept of <i>Data Cart</i> . . . . .	154
Figure 7.6	Screenshot <i>Data Cart</i> personal data management interface . . . . .	157
Figure D.1	Screenshot <i>Data Cart</i> landing page . . . . .	256

Figure D.2	Screenshot <i>Data Cart</i> processing activity selection . . . . .	257
Figure D.3	Screenshot <i>Data Cart</i> tuple specification . . . . .	258
Figure D.4	Screenshot <i>Data Cart</i> request customization . . . . .	259
Figure D.5	Screenshot <i>Data Cart</i> request verification . . . . .	260
Figure D.6	Screenshot <i>Data Cart</i> personal data management interface . . . . .	261

## LIST OF TABLES

Table 2.1	Mapping of privacy engineering activities and tasks to the systems engineering life cycle processes according to ISO/IEC TR 27550, focusing employee privacy . . . . .	32
Table 5.1	Study I - Participant demographics . . . . .	71
Table 6.1	Study II - Participant demographics summary . . . . .	102
Table 6.2	Study II - Latent groups of personal data and results of CFA for WTD and PDS . . . . .	111
Table 6.3	Study II - Groups of personal data examined . . . . .	113
Table 6.4	Study II - Results robust LMMs with random effects by participants	114
Table 6.5	Study II - Summary of variables used in SEM analysis . . . . .	117
Table 6.6	Study II - Construct reliability measures, validity measure, and correlations . . . . .	118
Table 6.7	Study II - Results SEM analysis non-latent groups of personal data	120
Table 6.8	Study II - Results SEM analysis latent groups of personal data . .	121
Table 6.9	Study II - Results SEM analysis antecedents . . . . .	122
Table 6.10	Study II - Results SEM analysis employee disposition to privacy .	124
Table 6.11	Study II - Comparison of the fit of different solutions for latent class analysis . . . . .	126
Table 7.1	Study III - Participant demographics . . . . .	142
Table 7.2	Study III - List of stakeholder requirements . . . . .	147
Table 7.3	Study III - Summary of themes related to digitalization and efficiency gains . . . . .	159
Table 7.4	Study III - Summary of themes related to data protection . . . . .	160
Table 7.5	Study III - Summary of themes related to general concerns . . . .	162
Table A.1	Literature review summary . . . . .	204
Table C.1	Study II - R packages used for analysis . . . . .	234
Table C.2	Study II - Participants' complete demographic data . . . . .	235
Table C.3	Study II - Comparison of different studies and personal data items	240
Table C.4	Study II - Personal data elements' average scores in different studies and assignment to different groups of personal data. . . . .	241
Table C.5	Study II - Results Kruskal-Wallis test demographic differences by privacy antecedents . . . . .	242
Table C.6	Study II - Results covariates analysis of demographic differences by privacy antecedents . . . . .	243
Table C.7	Study II - Results SEM analysis demographic variables . . . . .	245

## LIST OF ACRONYMS AND ABBREVIATIONS

---

AC2	Gwen's Gamma
APCO	"Antecedents → Privacy Concerns → Outcomes"
APPI	Act on the Protection of Personal Information
AVE	Average Variance Extracted
BDSG	Federal Data Protection Act
BetrVG	Works Constitutions Act
BfDI	Federal Commissioner for Data Protection and Freedom of Information
BVerfGE	Federal Constitutional Court
BYOD	Bring Your Own Device
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CFIP	Concern for Information Privacy
CI	Confidence Interval
CPM	Communication Privacy Management
CPRA	California Privacy Rights Act
CSP	Control-Seeking Pragmatist
DFCP	Data-Flow Concerned Protectionist
DPO	Data Protection Officer
EFA	Exploratory Factor Analysis
ESN	Enterprise Social Network
EU	European Union
FIP	Fair Information Practice
GDPR	General Data Protection Regulation
GFI	Goodness of Fit
HCD	Human-Centered Design
HCI	Human Computer Interaction
HR	Human Resources
HTMT	Heterotrait-Monotrait Ratio of Correlation
JIF	Journal Impact Factor
IRA	Inter-Rater Agreement
IUIPC	Internet Users' Information Privacy Concerns
LCA	Latent Class Analysis
LD SG	State Data Protection Act

LfD	State Commissioner for Data Protection
LGPD	General Data Protection Law
LMM	Linear Mixed-effects Model
MIMIC	Multiple Indicators and Multiple Causes
OSN	Online Social Network
OECD	Organization for Economic Cooperation
PbD	Privacy by Design
PET	Privacy Enhancing Technology
PII	Personally Identifiable Information
PD	Privacy Doctrinairist
PDS	Perceived Data Sensitivity
RBAC	Role-Based Access Control
RMSEA	Root Mean Square Error of Approximation
SEM	Structural Equation Modeling
SUS	System Usability Scale
TAM	Technology Acceptance Model
TET	Transparency Enhancing Technology
TOM	Technical and Organizational Measure
UI	User Interface
UCD	User-Centered Design
UTAUT	Unified Theory of Acceptance and Use of Technology
WLSMV	Weighted Least Square Mean and Variance Adjusted
WTD	Willingness to Disclose

## INTRODUCTION

---

*To unravel any mystery, find the start.  
Untie that riddle, and the rest will follow.*

— Alyssa Moon

### 1.1 MOTIVATION

The fundamental right to privacy applies to all situations and contexts in life, including the employment context. Privacy in Germany is tantamount to the right to informational self-determination, which guarantees individuals transparency and control over the collection, use, and disclosure of their personal data [1]. Its actual implementation in the employment context is primarily subject to the same strict rules of European and national privacy law that applies to non-employment contexts. At the same time, however, privacy in employment differs significantly from other contexts, as employees can hardly escape the processing of their personal data and privacy is also shaped by both national labor law and special regulations. In Germany, for legal and formal reasons alone, the disclosure of, e.g., church membership and social security numbers for tax and social welfare contributions, as well as detailed curricula vitae, is mandatory. In times of the COVID-19 pandemic, the German Infection Protection Act also required employees to disclose their vaccination status to their employer (§ 36 (3)). Beyond that, the ongoing digital transformation is also inevitably expanding the disclosure and processing of employee personal data to include, among other things, mobile working [2], the use of wearables [3], and the use of analytics and monitoring [4].

In this regard, potential privacy management strategies known from the private context, such as not disclosing personal data or refusing to use information systems, are not viable options for employees. Instead, they must accept limited self-determination abilities, in particular the limited ability to decide on the nature and scope of personal data processing, when law or employer interests outweigh employees' privacy interests. As a result, privacy and labor laws aim to enforce adequate privacy protection by making the different entities involved jointly responsible. To this end, the law essentially makes employers accountable for protecting employees' privacy. Thus, employers must ensure that the foundational principles of employee privacy law are respected in the processing of employee personal data. As outlined in Figure 1.1, this entails obligations to implement numerous rights of data subjects and ensure that these rights can be exercised by employees. In addition, employers must implement Technical and Organizational Measures (TOMs) to ensure and demonstrate compliance with privacy law. Consequently, employers have to ensure that employees who process personal data of other employees on their behalf may only do so using those TOMs and only if instructed to do so. For enforcement, the law provides for severe sanctions in the event of misconduct by employers and data processing employees. Indeed, employers have already been sentenced to heavy fines if they failed to implement data subject rights or did not adequately protect their employees' personal data [5].

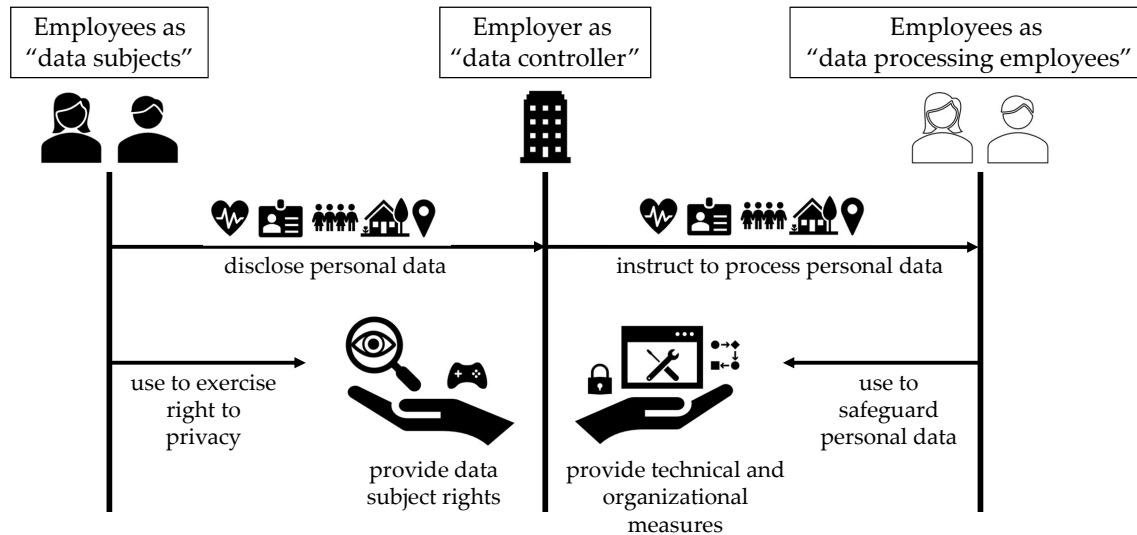


Figure 1.1: Simplified schematic representation of the processing of employee personal data, as well as the implementation of the right to privacy in the employment context.

In practice, the challenge is to translate the abstract principles and obligations stipulated in privacy and labor law into practical tools, measures, and processes [6, 7]. For this purpose, privacy engineering frameworks and tools exist today to assist software engineers, practitioners, and researchers in the various phases of analyzing and operationalizing privacy requirements, designing solutions, and evaluating them [7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17]. Central to all these approaches is their consideration of human factors, treating privacy as a socio-technical matter in which legal and technical requirements must be consolidated with the requirements of individuals. This includes not only respecting the Human Computer Interaction (HCI) implications arising from privacy and data protection principles [12, 16, 18, 19], but also incorporating theoretical and abstract privacy concepts throughout the privacy engineering process [8, 10, 13, 15, 20]. When applied to the implementation of data subject rights and TOMs in the employment context, this means that they must be designed in an employee-centric manner [21], i.e., take into account employees' strengths, limitations, preferences, and expectations towards privacy and personal data management, as well as meet usability criteria [22], i.e., protect employee privacy in an effective, efficient, and satisfactory manner. This necessitates a thorough understanding of employees' conceptualizations of privacy, e.g., their privacy interests, concerns, awareness, objectives, and perceptions of personal data processing [10, 12, 15, 16, 19, 23, 24]. To date, however, such insights are largely lacking for the employment context [25]. But since privacy is known to be a contextual concept [26, 27, 28], knowledge from contexts other than employment cannot be relied on. As a result, employers, researchers, and software engineers simply lack the fundamental knowledge necessary to, e.g., conduct an appropriate risk analysis or make implementation decisions for data subjects' rights and TOMs that address all stakeholders' privacy expectations, capabilities, and concerns [9]. Thus, potential privacy risks related to, e.g., unawareness and non-compliance [29] cannot be adequately addressed, potentially leading to a loss of employees' self-determination and trust [9, 10].



## 1.2 OBJECTIVES

This dissertation addresses prevailing gaps in knowledge and research on human factors in information privacy in employment. Its outcome is intended to enable stakeholders involved in privacy research and privacy engineering to develop employee-centric privacy controls under contemporary privacy law. The current state of research in this regard is insufficient in several respects. Firstly, previous work on privacy issues in employment has mostly focused on aspects of information system use [2, 3, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48], workplace monitoring and surveillance [4, 49, 50, 51, 52, 53, 54, 55, 56, 57], and on employee recruitment [58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70]. Their emphasis was on investigating (adverse) behavioral effects and developing remedial strategies to make sure (1) that employees accept new information systems, (2) that employees' work performance is not affected by monitoring activities, and (3) that organizations do not lose applicants due to privacy invasive recruiting strategies. Moreover, previous work that concerns theoretical and abstract privacy concepts is subject to enormous cultural bias from the U.S., and is largely from the 1980s to the 2010s, thus significantly predating modern privacy law and state-of-the-art information systems [71, 72, 73, 74, 75, 76, 77, 78, 79, 80]. As a result, previous work has focused on the U.S. view of privacy as the right to freedom from intrusion [81], which is largely incompatible with the European view of privacy that is more strongly embedded in the right to informational self-determination [81, 82, 83]. Consequently, these results must be interpreted with caution and are not easily transferable to regions other than the U.S. due to the contextual nature of privacy [26, 27, 28]. Furthermore, previous work targeting privacy engineering and privacy controls has focused on aspects of technical measures centered around both data minimization and anonymization that, however, ignored human factors [84, 85, 86, 87, 88, 89, 90, 91], or proposed employment specific design principles based on work from non-employment contexts [92, 93, 94]. Only few studies developed user-centered tools to exercise data subject rights [95, 96, 97] or manage privacy policies [98].

Unlike previous work, this dissertation does not consider privacy as a secondary factor for the acceptance of particular information systems and employer practices, but focuses on the concrete implementation and design of the right to privacy in employment. To counteract the aforementioned bias of previous work, this dissertation aims to provide contemporary and Eurocentric insights by focusing on Germany and the right to informational self-determination. This focus is intended to provide findings of high practical relevance for the implementation of employee privacy, which, taking into account cultural and legal differences, may also serve other European countries. The goal is to gain fundamental knowledge about employees' conceptualizations of the right to privacy and their perceptions of the processing of personal data in the employment relationship. The resulting knowledge will be useful to, e.g., employers, researchers, and software engineers for implementing data subject rights and TOMs, as well as privacy-friendly information systems and business processes that respect the socio-technical nature of employee privacy. Employees are expected to benefit from the design of solutions that support their privacy goals and capabilities.

Moreover, regarding previous work on specific privacy controls, this dissertation complements it by focusing on the key role of data processing employees in protecting employee privacy. The goal is to develop a usable personal data management solution

that helps data processing employees in the privacy-compliant processing of employee personal data, thereby contributing to the protection of employee privacy. The solution may serve software engineers and designers as a pattern for their own solutions [9]. Employers are expected to benefit by means of higher compliance.

In summary, this dissertation has two specific objectives:

- ▷ To provide fundamental knowledge about employees' conceptualizations of the right to privacy, including their perceptions, attitudes, desires, and knowledge regarding personal data processing and privacy in the employment context, taking into account factual privacy law and the specifics of the employment context under the right to informational self-determination.
- ▷ To develop feasible and usable privacy management solutions that support data processing employees in handling employee personal data in a privacy-compliant manner, and thus assist them in maintaining employee privacy. The solution is intended to support employers in meeting their obligations to implement data subject rights as well as technical and organizational measures.

### 1.3 METHODOLOGY

To achieve the aforementioned research objectives, we<sup>1</sup> first familiarized ourselves with both the legal regulatory setting and the research literature on employee privacy. For the former, we examined legal texts, judgments, and the legal literature on privacy and labor law in employment relationships in the European Union (EU) and in Germany in particular. For the latter, we then conducted a systematic literature review on employee information privacy to identify research gaps as well as study designs that would help fill such research gaps. Next, we divided our research into two thematic blocks. In the first block, we pursued the generation of fundamental knowledge about human factors in employee privacy in order to provide a foundation for future privacy research and privacy engineering in the employment context under contemporary and European-oriented privacy perspectives. In the second block, we addressed the design and development of practical and usable privacy controls tailored to the needs of data-processing employees to assist them in processing employees' personal data in a privacy-compliant manner, thereby serving employers' accountability obligations.

**GENERATION OF FUNDAMENTAL KNOWLEDGE** Based on the research gaps identified, we designed two studies to generate fundamental knowledge about human factors in employee privacy. In Study I, we conducted a qualitative interview study with 27 employees to elicit their conceptualizations of personal data processing in the employment context, with a particular emphasis on the right to informational self-determination. The results were evaluated and documented using appropriate analysis methods and tools from HCI. In Study II, we conducted a quantitative study with 553 employees, in which we elicited employees' willingness to disclose personal data and their perceived data sensitivity to investigate differences in employees' privacy perceptions. In addition, we

<sup>1</sup> Note that we refer to "we/us/our" as contributions made indifferently by either the author of this thesis or supported by others to ease the reading. A detailed overview of this dissertation's author's individual contributions is available in Section 1.5, though.

examined effects of privacy antecedents, including factors that we identified in Study I. The results were analyzed and documented using appropriate analytical methods from empirical social science and information systems.

We only recruited employees from Germany for both studies because regulatory differences in employment contexts do not allow us to mix participants without jeopardizing the validity of the results. Yet, we took care to balance the ratio of employees in their role as data subjects and data processing employees in both studies to account for potential differences in perceptions of privacy. For each study, we discussed our findings in terms of their significance for science, their meaning in terms of the legal framework, and their practical relevance. We then highlighted key implications for future research and, in particular, for the engineering of employee-centric privacy controls.

**DESIGN OF PRACTICAL AND USABLE PRIVACY CONTROLS** To design privacy controls for the privacy-compliant processing of employee-personal data, we conducted a User-Centered Design (UCD) study with 19 data processing employees of two public institutions in Germany. Due to the nature of a UCD study being extensive, it ran over the entire PhD project alongside the studies in the first block. Where appropriate, we used the knowledge gained in the first block to inform design decisions in later phases of the UCD study. As a result, we developed *Data Cart*, a privacy pattern consisting of a process model and interaction concept to provide a single point of access for data processing employees to obtain and manage employee personal data in a privacy-compliant manner. We investigated *Data Cart*'s feasibility and usability through multiple evaluations, including focus groups, usability walkthroughs, and formative usability testing. To this end, we eventually developed a high-fidelity "Wizard-of-Oz" prototype. We used realistic conditions as a basis in the development and in all evaluations.

## 1.4 CONTRIBUTIONS

We address the identified research gaps regarding fundamental knowledge about human factors in employee privacy, as well as research gaps on the development of practical and usable privacy controls for data processing employees, by making the following contributions, described in the sections below.

### 1.4.1 *Employee mental models of privacy and the right to informational self-determination*

We present employees' mental models of privacy in employment and, in particular, of the right to informational self-determination in employment. Our research contributes to the body of knowledge in several ways:

(1) We present preliminary insights into employees' conceptualizations of (the right to) privacy in employment under contemporary privacy law. First, we reveal ambiguity and lack of clarity in terminology rooted in privacy legislation, even for employees familiar with personal data processing. Nevertheless, we provide guidance on its use and highlight aspects to consider in meeting the legal requirements for clear and plain language in the employment context. Furthermore, we find that employees' conceptualizations of privacy are characterized by a high level of confidence in the lawful processing of personal data by employers and a low level of both concern and awareness about potential privacy invasions. In addition, conceptualizations are strongly influenced by uncertainty

regarding the processing of personal data, including unawareness about the entities involved in data processing, whether data exist, how data are transferred, where data are stored, and how data are protected. Ignorance is compensated for by high levels of trust in electronic data processing, in the conduct of employers, and by having confidence in TOMs to protect privacy. Lack of risk awareness with regard to privacy in employment is compensated for with analogies to private online use. In addition, hackers and internal attackers are assumed to pose a major threat to privacy in employment.

(2) Furthermore, we present the first mental models of the right to informational self-determination in employment, finding that they are characterized by high demands for ex ante control over the dissemination and use of personal data. We further identified three distinct types of mental models that differ in employees' desire for control over (1) the disclosure of personal data, (2) the flow of personal data, and (3) the unrestricted control over the processing of personal data. Despite strong demands for self-determination, exercising the right to informational self-determination is seen as a burden in the face of privacy controls available today. In addition, demands for ex post control and transparency as key elements of the right to privacy remain less pronounced, uncovering a source of potential conflict for privacy in employment.

By uncovering misconceptions and limitations in employees' mental models, we reveal what privacy controls employees desire. Stakeholders concerned or involved with employee privacy, such as employers, software developers, and researchers, benefit from understanding threats and risks to employee freedom and rights when human factors are neglected in the development of privacy controls, but also gain insights about theoretical and abstract privacy concepts for future research. At the same time, the mental models provide valuable guidance throughout the entire privacy engineering process [9] on how to conceptualize and design usable employee-centric privacy controls.

#### 1.4.2 *Empirical evidence of employee privacy perceptions*

We provide the first in-depth analysis of employee privacy perceptions of perceived sensitivity and willingness to disclose personal data along with the determinants of these perceptions. Our research contributes to the body of knowledge in several ways:

(1) We provide evidence that the perceived sensitivity of personal data in the employment context differs significantly from the results of previous studies in other domains. Furthermore, we demonstrate that frequently used legal and contextual distinctions between different types of personal data do not accurately reflect the subtleties of employees' privacy perceptions. Instead, based on an assessment of perceived sensitivity and willingness to disclose 62 different personal data elements, we identified four groups of personal data with distinct characteristics that better reflect the multi-dimensionality of employees' perceptions. Moreover, we show that perceived data sensitivity proves to be a fairly stable moderate predictor of employees' willingness to disclose across different groups of personal data. However, context may have different effects on perceived sensitivity and willingness to disclose, causing employees to be potentially unwilling to share non-sensitive data but willing to disclose data perceived as sensitive.

(2) Furthermore, we provide the first systematic analysis of frequently used personal data disclosure antecedents in online privacy research for privacy in employment. We show that employees with strong beliefs in a right to privacy are quite concerned about the collection and unauthorized secondary use of their personal data by employers.

However, employees' overall risk perception is low and overall trust in employers is high. In addition, employees' willingness to disclose is not affected by these factors.

(3) Last but not least, we present the first three groups of employees that differ in their perceived data sensitivity and willingness to disclose. One group is willing to disclose, depending on the personal data's sensitivity and contextual appropriateness for employment. Another small group is reluctant to disclose truthful data, even if they were essential to the employment relationship. A third group is very willing to disclose all but the most sensitive personal data. However, the groups do not differ in either their privacy beliefs nor in their demographics.

Our findings therefore provide empirical evidence to respect contextual differences and the uniqueness of privacy perceptions among individuals in employee privacy. Our contributions specifically address the need for privacy engineering in activities of requirements elicitation, risk management, or architecture decisions to include context-specific conceptualizations of personal data and stakeholder groups [12, 15, 16, 99]. In addition, the results serve employers, policymakers, and researchers with an overall better understanding of employees' privacy perceptions, and as a basis for future targeted research on specific types of personal data, employees, and tool support.

#### 1.4.3 *Data Cart: A privacy pattern for the GDPR-compliant handling of personal data by employees*

Data processing employees play a critical role in protecting privacy and are thus expected to follow strict data protection guidelines and practices. We present the results of a UCD study in which we worked together with 19 data processing employees from two large public organizations in Germany. We provide profound qualitative insights into the needs of data processing employees for usable privacy controls that help them comply with privacy obligations when processing employees' personal data. To address their requirements, we present the novel privacy pattern *Data Cart*, which can be leveraged to design tools and processes that assist data processing employees with both data management and privacy law compliance. We also provide an associated implementation concept and "Wizard-of-Oz" prototype implementation. *Data Cart* maps processes that involve the retrieval and the management of personal data into a generic workflow that enforces a data protection compliant handling of personal data through Privacy by Design (PbD). The privacy pattern provides for streamlining the collection of personal data, standardizing access to personal data, and facilitating employee access to privacy policies and documentation. Formative usability testing of the prototype revealed that it would provide data processing employees with a sense of security when processing employee personal data. Furthermore, our participants expected *Data Cart* to raise their awareness of privacy obligations, reduce errors, and increase work efficiency. Our results suggest that if PbD becomes an integral part of digitalization, employee perceptions of data protection may be positively altered.

In particular, stakeholders involved in privacy engineering, such as employers, IT engineers, and researchers, benefit from our work by gaining insights into ways to improve the usability of privacy-compliant tools for managing employee personal data. At the same time, the privacy pattern aids in both architecture and system definition in privacy engineering, and assists employers as data controllers in regulatory compliance.



## 1.5 IMPACT

The results of all studies have been published in international peer-reviewed conferences, journals, and workshops. This section provides a summary of the different publications and highlights the contributions of the author of this dissertation. If available, we also indicate the rating using the CORE<sup>2</sup> list and the Journal Impact Factor (JIF)<sup>3</sup>.

In the following, we provide a summary of papers that are part of this dissertation. The papers divide into work that focuses on fundamental knowledge of employee privacy, presented in Section 1.5.1, and work that focuses on the employee-centric design of privacy controls for data processing employees, presented in Section 1.5.2. In addition, Section 1.5.3 contains a summary of work related to the topic of this dissertation that further illustrates the impact of the author's work, but is not part of this dissertation.

1.5.1 *Generation of fundamental knowledge about human factors in employee privacy*

The contents of the following three papers form the basis for Chapter 5 and Chapter 6 of this dissertation.

- ▷ J. Tolsdorf and F. Dehling. In Our Employer We Trust: Mental Models of Office Workers' Privacy Perceptions. In *Proceedings of the 1st Asian Workshop on Usable Security (AsiaUSEC, FC workshop)*, pages 122–136, 2020. [100]

I am the lead author of this workshop paper. I contributed to all stages and contents of the study, including the study and questionnaire design, recruitment, conducting and transcribing interviews, as well as evaluation and interpretation.

- ▷ J. Tolsdorf, F. Dehling, D. Reinhardt, and L. Lo Iacono. Exploring Mental Models of the Right to Informational Self-Determination of Office Workers in Germany. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2021(3):5–27, 2021. [101] – Rating: CORE A

I am the lead author of this journal paper. I contributed to all stages and contents of the study, including study and questionnaire design, recruitment, conducting and transcribing interviews, as well as evaluation and interpretation.

- ▷ J. Tolsdorf, D. Reinhardt, and L. Lo Iacono. Employees' Privacy Perceptions: Exploring the Dimensionality and Antecedents of Personal Data Sensitivity and Willingness to Disclose. *Proceedings on Privacy Enhancing Technologies (PoPETs)*, 2022(2):68–94, 2022. [102] – Rating: CORE A

I am the lead author of this journal paper. I designed and conducted all stages and contents of the study, including the study and questionnaire design, recruitment, data analysis, and interpretation.

<sup>2</sup> <http://portal.core.edu.au/conf-ranks/>

<sup>3</sup> <https://jcr.clarivate.com/jcr/home>

### 1.5.2 Design of practical and usable privacy controls for data processing employees

The contents of the following two papers form the basis for Chapter 7 of this dissertation.

- ▷ J. Tolsdorf, F. Dehling, and L. Lo Iacono. Data Cart – Designing a Tool for the GDPR-compliant Handling of Personal Data by Employees. *Behaviour & Information Technology (BIT)*, 41(10):2070–2105, 2022. [103] – Rating: CORE B, JIF 3.086

I am the lead author of this journal paper. I contributed to all stages and contents of the study, including designing the various studies, recruitment, conducting and transcribing focus group sessions and interviews, evaluation and interpretation. Moreover, I provided the implementation for the prototype.

- ▷ F. Dehling, D. Feth, S. Polst, B. Steffes, and J. Tolsdorf. Components and Architecture for the Implementation of Technology-driven Employee Data Protection. In *Proceedings of the 18th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*, pages 99–111, 2021. [104] – Rating: CORE B

I initiated this conference paper and took a leading role in its finishing. I designed the presented micro frontend architecture using Domain Driven Design, and contributed to the integration procedure. Moreover, I provided the literature research and contributed to both the introduction and the results' interpretation.

### 1.5.3 Further impact

In addition to the contributions and impact outlined above, which make up the content of this dissertation, the author of this dissertation has also contributed to both national and international forums on privacy in employment and privacy online. The focus was on investigating and implementing data subject rights in the form of privacy dashboards and related concepts.

- ▷ J. Tolsdorf, C. K. Bosse, A. Dietrich, D. Feth, and H. Schmitt. Privatheit am Arbeitsplatz - Transparenz und Selbstbestimmung bei Arbeit 4.0. *Datenschutz und Datensicherheit (DuD)*, 44(3):176–181, 2020. [105]

I am the lead author of this journal paper. I provided the literature research and discussion on privacy dashboards for using them as a means to promote transparency and control in an employment context, and contributed to the privacy dashboard framework presented.

- ▷ J. Tolsdorf, F. Dehling, and D. Feth. Benutzerfreundlicher Datenschutz in Cloud-basierten Office-Paketen. *Datenschutz und Datensicherheit (DuD)*, 45(1):33–39, 2021. [106]

I am the lead author of this journal paper. I designed and conducted the walk-through study to evaluate the transparency and control capabilities of office clouds in terms of their usability for employees.

- ▷ J. Tolsdorf, F. Dehling, and L. Lo Iacono. Take Back Control! The Use of Mental Models to Develop Privacy Dashboards. *ITG News*, 8(3):15–20, 2020. [107]

I am the lead author of this journal paper. I provided the literature research and discussion on how to use mental models of privacy to design privacy dashboards.

- ▷ J. Tolsdorf, M. Fischer, and L. Lo Iacono. A Case Study on the Implementation of the Right of Access in Privacy Dashboards. In *Proceedings of the 9th Annual Privacy Forum (APF)*, pages 23–46, 2021. [108]

I am the lead author of this conference paper. I supervised the design and execution of the study conducted as part of a bachelor thesis. Moreover, I evaluated and interpreted the data, and provided the literature research and discussion on privacy dashboards and the right to access under the General Data Protection Regulation (GDPR).

- ▷ C. K. Bosse, A. Dietrich, P. Kelbert, H. Küchler, H., H. Schmitt, J. Tolsdorf, and A. Weißner. Beschäftigtendatenschutz: Rechtliche Anforderungen und Technische Lösungskonzepte. In *Tagungsband des 23. Internationalen Rechtsinformatik Symposions (IRIS)*, page 1–8, 2020. [109]

I supported this work by contributing to the technical solution concepts for the introduction of privacy technologies in organizations and, in particular, by incorporating a model for the gradual introduction of company privacy dashboards.

- ▷ S. Polst, J. Tolsdorf, F. Dehling, und D. Feth. Verarbeitung von Beschäftigtendaten. *Datenschutz und Datensicherheit (DuD)*, (45)(1):19–22, 2021. [110]

I supported this work by contributing parts of the mental models study on the comprehensibility of terminology, perception of data processing, and risk awareness. I also supported the discussion of the results.

- ▷ S. Wiefeling, J. Tolsdorf, and L. Lo Iacono. Privacy Considerations for Risk-based Authentication Systems. In *Proceedings of the 7th IEEE International Workshop on Privacy Engineering (IWPE)*, pages 320–327, 2021. [111]

I supported this work by contributing the privacy requirements for the use of Risk Based Authentication derived from privacy law and international standards. I also supported in the literature research.

## 1.6 DISSERTATION OUTLINE

The remainder of this dissertation is structured as follows:

Chapter 2 “*Foundations*” sets our work within the larger field of workplace privacy, details the legal framework, and introduces key aspects of privacy engineering and human-centric privacy research.

Chapter 3 “*Information privacy in employment: A literature survey*” presents the results of a systematic literature review on information privacy in employment, and outlines the state of the art.

Chapter 4 “*Problem statement and research questions*” derives our specific research questions to address existing knowledge gaps.

Chapter 5 “*Study I — Employees’ conceptualizations of the right to informational self-determination*” presents the study design, methodology, and results of our first and exploratory study with 27 employees.



Chapter 6 “*Study II — Determinants and differences of employees’ perceptions of personal data*” presents the study design, methodology, and results of our second and quantitative study with 553 employees.

Chapter 7 “*Study III — Data Cart: A privacy pattern for the GDPR-compliant handling of employee personal data*” presents the study design, methodology, and results of the UCD study involving 19 data processing employees.

Chapter 8 “*Conclusion*” summarizes the contents and contributions of this dissertation, and gives an outlook on future work.



*One point on which there seems to be near-unanimous agreement is that privacy is a messy and complex subject.*

— Hellen Nissenbaum

Privacy is a multifaceted concept that is highly contextual, with little agreement on its definition due to diverse perspectives and theories [24, 112, 113, 114, 115, 116]. This dissertation focuses on a concept of privacy referred to as “information privacy” and applies it to the employment context. Information privacy reflects the impact of technological development and related social change on the freedom and power of individuals to disclose their information or to withhold it from others. As a result, there is widespread consensus that information privacy concerns socio-technical issues that require taking into account legal, social, organizational, technical, and human factors [7, 13, 15, 16, 23, 117]. Based on this notion, this chapter presents the foundations that are essential for fulfilling the objectives of this dissertation. First, in Section 2.1, we situate this dissertation within the scientific-theoretical framework of privacy. Then, in Section 2.2, we turn to the legal perspective and present our working definition of privacy as “the right to informational self-determination”. We next present the fundamentals of privacy engineering in Section 2.3, including relevant concepts, processes, and tools. This is followed by an introduction to human-centric privacy research in Section 2.4, where we also explain its relevance to privacy engineering. Finally, we conclude this chapter with a summary of the presented foundations in Section 2.5.

## 2.1 INFORMATION PRIVACY

This dissertation is situated in the broader field of “workplace privacy” [25] and “organizational privacy” [69], in which “*privacy is defined as a state or condition in which the individual has the capacity to (a) control the release and possible subsequent dissemination of information about him or herself, (b) regulate both the amount and nature of social interaction, (c) exclude or isolate him or herself from unwanted (auditory, visual, etc.) stimuli in an environment, and, as a consequence, can (d) behave autonomously (i.e., free from the control of others)*” [69]. According to this definition, workplace and organizational privacy is composed of “solitude privacy”, “work environment privacy”, “autonomy privacy”, and “information privacy” [25, 69, 118]. That said, it is impossible to draw a clear line between information privacy and other dimensions of workplace and organizational privacy, as they overlap in scope and have influenced each other’s development over time. Especially, solitude privacy and work environment privacy are closely related, as they are both conceptually related to “physical privacy” [113] and concern physical access to an employee’s spatial environment, presence, and private space. They build heavily on early theory that conceptualizes privacy as a set of states [119] and require the regulation of boundaries and interaction with others [119, 120, 121]. Autonomy privacy means

the ability of individuals to escape the supervision and control of their behavior in order to ensure free development and independence. It is used by employees to maintain autonomy over, e.g., work processes, methods, work pace, and decision-making [122]. Information privacy, in turn, is traditionally understood as information disclosure and is closely related to the ability of individuals to control the processing of personal data and information [123]. However, modern legal and scholarly conceptualizations of information privacy acknowledge its potential to serve individuals as a means of managing privacy states and achieving autonomy in the information era. As a result, information privacy is now embedded in a strong and comprehensive theoretical, scientific, and legal framework, comprising a wide range of disciplines, including philosophy, politics, social sciences, law, psychology, economics, media studies, computer science, and engineering.

While first definitions of privacy for the technology era were relatively simple, viewing privacy as a “right to be let alone” [124], the very rapid and ongoing development of information systems and the resulting impact on people’s everyday lives soon led to more sophisticated definitions and broader perspectives. Today, vital elements of definitions of information privacy include the following:

- **Control over access to information:** Information privacy research has placed a strong emphasis on control over personal information, adopting Westin’s definition of privacy, which is *“the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others”* [123]. Research subsequently adapted this definition to the employment context, stating that privacy in employment *“entails (perceptions of) control over the acquisition, storage, use, dissemination, and dispersal of employees’ data. That is, it concerns control over the information that could be made available to others”* [25]. In this regard, strong emphasis has been put on control over both the *gathering* and the *handling* of employees’ personal information [25, 72, 125].
- **Management of privacy boundaries:** Information privacy research has further been influenced by the definition of privacy as *“an interpersonal boundary process by which a person or group regulates interaction with others”* [120]. The boundary metaphor has evolved through Communication Privacy Management (CPM) theory, which provides explanations for the decisions people make about disclosing or concealing private information based on an internal mental calculus [126]. 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. CPM theory has been applied to workplace privacy, examining employees’ perceptions of computer-mediated communication [49, 56] and employee surveillance [57], as well as for investigating reasons for interpersonal employee information disclosure behavior [127].
- **Appropriate flow of information, context dependence, and norms:** Contextual Integrity uncouples information privacy from a pure control perspective by asserting that privacy is about *“whether information is appropriate or inappropriate for a given*

context, [and] whether its distribution, or flow, respects contextual norms of information flow” [27]. It emphasizes on the appropriate flow of information based on a tuple comprising sender, data subject, recipient, data, and context. Taking into account social norms for a particular context, different transmission principles apply to a tuple. Consequently, people’s privacy decision-making process heavily rely on implicit rules, as well as contextual and cultural differences [27, 28]. In this regard, it was found that employees’ *perceived legitimacy* of the employer to process personal information (e.g., expected usage) is also important for information privacy in employment [25, 72, 125]. Employees may perceive an invasion of their privacy if employers’ actual data processing do not meet their expectations.

- **Uniqueness of privacy perceptions among individuals:** Privacy also depends strongly on inter-individual differences, such as personality, gender, age, or cultural background of a person [24]. However, these types of differences have received limited attention in the employment context [25]. Some exceptions include studies on gender differences in the impact of perceived control [125], studies on the impact of workers’ ethical characteristics on perceived privacy invasion by employer practices [71], and studies with cross-national samples [33, 38].

## 2.2 LEGAL FOUNDATIONS AND PRIVACY DEFINITION

Today, information privacy is recognized as a fundamental right worldwide, with the United Nations Human Rights Council codifying it as *the right to privacy in the digital age* in 2019 [128]. The resolution calls on states and business enterprises to take regulatory, economic, and technological steps to protect individuals from privacy risks posed by digital transformation. However, the groundwork for a right to information privacy was already laid nearly half a century earlier.

**DEVELOPMENT OF MODERN DATA PROTECTION LAW** The first efforts were made in Europe and North America as early as the 1970s, when modern data protection laws were enacted in response to the rapid growth of information systems and the processing of personal data. During this time, ideas were born to establish a Code of Fair Information Practices (FIPs) [129] as well as to enact privacy principles and safeguards for automated personal data systems [130]. Since then, FIPs and privacy principles have influenced the discourse on information privacy and remain an integral part of privacy laws and frameworks around the world [131]. In an initial attempt to facilitate the harmonization of privacy laws, and to promote a minimum level of privacy protection worldwide, the Organization for Economic Cooperation (OECD) developed the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* in 1980. Subsequently, FIPs and privacy principles were further developed in the context of data protection laws and industry approaches to self-regulation. However, the laws and approaches available in the 2000s were criticized for their ineffectiveness in safeguarding information privacy [132]. In particular, the lack of effective sanctions was identified as a key problem. Legislators responded to this lack with new data protection laws introduced in the 2010s, which now impose strict sanctions for non-compliance with these laws. In this context, the advent of the GDPR [133] in 2016 marks a turning point in that the regulation provides for fines of up to €20 million or up to 4% of a company’s total annual global turnover

(Art. 83 (5) [GDPR](#)). The [GDPR](#) has thereby caused a worldwide stir, as its scope has been defined to affect all data processing entities that have their registered office or maintain an establishment in the [EU](#). It also applies when individuals located in the [EU](#) are offered goods or services from a third country or when their behavior is monitored from there. Consequently, the [GDPR](#) has led to significant harmonization and enforcement of data protection practices on a global scale. This is complemented by legislative initiatives around the world that have followed the [GDPR](#)'s lead. Examples include the California Privacy Rights Act ([CPRA](#)) in the U.S. (enacted: 2023) [[134](#)], the General Data Protection Law ([LGPD](#)) in Brazil (enacted: 2020) [[135](#)], and the amended Act on the Protection of Personal Information ([APPI](#)) in Japan (enacted: 2022) [[136](#)]. One reason for this development is that personal data may only be transferred to non-[EU](#) Member States if the European Commission has decided “*that the third country [...] ensures an adequate level of protection*” (Art. 45 (1) [GDPR](#)).

**APPLICABILITY OF DATA PROTECTION LAWS TO EMPLOYMENT** In terms of information privacy in employment, the rights provided to individuals under contemporary data protection laws generally also apply to employees. Some laws, such as the [CPRA](#), include the employment context explicitly, whereas other laws, like the [GDPR](#) and the [LGPD](#), cover the employment context implicitly. Nevertheless, privacy in the employment context is subject to enormous regional differences, even within the [EU](#). Specifically, the [GDPR](#) contains an opening clause that allows Member States to “*provide for more specific rules to ensure the protection of the rights and freedoms in respect of the processing of employees’ personal data in the employment context*” (Art. 88 (1) [GDPR](#)). At the time of writing this dissertation, 17 Member States, including Germany, make use of this option [[137](#)]. In contrast to other contexts, the definition and interpretation of the right to privacy in the employment context therefore heavily depends on a mixture of national and international law and regulations. This dissertation focuses on the cultural context of Germany.

**COMPOSITION OF EMPLOYEE DATA PROTECTION RULES** Despite both governmental and non-governmental efforts to create uniform rules for employee privacy, there does not exist a dedicated employee data protection law in Germany. Instead, the rules remain a mixture of [EU](#), federal, and state laws, as well as [EU](#) and national case law. The basic legal framework that underlies this dissertation is summarized in Figure 2.1. In this context, data protection rules are generally subject to the primacy of [EU](#) law and the principle of subsidiarity. Primacy of [EU](#) law means that [EU](#) law takes precedence over national law. The principle of subsidiarity entails that sector-specific special laws also take precedence over general laws. Application of these principles to data protection rules in Germany results, among other things, from § 1 (2) and § 1 (5) of the amended Federal Data Protection Act ([BDSG](#)), which came into force in 2018. The provisions of the [BDSG](#) generally apply to companies and federal authorities. The German legislator also makes use of the opening clause of Art. 88 [GDPR](#) to regulate data processing for purposes of the employment relationship in § 26 [BDSG](#). It also stipulates that collective agreements and works or service agreements can define more specific rules. Besides the [BDSG](#), each federal state also has a State Data Protection Act ([LD SG](#)), whose provisions apply to state and local authorities. The rules for employee data protection are thus derived as follows: The basic rules result from the [GDPR](#). The [BDSG](#) determines who is considered an employee in Germany and under which conditions personal data may be processed

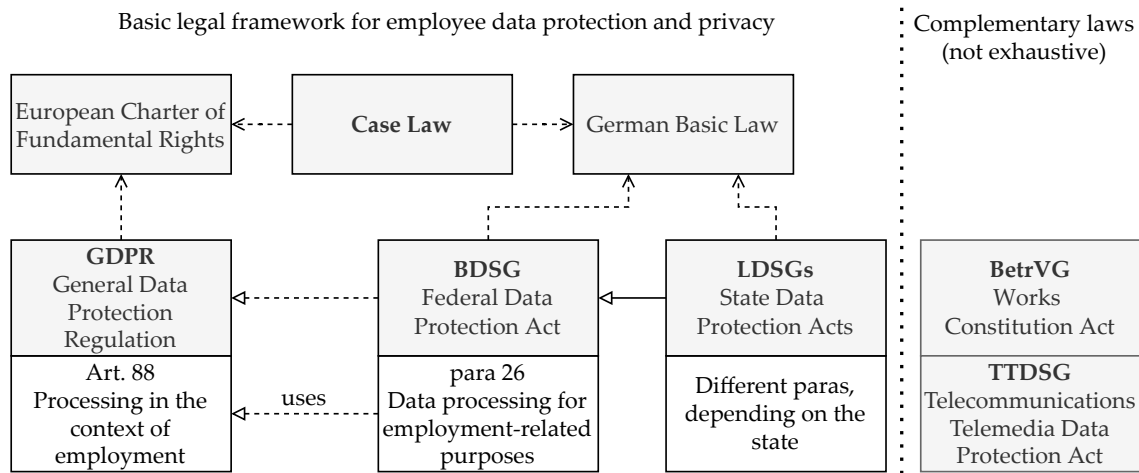


Figure 2.1: Basic legal framework and complementary laws for employee privacy.

in an employment relationship. The conditions are supplemented by collective agreements and works or service agreements. The **LDSGs** of the federal states supplement the **BDSG**, primarily by adding specific purposes for which personal data may be processed. Furthermore, the Works Constitutions Act (**BetrVG**) and the Telecommunications Telemedia Data Protection Act in particular may also have consequences for employee data protection. Furthermore, it is worth noting that the Protestant and Catholic churches in Germany each have their own employment and data protection laws, which, however, are not taken into consideration in the course of this dissertation.

In addition, there are also rules and rights resulting from case law. In the past, landmark judgments have been made on the basis of both the European Charter of Fundamental Rights and the German Basic Law. At the **EU** level, the decisions on the “Safe Harbor” agreement and the “EU-U.S. Privacy Shield” are essential, as they restrict the processing of employees’ personal data. At the national level, rights derived from the general right to free development of personality are particularly important.

On this basis, the remainder of this section first presents this dissertation’s privacy definition of the right to informational self-determination in Section 2.2.1. This is followed by definitions of stakeholders in Section 2.2.2 and terminology in Section 2.2.3. Afterwards, the objectives and principles of data protection law are outlined in Section 2.2.4, and employee privacy rights are presented in Section 2.2.5.

### 2.2.1 Definition of the right to privacy as informational self-determination

Generally speaking, in Germany, the right to information privacy is tantamount to the fundamental right to informational self-determination. It guarantees the authority of the individual to determine for themselves on the disclosure and use of their personal data. The right was not enacted by the legislature, but was established by the German Federal Constitutional Court (**BVerfGE**) in December 1983 in the context of the Census Ruling (**BVerfGE** 65, 1 - Volkszählung). Here, the Federal Constitutional Court derived the right to informational self-determination from the basic right of free development of personality pursuant to Art. 2 (1) in conjunction with the principle of human dignity pursuant to Art. 1 (1) of the German Basic Law (i.e., Germany’s constitution). In this



context, informational self-determination is regarded a necessity in order to protect individuals from the unlimited collection, storage, use, and disclosure of their personal data, and thus to ensure the free development of personality. As a result, the German Census Law was judged unconstitutional, in particular because the planned forwarding of non-anonymized personal data to other agencies for vaguely defined purposes violated the basic right of free development of personality.

**PROTECTION OBJECTIVE** The Federal Constitutional Court described informational self-determination as an indispensable right for the preservation of the free democratic basic order, as it protects the individual from the panopticon effect: *"The right to informational self-determination would be incompatible with a social order and a legal system, in which citizens can no longer know who knows what, when, and on what occasion about them. Those who are uncertain whether deviant behavior is recorded at all times and permanently stored, used, or forwarded in the form of information will try to avoid attracting attention through their behavior. [...] This would not only impair the individual's opportunities for development, but also the common good, because self-determination is an essential prerequisite for the functioning of a free democratic society"* (BVerfGE 65, 1 (146), translated).

**SCOPE AND APPLICATION** Even though the right to informational self-determination was originally created to protect citizens from the state, the Federal Constitutional Court recognizes the right as an objective norm (BVerfGE 84, 192). This means that it must also be applied to the interpretation and application of private law issues. The right to informational self-determination thus also affects the employment context in Germany and has been the subject of recent rulings in labor law, e.g., on the monitoring of employees by employers and on the mandatory disclosure of personal data.<sup>1</sup> Furthermore, the right has been incorporated into German legislation, meaning that the perception of privacy in Germany is largely shaped by the right to informational self-determination. It has particularly influenced national laws like the BDSG and LDSGs.

Furthermore, the concept of informational self-determination does not allow for "trivial" data. In other words, there are no data that are not protected by the right per se. This is justified by the fact that data sensitivity depends primarily on the ability to use and utilize data in the context of information technology. The true sensitivity of data therefore only emerges after the purpose, the linking potential, and the potential uses have been identified. The sphere theory developed by the Federal Constitutional Court to classify the sensitivity of information is therefore only conditionally applicable today [138]. The sphere theory classifies information into an intimate sphere, a private sphere, and a social sphere in order to assess the legitimacy of an encroachment on the right to personality. In general, what was once considered low-sensitivity information from the social sphere can now be coded as data and be combined with other data to produce sensitive information. As a result, an encroachment of the right to informational self-determination occurs whenever individuals are forced to disclose their data or do so unwittingly. In contrast, no interference occurs if the individual can decide to disclose their data completely voluntarily.

<sup>1</sup> Federal Labor Court (BAG) 27 July 2017 - 2 AZR 681/16 - Rn. 17, BAGE 159, 380  
 State Labor Court (LAG) Hessen 25 October 2010 - 7 Sa 1586/09  
 Federal Labor Court (BAG) 25 September 2013 - 10 AZR 270/12 - Rn. 32, BAGE 146, 109  
 State Labor Court (LAG) Thüringen 16 May 2018 - 6 Sa 442/17



**BOUNDARIES AND RESTRICTIONS** Nevertheless, the right to informational self-determination is not absolute, because it may conflict with other (fundamental) rights. As a consequence, individuals may have to accept the mandatory disclosure of personal data to preserve those rights. Restrictions to informational self-determination must be accepted, in particular in the case of predominant public interest. Encroachments on informational self-determination must also be accepted in employment if they are indispensable for the purposes of the employment relationship or are required by law. Such restrictions, however, must meet the following requirements [139]:

1. The restriction must have a (constitutional) legal basis. This means that a law must permit the restriction.
2. The legal basis must comply with the principle of proportionality. This means that, on the one hand, the restrictions must not be excessive. On the other hand, restrictions must be indispensable for the protection of public interests. A restriction is deemed proportionate if it is suitable and necessary to achieve the intended objective and proves to be appropriate in a weighing of interests. So far, the weighing of interests has indeed been of predominant relevance in the jurisdiction of the German Federal Constitutional Court [140].
3. The legal basis must comply with the principle of clarity. This means that the scope of the restriction must be clear and apparent to the individual. It is therefore required that the reason, purpose, and scope of the restrictions to the right to informational self-determination must be formulated in a domain-specific and precise manner.
4. The principle of clarity also implies the necessity of purpose limitation. This means that the use of personal data must be limited to a predefined legal purpose. In general, changes of purposes are allowed *ex post*. However, such changes then represent a restriction themselves and require an independent legal basis subject to the same requirements as those outlined above.

In its ruling against the German Census Law, the German Federal Constitutional Court stated that the mandatory disclosure of personal data must always be accompanied by measures to prevent unrestricted use and misuse. According to the ruling, this shall include at least the following measures (BVerfGE 65, 1 (152 – 155)):

1. Defining purposes in a domain-specific and precise manner;
2. Determining the suitability and necessity of the data for data minimization;
3. Restricting the use of data to the specific purposes;
4. Providing for protection against misuse;
5. Providing a duty to inform individuals;
6. Providing obligations to provide information upon request;
7. Providing obligations to delete data;
8. Providing for involvement of independent data protection officers.

**COMPATIBILITY WITH PRIVACY LITERATURE** The concept of the right to informational self-determination is consistent with the definitions of information privacy provided in Section 2.1. In particular, it emphasizes the notion of autonomy by means of control and transparency over personal information acquisition, storage, use, dissemination, and dispersal. We thus consider the right to informational self-determination as a decent proxy for the studying of information privacy in employment, and use it as our definition of privacy in the context of this dissertation.

### 2.2.2 *Key stakeholders in employee privacy*

Preserving privacy in employment requires the consideration of numerous actors and stakeholders. In the following, the various actors and stakeholders are introduced by describing their roles and responsibilities based on the classification provided by EU and German data protection laws. Accordingly, actors and stakeholders of major concern are subdivided into (1) entities involved in personal data flow and processing, and (2) supervisory bodies and authorities. A summary of all actors and stakeholders, including their relations and examples, is presented in Figure 2.2.

**ENTITIES INVOLVED IN PERSONAL DATA FLOW AND PROCESSING** In the following, the main actors and stakeholders in the context of employee privacy as defined in Art. 4 GDPR are described.

- **Data subject:** Any identifiable natural person whose personal data are processed is referred to as a “data subject”. In general, data subjects are granted extensive rights in terms of transparency and control over the processing of their personal data (cf. Section 2.2.5). In an employment relationship, this role is filled by employees. The German legislator defines “employee” very comprehensively, including: Temporary workers in relation to the hiring party, trainees, people undergoing rehabilitation, people employed in workshops for the disabled, volunteers performing a service under the Youth Volunteer Service Act or the Federal Volunteer Service Act, economically non-independent persons, home workers, civil servants, judges, soldiers, persons performing civilian service, and job applicants (§ 26 (8) BDSG).
- **Recipient:** Any entity to which personal data are disclosed is considered a recipient. Excluded are public authorities, such as tax authorities and compulsory social security, which are not considered to be recipients under the regulation. Apart from this exception, entities that fall within the definition of recipient are affected by the provisions of data protection law, e.g., in the context of data subjects’ rights. The regulation further differentiates between different types of recipients, discussed below.
- **Controller:** A recipient of utmost importance is the “(data) controller”, as it is the entity that determines the purposes of the processing of personal data. In an employment relationship, this role is taken by the employer. They bear full responsibility and must take measures to ensure and demonstrate compliance with data protection law (Art. 24 GDPR). In addition, it has extensive documentation obligations and is obligated to ensure that data subjects can exercise their rights. The

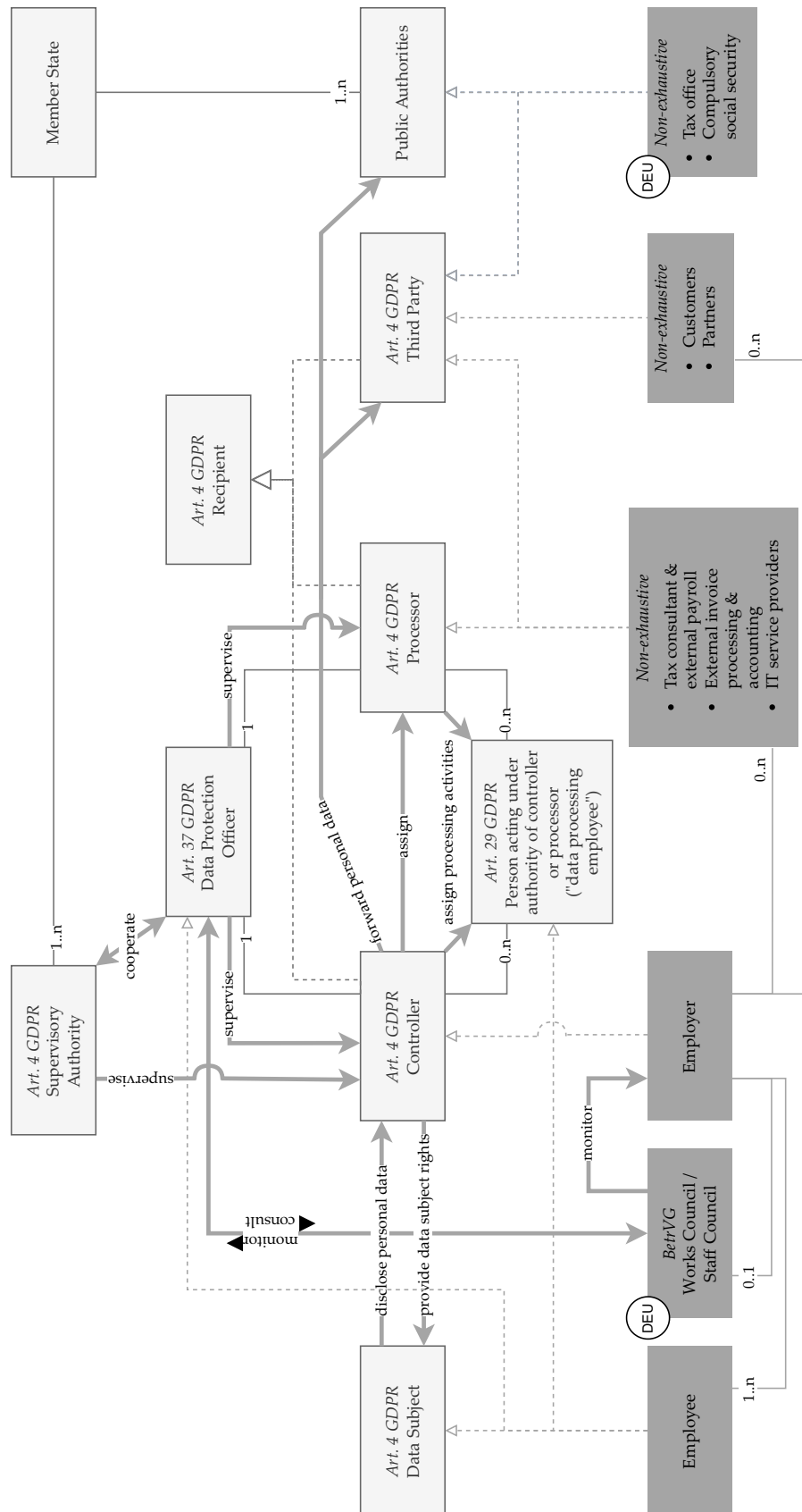


Figure 2.2: Stakeholder map of the GDPR with a mapping to entities in the employment context. Entities specific to Germany are marked accordingly (DEU).

responsibilities and obligations of the data controller apply regardless of whether personal data are collected, stored, processed, or disclosed by them or by an authorized party on their behalf.

- **Processor:** A recipient who processes personal data on behalf of a controller is referred to as a “(data) processor”. For the most part, processors are subject to the same rules as controllers, but in a considerably more relaxed form. Yet, they are supposed to support controllers in fulfilling their obligations. Processors in the employment context include, e.g., tax consultants who prepare payroll on behalf of the employer, or IT service providers who provide the employer’s IT infrastructure and the software used by employees.
- **Data processing employee:** A natural person that is authorized to process personal data under the direct authority of a controller or processor is referred to as a “(personal) data processing employee” in the scope of this dissertation, since privacy law does not provide for a short form definition. According to the law, data processing employees “*shall not process [...] [personal] data except on instructions from the controller, unless required to do so by Union or Member State law*” (Art. 29 GDPR). Data processing employees are not considered processors themselves, but agents of the controller or processor. In Germany, federal and state supervisory authorities have thus decided that employers in their role of controllers and processors are liable for their data processing employees’ compliance errors [141]. This view has also been confirmed by court decisions.<sup>2</sup> Nevertheless, privacy violations caused by data processing employees may result in disciplinary and legal consequences for them, depending on the severity of the misconduct.
- **Third party:** A recipient other than the data subject, controller, processor, and data processing employee are referred to as “third parties”. In employment, this role may be taken by customers to whom employee personal data are disclosed.

**SUPERVISORY AUTHORITIES AND BODIES** To monitor the application of employee data protection rules, EU and German law provide for different types of supervisory bodies. Those are subdivided into public supervisory authorities and supervisory bodies within an organization.

- **Supervisory authorities:** Independent public authorities that supervise the application of data protection rules are referred to as “supervisory authorities” or Data Protection Authorities (Art. 51 GDPR). For this purpose, Germany has established the Federal Commissioner for Data Protection and Freedom of Information (BfDI) together with State Commissioners for Data Protection (LfDs) in each federal state. Generally speaking, the BfDI is responsible for the monitoring of the application of data protection rules for public institutions and federal agencies, whereas the LfDs are responsible for non-public entities and state agencies. Depending on the nature of the employment relationship, employees may contact either the federal or state agency with complaints against the employer.

<sup>2</sup> Regional Court (LG) Bonn 11 November 2020 - 29 OWi 1/20

If possible, privacy issues should be avoided from the outset and resolved internally instead. Hence, EU and German law also provides for the establishment of supervisory bodies within an organization:

- **Data protection officer:** First, data protection law provides for the appointment of a Data Protection Officer (DPO), who is designated by the data controller, i.e., the employer (Art. 37 GDPR). A DPO must be appointed if the organization is a public authority or body, or the processing of personal data is part of the core activity, or at least 20 persons are permanently engaged in the automated processing of personal data (Art. 37 GDPR and § 38 BDSG). A DPO is considered a representative of the employer and should be involved in all issues related to the protection of personal data. The role of a DPO can either be fulfilled by employees of the organization or by external bodies. According to the law, a DPO must not be subject to receiving instructions regarding the exercise of their tasks, shall not be dismissed or penalized for their tasks, and shall directly report to the highest management (Art. 38 (2) GDPR). Furthermore, a DPO is supposed to collaborate with the federal or state supervisory authority as required.
- **Works council:** The second internal supervisory body is the “works council”, which may be formed in all organizations with five or more employees entitled to vote. Its responsibility to monitor compliance with data protection provisions results from the works council’s duty *“to see that effect is given to Acts, statutory instruments, safety regulations, collective agreements and works agreements for the benefit of the employees”* (§ 80 (1) No. 1 BetrVG). The works council is thus responsible to monitor compliance with both data protection law and the free development of personality, including the therefrom resulting right to informational self-determination. Furthermore, the works council is granted a right of co-determination if employers plan *“the introduction and use of technical devices designed to monitor the behavior or performance of the employees”* (§ 87 (1) No. 6 BetrVG). Although the works council may process personal data independently, i.e., without the employer’s supervision, it does not constitute a data controller on its own. Instead, *“the employer is the controller for the processing of personal data within the meaning of data protection law”* (§ 79a BetrVG).

Overall, the tasks and activities of the two internal supervisory bodies are mutually dependent. For one thing, the works council may be involved in the process to designate a DPO. While an employer can always appoint external bodies or managerial employees as a DPO, the works council must be involved in the selection process in the case of non-managerial or new employees. In this case, the works council may verify whether the person in question qualifies as a DPO. Moreover, irrespective of who eventually performs the role of the DPO, the works council must monitor that the DPO performs their duties correctly and that they are not subject to instructions from the employer. On the other hand, the works council is also accountable to the DPO, as it must coordinate the processing and protection of personal data with the DPO.

### 2.2.3 Definitions of data and information concerned

Generally, privacy legislation aims to protect the privacy of individuals and therefore only applies to data that are personally identifying. In Europe, such data are referred

to as “personal data”, enshrined in *Article 8 – Protection of personal data* of the EU Charter of Fundamental Rights. At the international level, the term “personal data” is often used interchangeably with, e.g., “personal information” or “personally identifiable information”. In the German language, one also commonly distinguishes between different subcategories of personal data to refer to different aspects within the meaning of the GDPR. However, the terms’ usage in the literature, in reasons for judgments, but also in privacy notices is inconsistent and partially nonspecific. For this reason, definitions of common terms are presented below and explained as they are used in this dissertation:

- **Data** (German: *Daten*): Unspecific in the context of privacy legislation, but often used in practice to refer to various categories of data.
- **Information** (German: *Informationen*): Unspecific in the context of privacy legislation, and frequently used interchangeably with “data”. Nevertheless, the right to informational self-determination acknowledges that information is the interpretation of data in a given context. In this regard, information may also be coded as data to be used to generate additional information.
- **Personal data** (German: *Personenbezogene Daten*): This is the official legal term in EU and German data protection law. It means any information that would allow identifying a data subject both “directly or indirectly, [but] in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person” (Art. 4 GDPR). Recital 26 further clarifies that “[t]o determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used [...]”. Consequently, the definition of personal data applies to both identified and potentially identifiable data, including pseudonymized data. Only strictly anonymized data are excluded from this definition and are thus not affected by the GDPR’s provisions. This broad definition of personal data is certainly in line with the Federal Constitutional Court’s notion that “trivial” data does not exist under the right to informational self-determination.  
*Examples:* All data under GDPR, incl. name, nationality, IP address, an employee personnel number, and picture.
- **Personally Identifiable Information (PII)** (German: *Personenbezogene Daten*): There does not exist a uniform definition for this term [142]. Different to “personal data” under the GDPR, however, PII is generally characterized by narrow definitions that define a set of information and data which allows for mostly *direct* identification of a data subject [143, 144]. This means that “personally identifiable information” often simply refers to “personally identified data” in practice. Such limited definitions are predominantly shaped by U.S.-views of privacy and deemed incompatible with the GDPR’s definition [145]. Nevertheless, the notion of PII is widely used in international privacy standards [9, 143, 146].  
*Examples:* Name, and social security number.
- **Personal identified data** (German: *Personenbezogene Daten*): Similar to PII, in German one sometimes refers to the subcategory of only directly identified data [145] that have a direct personal reference. However, the German term does not differ from that for “personal data” nor from that for “PII”.  
*Examples:* All data with a direct personal reference, incl. name, and picture.



- **Personal identifiable data** (German: *Personenbeziehbare Daten*): Another subcategory of personal data, solely referring to data with indirect personal reference but from which an individual can be identified.  
*Examples:* Nationality, IP address, and employee personnel number.
- **Personal aspects data** (German: *Persönliche Daten*): The literal translation of “persönliche Daten” into English would be “personal data,” but since this term is already occupied, the term “personal aspects data” is used in this dissertation. The [GDPR](#) refers to personal aspects mainly in profiling and can be seen as an unspecified subcategory of personal data. In practice, however, the German term is inconsistently used in the literature, in reasons for judgements, and in privacy notices. It is commonly referred to in the context of the protection of personal data on the basis of the general right of personality under the German Basic Law [138]. As such, the German Constitutional Court referred to personal aspects data in its Census Ruling. Consequently, in theory, all data relating to the personality of a person fall under this term. The extent to which these data are entitled to protection is assessed by classifying them into public, private, and intimate spheres [138].  
*Examples:* Personal preferences, personal interests, behavior, personal data.
- **Private data** (German: *Private Daten*): In Germany, the concept of when data and information from the personal domain are considered private has been shaped to a large extent by judgments. Accordingly, data are considered private if their disclosure is considered indecent, or embarrassing, or if they trigger adverse reactions due to special contexts [138]. Aside from its use in law, the term is also inconsistently used in privacy notices and privacy settings of software to refer to data or access rules. In the employment context, the (permitted) private use of work materials and equipment (e.g., IT devices) can also have legal consequences. Court rulings have established that, in principle, employers must not access data marked as “private” by their employees, without further ado.<sup>3</sup>  
*Examples:* Private files, and private emails.

In addition to the definitions outlined above, privacy legislation also explicitly distinguishes between different groups of personal data based on their respective sensitivity:

- **Special categories of personal data** (German: *Besondere Kategorien personenbezogener Daten*): The [GDPR](#) recognizes the special sensitivity of data concerning the “racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation” (Art. 9 [GDPR](#)). The regulation also acknowledges the sensitivity of information on criminal convictions and offenses, but these do not formally belong to the special categories of personal data (Art. 10 [GDPR](#)).  
The scope for processing sensitive personal data is much more restricted than for traditional personal data, and may only take place if privacy legislation defines exceptions that explicitly allow the processing. For example, the processing of special categories of personal data is permitted, among other things, if data subjects provide explicit consent or if the processing “is necessary for the purposes of carrying out

<sup>3</sup> Federal Labor Court (BAG) 31 January 2019 - 2 AZR 426/18 - Rn. 13, BAGE 165, 255

*the obligations and exercising specific rights of the controller or of the data subject in the field of employment [...]*" (Art. 9 GDPR). It should be noted at this point that in order to carry out an employment relationship in Germany, it is quite likely that employers collect personal data that belong to the special categories. For example, a membership in a Christian church or the country of origin may be requested when registering an employee for compulsory social insurance. In addition, in rare cases even the existence of a severe disability and illnesses may be processed, insofar as there is a factual connection with the employment relationship.

#### 2.2.4 Objectives, principles, and provisions of privacy legislation

The GDPR's objective is to harmonize data protection rules in order to guarantee a high level of data protection across national borders and thus enable cooperation between countries (cf. Recital 3 - 6, 8, 10 GDPR). In particular, the objective is to create a uniform legal framework based on control and certainty, with equivalent powers and sanctions (cf. Recital 7, 11 GDPR). German national data protection law further aims to safeguard the fundamental right to informational self-determination. To achieve these objectives, privacy legislation defines several principles, to which all personal data processing must be subject (Art. 5 GDPR). In addition, privacy legislation contains several provisions to which data controllers and processors must adhere (Arts. 24 - 37 GDPR). The principles and provisions with particular regard to the employment context are described below:

- **Lawfulness, fairness, and transparency:** The GDPR provides for comprehensive requirements to process personal data fairly, lawfully, and transparently towards data subjects, for which a key element is the principle of "prohibition with subject to permission". In employment, this means that employers may only process personal data of their employees if this is permitted by § 26 BDSG or Art. 6 GDPR. Accordingly, data processing is permissible, e.g., if:
  - It is *"necessary for hiring decisions or, after hiring, for carrying out or terminating the employment contract or to exercise or satisfy rights and obligations of employees' representation laid down by law or by collective agreements or other agreements between the employer and staff council"* (§ 26 (1) BDSG);
  - It serves to detect crimes (§ 26 (1) BDSG);
  - It is based on freely given consent (Art. 6 (1) a GDPR, § 26 (2) BDSG);
  - Other permissible conditions are met, e.g., the processing is necessary for compliance with a legal obligation or for the purposes of legitimate interests (Art. 6 (1) c-f GDPR).

It should be noted that although consent is in principle a valid legal basis, in practice it hardly ever plays a role in the employment setting. This is mainly due to the fact that the essential requirement of free will can hardly be proven. In Germany, freely given consent is recognized in employment if it is associated with a legal or economic benefit for the employee or if the employer and employee pursue the same interests. In this regard, the legislator points out that *"employees are seldom in a position to freely give, refuse or revoke consent, given the dependency that results from the employer/employee relationship"* [147]. The legislator thus recommends to always base personal data processing on other grounds than consent.



With regard to transparency, employers must provide their employees with comprehensive information on the processing of their personal data. Such information must be provided in a *“concise, transparent, intelligible and easily accessible form, using clear and plain language”* (Art. 12, Recital 58 [GDPR](#)). The legislator emphasizes that the scope can be very broad, including comprehensive information on monitoring activities [\[147\]](#). It is also recommended that a representative sample of employees be involved in the drafting and evaluation of rules and measures.

- **Purpose limitation:** Employers may only process personal data from employees for legitimate purposes that have been explicitly stated. Further processing is not permitted, unless employers verify that changing or adding purposes is compatible with the original purpose (Art. 6 (4) [GDPR](#)). A general exception applies to archiving of personal data. For one thing, archiving may be required by law, e.g., documents relating to trade and tax law must be retained for 10 years. Besides, archiving can also be based on a legal interest of the employer, e.g., in order to *“protect the establishment, exercise or defense of legal claims”* (Art. 17 (3) [GDPR](#)).
- **Data minimization:** Employers may only collect, store, and use personal data of employees if the processing of such data is appropriate and limited to the extent necessary within the scope of the employment relationship. The legislator stresses that data processing must be proportionate to the risks faced by both employers and employees to minimize the amount and time of processing [\[147\]](#). In Germany, the scope of permitted personal data is significantly restricted by laws such as the General Equal Treatment Act, the Gene Diagnostics Act, or the Federal Central Register Act. Accordingly, the collection of employees’ genetic material, party affiliation, religious affiliation, pregnancy, union membership, diseases, disabilities, or all previous convictions is inadmissible. Aspects of the living conditions that are to be assigned to the private or intimate sphere also do not have to be disclosed.
- **Accuracy:** Employers must ensure that personal data of employees they store are accurate and up to date. For this, employers must take all reasonable steps to ensure that inaccurate personal data are either erased or rectified without delay.
- **Limitation of storage:** Employers may only store personal data of employees for as long as is necessary for the purposes of data processing. For example, in Germany, records of rejected applicants must be deleted after 6 months. The legal retention periods for wage tax documents, employment contracts, or payslips are between one and 10 years. Thereafter, the data must either be deleted or transformed into non-personal data. To this end, employers must develop and maintain a deletion concept according to which certain employee data are deleted or anonymized after specified periods of time. In addition, employers are allowed to store basic information about employees who have left the company for an indefinite period, for instance if the employer needs this information to track decisions.
- **Integrity and confidentiality:** Employers must implement [TOMs](#) to protect the personal data of employees against accidental or unlawful destruction, accidental loss, and alteration. Employers must also protect the data from unauthorized disclosure or access.

- **Accountability:** Employers are obligated to demonstrate compliance with the principles outlined above. In order to comply with this obligation, privacy legislation contains several provisions that employers must comply with:
  - Implement **TOMs** to ensure and demonstrate that processing of employee personal data complies with legal requirements (Art. 24 (1) **GDPR**). Their implementation must take into account the state of the art and incorporate the principles of “[d]ata protection by design and by default” (cf. Section 2.3.1). This requires **TOMs** to be implemented “in an effective manner and to integrate the necessary safeguards into the processing” (Art. 25 (1) **GDPR**) to ensure adequate protection against unauthorized access, as well as the integrity, availability, and resilience of the entire processing (Art. 32 **GDPR**).
  - Address the risks posed by processing to the rights and freedoms of employees by conducting privacy impact assessments “taking into account the nature, scope, context and purposes of the processing” (Art. 35 (1) **GDPR**).
  - Create and maintain a directory of records of processing activities documenting the employee personal data processed and the employer’s handling of such data (Art. 30 **GDPR**). This includes but is not limited to a description of the purposes, categories of data subjects, categories of personal data, categories of recipients, the envisaged time limits for erasure, and a description of **TOMs** implemented.
  - Inform employees about the data processing on their own initiative “in a concise, transparent, intelligible and easily accessible form, using clear and plain language” (Art. 12 (1) **GDPR**). For this purpose, employers must disclose extensive information about the details of the processing to their employees. In addition, they must inform employees about their rights to lodge a complaint, as well as to access, rectify, and erase personal data (Art. 13 **GDPR**) (cf. Section 2.2.5).

#### 2.2.5 Rights of data subjects and employees

Employees have several rights regarding the personal data processed by their employers. The rights are primarily composed of the general rights of data subjects under data protection law (Arts. 12 - 22 **GDPR**) and employee rights under labor law (§ 83 **BetrVG**). In addition, the German legislator makes use of another opening clause of the **GDPR** (Art. 23 (1)) and restricts the rights of data subjects (paras 32 - 37 **BDSG**). In the following, we list the various rights and explain their consequences for the employment relationship.

- **Rights to information and access to personal data:** Although not explicitly mentioned, employer’s information obligations under Arts. 12 - 14 **GDPR** are understood in practice as a “right” to information for employees. Accordingly, employees must be informed by their employers whenever personal data are collected, either directly from the employee or from other sources. The information provided must include, but is not limited to, details about the categories of personal data collected, the employer’s representative, the **DPO** in charge, the purposes of the processing, the legal basis, the recipients, the transfer to a third country, the period of processing, and the source. Employees may also proactively request this information at regular intervals by exercising their right of access (Art. 15 **GDPR**).

Under this right, they may also request a copy of their personal data, insofar as a copy does not interfere with the rights and freedoms of other individuals (Art. 15 (3) GDPR). Similarly, employees also have a right to data portability (Art. 20 GDPR) which in principle allows the taking of information provided by the employee to the employer in a machine-readable format. However, German law restricts both these employees' rights if the data are stored only on the basis of a legal obligation to retain them or exclusively for the purposes of monitoring or safeguarding data (protection) (§ 34 (1) Nr. 1 BDSG). Nevertheless, these exceptions only apply if *"providing information would require a disproportionate effort, and appropriate technical and organizational measures make processing for other purposes impossible."* Accordingly, employers are only required to provide information on the *primary* processing purposes. Apart from this, German labor courts have not yet conclusively clarified how specifically data must be requested by employees in order to be eligible to exercise the right to access.<sup>4</sup> For example, although employees must always be allowed to inspect their personnel files (BetrVG), it is often unclear what additional data are affected by the right to access. It is also unclear how exactly the data must be prepared and presented, with the exception that this should be done in a consistent format.<sup>5</sup>

- **Rights to data correction:** Under the rights to data correction one refers to the rights to rectification, deletion, restriction, and objection according to Arts. 16 - 18, and 21 GDPR [148]. Under these rights, employees may request that outdated, inaccurate, incomplete, or unlawfully collected personal data be corrected, completed, deleted, or their processing be restricted. Once employees exercise their right to data correction, employers are obligated to communicate the corrections to all recipients to whom the employees' personal data have been disclosed (Art. 19 GDPR). The scope of these rights is, however, limited by legal provisions as described above (cf. previous Section 2.2.4). In principle, employers are required to include data in the personnel file at the employee's request if the data are related to the employment relationship (e.g., additional qualifications). In addition, data must be removed from the personnel file if they jeopardize the employee's career advancement and the employer's interest in retaining the data does not outweigh the employee's need for protection [148].
- **Right to protection against automated processing:** Employees have the right not to be subject to a decision based solely on automated processing that produces a legal effect, unless it is necessary, authorized by law, or based on employees' consent (Art. 22 GDPR). In particular, employees should be protected from "black box" decisions.

## 2.3 PRIVACY ENGINEERING

After having placed this dissertation in the theoretical-scientific context of privacy in Section 2.1 and having presented the corresponding socio-legal framework in the previous Section 2.2, this section now turns the focus to issues concerning the practical

<sup>4</sup> Federal Labor Court (BAG) 27 April 2021 - 2 AZR 342/20

<sup>5</sup> State Labor Court (LAG) Baden-Württemberg 17 March 2021 - 21 SA 43/20

implementation of privacy by means of privacy engineering. Privacy engineering concerns the design, implementation, and evaluation of theories, methodologies, strategies, and tools to systematically capture and handle privacy challenges in socio-technical systems by incorporating privacy issues into systems engineering [13]. Overall, it is an extremely heterogeneous field, shaped by stakeholders from the public sector [10, 11, 149], research [7, 13, 15, 150], and industry [8, 9, 17]. The remainder of this section first introduces the design philosophy underlying privacy engineering in Section 2.3.1, followed by a brief description of how it integrates into the systems engineering life cycle in Section 2.3.2. Next, we briefly introduce privacy enhancing technologies in Section 2.3.3 and privacy patterns in Section 2.3.4, two tools that are commonly used in privacy engineering to implement legal obligations regarding data subjects' rights and TOMs, and thus are of central importance for the objectives of this dissertation (cf. Section 1.2).

### 2.3.1 *Privacy and data protection by design & by default*

Privacy engineering is inherently linked to the concept of Privacy by Design (PbD) [6, 11, 146, 151]. PbD is a design philosophy that advocates for privacy assurances to become the default by “baking” privacy principles arising from privacy best practices (e.g., FIPs), privacy laws (e.g., GDPR, BDSG), and privacy standards (e.g., ISO/IEC 29100) into IT systems, business processes, and physical design from the outset [8, 10, 11, 149]. It incorporates seven foundational principles:

- **Proactive not reactive; preventative not remedial:** All privacy policies and mechanisms must be in place prior to processing so that privacy issues can be resolved before they become real problems.
- **Privacy as the default:** The default case should guarantee integrity of privacy and provide for fair processing of personal data, including but not limited to purpose limitation, data minimization, transparency, and intervention capabilities.
- **Privacy embedded into design:** Privacy protection should not be considered an “add-on” but an integral part of information systems and business practices. It requires considering the broader context and all stakeholder views for finding the best solution.
- **Full functionality – positive sum, not zero-sum:** PbD means promoting privacy as a complement, not a trade-off, and provides for innovative and creative solutions that take into account all legitimate interests.
- **End-to-end security – lifecycle protection:** Privacy requires consideration of the entire processing chain, from collection to destruction of personal data (“cradle to grave”).
- **Visibility and transparency – keep it open:** Data controllers should meet their accountability obligations by demonstrating compliance and providing truthful information about the processing.
- **Respect for user privacy – keep it user-centric:** Data protection should reflect the interests and needs of data subjects, and requires user-oriented approaches in the design of tools, information systems, and business processes.

Adhering to PbD is intended to reduce unintended privacy consequences, demonstrate and strengthen accountability, and earn trust, among other things [11]. The 2010 International Conference of Data Protection and Privacy Commissioners recognized PbD “as an essential component of fundamental privacy protection” [152] and promoted its widespread adoption in legislation. EU privacy legislation heeded this call by establishing the principles of *data protection by design and by default* in Art. 25 GDPR. The legislator acknowledges, however, that these principles do not address the “visionary and ethical dimension” [153] of PbD. Instead, *data protection by design and by default* are considered legal proxies of PbD that are limited to specific legal obligations [153]. Nevertheless, the principles result in a number of obligations for employers, including [153]: Establishing personal data processes as an outcome of a design project; implementing measures to protect employees’ fundamental rights and freedoms based on a risk management approach and an analysis of the state of the art; ensuring that the implemented measures are appropriate and effective to uphold the GDPR’s foundational principles; integrating safeguards into the processing; and taking measures to meet employees’ expectations about personal data processing. Beyond that, PbD also became part of international privacy standards [99] and frameworks [143], making it a key element of privacy engineering today.

### 2.3.2 Engineering processes, activities, and tasks

Simply put, PbD and *data protection by design and by default* generally describe *what* should be done to ensure privacy, whereas privacy engineering resolves *how* it should be done [11]. As such, privacy engineering is essentially concerned with the operationalization of the foundational principles of PbD, and the integration of the resulting activities into systems engineering processes. To this end, numerous approaches, frameworks, concepts, and principles have been proposed in academia and industry over the past decade [6, 7, 8, 9, 11, 15, 20, 149, 154]. They all offer slightly different approaches to integration with systems engineering and are ambiguous about which processes are involved. Throughout this dissertation, we draw exclusively on ISO/IEC TR 27550 [9], as its guidelines for integrating privacy engineering into system life cycle processes in accordance with ISO/IEC/IEEE 15288 [155] represent the most recent consolidation of previous approaches. According to the report, a total of nine of the 30 system lifecycle processes are affected by privacy engineering issues. In the following paragraphs, we provide a brief overview of the privacy engineering activities and tasks per process, divided into the four subclasses described in ISO/IEC/IEEE 15288 and taking the employment context into account. A summary of this overview is provided in Table 2.1.

**AGREEMENT PROCESSES** Activities in this subclass aim to negotiate agreements between organizations concerning privacy, which ultimately affects the two processes *acquisition* and *supply*. In employment, privacy-related requirements are to be established within both these processes by reaching agreements between employers (acquirer) and processors or providers of sub-systems (suppliers) for compliance with employee privacy obligations [9]. This may include agreements regarding relevant privacy standards and privacy controls to be implemented and guaranteed for.

Table 2.1: Mapping of privacy engineering activities and tasks to the systems engineering life cycle processes according to ISO/IEC TR 27550, focusing employee privacy.

Processes	Privacy engineering activities and tasks
Agreement processes	
Acquisition	Establishing agreements on privacy obligations between employer and suppliers or processors.
Supply	
Organizational project-enabling processes	
Human resources management	Providing personnel with employment-specific expertise in privacy (engineering) and data protection.
Knowledge management	Implement multidisciplinary knowledge bases on employee privacy.
Technical management processes	
Risk management	Conducting risk management, taking into account risks and implications for the freedom and privacy rights of employees.
Technical processes	
Stakeholder needs and requirements	Identification of stakeholders and potential privacy preserving features to address privacy expectations.
System requirements definition	Operationalization of privacy principles into system requirements.
Architecture definition	Designing a system architecture taking into account different privacy (design) strategies.
Design definition	Detailed specifying of the system and its privacy controls.

**ORGANIZATIONAL PROJECT-ENABLING PROCESSES** Processes in this subclass are used to direct, enable, control, and support the integration of privacy engineering into the system lifecycle. Two essential processes are identified for this purpose [9].

*Human resources management* must ensure the availability of personnel qualified and experienced in privacy engineering for, e.g., employee privacy. This may include expertise in software engineering, law, and social sciences to take into account the interdisciplinary nature of privacy. The process can be accompanied by employee training programs and assessments targeting employee privacy [9].

The purpose of the second process, *knowledge management*, is to define privacy engineering knowledge requirements, provide a corresponding knowledge repository, and track its use. The creation of the knowledge base requires multidisciplinary input from technical, legal, socio-cultural, and ethical perspectives to account for the socio-technical nature of privacy. The knowledge may then be made available to privacy engineers in the form of concepts, rules, guidelines, and reference models [146], but may also include catalogs of privacy controls and patterns [156].



**TECHNICAL MANAGEMENT PROCESSES** Technical management processes are used to develop, refine, and implement plans to protect employee privacy, as well as to assess progress and achievements. Herein, *risk management* is identified as the essential process shaped by privacy engineering to continuously identify, analyze, treat, and monitor risks related to privacy [9]. Activities and tasks should generally be based on formal privacy impact assessments in accordance with ISO/IEC 29134 [157]. In employment contexts, the analysis must particularly take into account risks and threats to the freedom and privacy of the employee. This implies risks that arise from the processing of personal data, such as surveillance, appropriation, or unanticipated revelation. Risk analysis must therefore include the extent to which processing exceeds employees' expectations, leads to a loss of freedom and autonomy, a loss of trust, or a power imbalance. In addition, "hard privacy" threats such as linkability, "soft privacy" threats such as employee unawareness, or security threats such as data breaches must also be considered [9]. The identified risks are then to be evaluated in terms of their likelihood and consequences. Likelihood in this case refers to the probability that the privacy rights and freedoms of a representative or typical individual are at risk [10]. Likelihood assessment must therefore incorporate contextual factors. Its assessment can be supported, in particular, by the inclusion of employee privacy concerns and demographic data resulting from knowledge obtained through empirical sociological methods [10]. Potential consequences to be considered include, in particular, the impact on employees' privacy, but also the impact on employers, e.g., in the form of penalties for non-compliance, or damage to reputation.

**TECHNICAL PROCESSES** Four processes are identified to define privacy requirements, and transform them into effective privacy controls [9].

The *stakeholder needs and requirements definition* process defines the stakeholders' privacy requirements for a system to provide the privacy capabilities needed by, e.g., employees. The process includes the identification of all affected stakeholders, e.g., employers, employees, and processors, as well as the identification of potential privacy preserving features, such as mechanisms for exercising employee privacy rights.

Next, *system requirements definition* is used to transform the stakeholder, employee-oriented view of desired privacy capabilities into system privacy requirements that meet employees' operational needs. This includes defining privacy controls and supporting privacy management services and functions. Requirements may result from either a goal-oriented or risk-oriented analysis [7]; in the former, requirements are derived from, e.g., privacy principles of international standards and laws. In the latter, requirements are derived by identifying threats that can compromise employee privacy (see above).

This is then followed by the *architecture definition* process to generate and assess system architecture alternatives that address stakeholder privacy concerns. The process requires reviewing the state of the art and previously elicited requirements, as well as identifying additional stakeholder requirements related to, e.g., effectiveness, usability, and adaptability [155]. The development of candidate architectures should include applying privacy design strategies [158, 159] and privacy patterns [156], commonly dividing into approaches of privacy-by-policy and privacy-by-architecture [15].

The final process identified is *design definition*, which provides a specification of privacy controls based on the requirements vetted by the previous processes [9]. This includes assessing and selecting both privacy and security controls. Assessment should include reiterating the *risk management* process. For selection, privacy design strategies

and patterns can be used, as well as catalogs of privacy controls with concrete proposals for, e.g., privacy and transparency enhancing technologies [9].

### 2.3.3 Privacy and transparency enhancing technologies

Privacy Enhancing Technologies (PETs) refer to all kinds of technologies and implementation approaches that help protect or enhance the privacy of individuals and facilitate the exercise of data subject rights [160, 161]. PETs are frequently linked to PbD, because their development usually implicitly takes into account some PbD principles, in particular *privacy by default* and *end-to-end security* [149]. Approaches to PETs can be roughly divided into three types [160]: (1) “Traditional” approaches targeting anonymity, unlinkability, unobservability, and pseudonymity; (2) approaches that enforce legal privacy requirements such as informed consent management and the implementation of data subjects’ rights; and (3) mixed approaches that combine both types and thus allow the implementation of comprehensive solutions. Some scholars further distinguish between PETs and Transparency Enhancing Technologies (TETs), with the latter enabling individuals to exercise their right to transparency and technology-enabled intervention capabilities [162, 163]. Under this view, PETs refer primarily to privacy-by-architecture approaches [15], i.e., enforcing restrictions on data collection and processing using tools and techniques such as onion routing [164], k-anonymity [165], and differential privacy [166]. In contrast, TETs primarily support privacy-by-policy approaches to notice, choice, and access [15], but can also demonstrate compliance [167]. For this purpose, TETs are divided into tools for ex ante and ex post transparency. Ex ante transparency informs about the intended data processing, whereas ex post transparency informs about the performed data processing. Exhaustive overviews of PETs and TETs are provided in [160, 161, 162, 163, 168].

### 2.3.4 Privacy (design) patterns

While PETs are often added at the end of a privacy engineering process or are even its output, so-called privacy patterns provide support already in the early phases of privacy engineering, such as in the *knowledge management* process (cf. Section 2.3.2). Privacy patterns are design patterns used to translate the abstract principles of PbD and *data protection by design and by default* into practical advice for developing privacy-friendly systems and processes. Design patterns are proven solutions to known and recurring problems in a specific domain that are systematically recorded and documented [169]. They are commonly arranged in pattern catalogs, i.e., collections of design patterns that systematically classify design patterns into different categories [170]. A more formal representation is a pattern system [170], also known as pattern language, which describes dependencies between individual design patterns based on a predefined set of relationship types [171].

**PRIVACY PATTERN COLLECTIONS** The concept of design patterns from software engineering was later extended to security [172] and privacy [173, 174]. Continuous efforts by the research community have resulted in a comprehensive collection of privacy patterns being available today, covering a multitude of topics including but not limited to anonymity [174] and pseudonymity [175], the development and application of PETs [176],



as well as issues targeting HCI [177, 178, 179] with an emphasis on transparency [180]. To support privacy engineers in the *architecture definition* and *system definition* processes, pattern descriptions are often accompanied by conceptual representations, UML diagrams, sequence diagrams, and screenshots. Many of the privacy patterns available have further been documented in a repository that is maintained by a collaboration of international researchers [156]. The patterns have also been organized into catalogs targeting specific domains, such as the online context [173, 181] and the Internet of Things [182]. In addition, some catalogs categorized patterns according to the principles of the privacy framework in ISO/IEC 29100 [143] with the aim of further simplifying the application of privacy patterns to comply with international standards and privacy laws [181, 183]. Meanwhile, there are first proposals for privacy pattern systems [176, 184, 185], as well as proposals for a suitable modeling language to concisely describe dependencies between privacy patterns [171].

**PATTERNS FOR BUSINESS PROCESSES AND WORKFLOWS** Akin to design patterns for system design and architecture, there also exist patterns for modeling business processes to include obligations imposed by privacy laws [186, 187, 188, 189, 190, 191]. Such patterns support organizations in modeling their high level architecture and business processes while incorporating PbD. Some approaches employ enterprise architecture model description languages to make the interdependence of systems and the associated data flows transparent and understandable [190]. This also allows determining which components must be added or implemented in order to comply with privacy principles or regulatory requirements [192]. Other approaches employ description languages for business process models to incorporate privacy principles and regulatory-mandated organizational measures into business processes by default [186, 187, 188, 189, 191].

**INTERACTION PATTERNS** Privacy patterns focus not only on technical and architectural aspects, but also about usability aspects, i.e., designing privacy protection in a human-centered manner to make it efficient, effective, and satisfying. To this end, numerous so-called HCI patterns have been proposed to provide usable interfaces for PETs [178, 179]. In particular, several patterns have been proposed under the design strategy *inform*, particularly suitable for implementing data subjects' rights [178, 180].

Independent of the topic of privacy, patterns that define problems and solutions targeting the perceived interaction behavior are generally referred to as interaction design patterns [193]. The term emerged in the HCI community to clearly distinguish design patterns with a focus on interaction behavior from design patterns for the realization of interfaces in software engineering. Interaction design patterns are usually the result of a human-centered design process in which the pattern was developed and evaluated together with the affected stakeholders [178, 194].

## 2.4 HUMAN-CENTRIC PRIVACY RESEARCH

As has been outlined in Section 2.3, privacy engineering builds on the notion that privacy is socio-technical in nature, which means that both technical-legal and socio-cultural aspects must be considered in the design and development of privacy-friendly systems, processes, and controls [7, 11, 13, 15, 16, 117]. In this regard, the discourse and consideration of PbD has been criticized as being too constrained by the *data protection by design*

perspective in the past, i.e., interpreting PbD primarily in terms of legal and technical perspectives [6, 195, 196]. Using a purely “legally-oriented process”, however, promotes the manifestation of “one-size-fits-all” solutions that are detrimental to effective privacy protection [11, 13], because they disregard the nature of privacy, which is individualistic, contextual, diverse, and multifaceted (cf. Section 2.1).

That said, PbD itself already takes this very much into account, promoting the principle of *respect for user privacy - keep it user-centric*. It essentially requires human factors of privacy to be incorporated in every IT system and business process [11, 151]. In particular, it emphasizes on the need for privacy controls to be “*human-centered, user-centric and user-friendly so that informed privacy decisions may be reliably exercised*” [151]. Similarly, the principle of *visibility and transparency* is also inherently socio-technical in nature [197], since the (legal) requirement to provide comprehensive information about the processing of personal data in a concise, intelligible manner, and in plain and clear language effectively requires consideration of human factors, especially usability [163, 198]. As such, there are increasing efforts to reinforce this principle in privacy engineering [160] and to expand the implementation of PbD to a “human-centric process” that accounts for this need [12, 16, 195, 199]. Human-centric privacy research lays the necessary foundations for this by providing methods, knowledge, and tools that enable privacy engineering to incorporate people’s privacy expectations, privacy concerns, privacy internalizations, and behaviors into the design and development process. It essentially uses concepts from the fields of HCI and information systems, and applies them to information privacy. Privacy engineering activities inherently rely on the inclusion of these results in multiple system engineering processes (cf. Section 2.3.2): In *knowledge management* to understand theoretical and abstract privacy concepts; in *risk management* to identify potential problems and determine their likelihood and consequences based on stakeholder concerns and demographics; in *stakeholder needs and requirements* for effective elicitation; in *system definition* to identify stakeholders’ privacy interests and capabilities; in *architecture definition* to identify specific requirements, e.g., in terms of usability; and in *design definition* to decide for or against the selection of specific security and privacy controls due to, e.g., usability criteria.

The remainder of this section lays out the methods and concepts commonly used in privacy research to explore socio-technical aspects. Since the methods available in the literature are extensive, the focus is on methods and concepts that are deemed most appropriate for achieving the goals of this dissertation: First, the basics of Human-Centered Design (HCD) are presented in Section 2.4.1, followed by a brief introduction to usable privacy in Section 2.4.2, along with an introduction to mental models in Section 2.4.3 as one of the most influential tools in HCI. Next, privacy macro models are presented in Section 2.4.4 that have been popularized by information systems research to explore socio-technical properties of information privacy. However, detailed information on the methodological approaches are not presented in this section, but will instead be discussed in the individual studies in Chapter 5, Chapter 6, and Chapter 7, respectively.

#### 2.4.1 Human-centered design

According to ISO 9241-210 [21], Human-Centered Design (HCD) represents a design philosophy that intends to make information systems more usable in applying knowledge and techniques from the fields of occupational science/ergonomics and usability. In ac-

cordance with ISO 9241-11 [22], a system is deemed usable if it can be used effectively, efficiently, and satisfactorily by specific individuals in a specific context to achieve specific goals. The application of HCD means that system design must be based on a comprehensive understanding of the stakeholders affected. To this end, they must be involved in the design and development at various points in time. In the case of participatory design, stakeholders are even included as equivalent “partners” in the design process. This allows researchers, designers, and stakeholders to benefit from each other’s experience and knowledge when developing new tools [200]. Furthermore, the design solution is continuously refined and adapted through user-centered evaluations. It should be noted, however, that unlike User-Centered Design (UCD) [201], HCD takes a holistic approach that also considers the interests of stakeholders who are not necessarily direct users of a system. In practice, though, UCD and HCD are often used as synonyms because they employ a similar methodology. In this respect, HCD and UCD represent an iterative process consisting of the following four steps (ISO 9241-210):

1. Understand and define the context of use, for example with the help of as-is scenarios and persona profiles. Possible methods for the survey are background interviews, questionnaires, sequence of work interviews, focus groups, and on-site observations [202].
2. Determine requirements, taking into account identified and derived requirements, as well as applicable design rules. Potential requirements may be identified, documented, categorized, and prioritized using brainstorming, card sorting, and affinity diagramming [203].
3. Development of design solutions, for example in the form of use scenarios, storyboards, and prototypes [203, 204]. Depending on the iteration loop, low- and high fidelity prototypes can be developed.
4. Evaluation of the design, for example in the form of usability test reports or user survey reports. Depending on both the iteration loop and resources available, potential methods include formal usability inspections, cognitive or pluralistic usability walkthroughs, and heuristic evaluation [205]. This may further include the use of interviews, questionnaires, and role playing [202].
5. Repeat steps 1 to 4 as necessary.

#### 2.4.2 Usable privacy

Studies that explore HCI aspects of PETs and apply HCD in the research field of information privacy fall within the domain of “usable privacy”. The focus, however, is usually on user-system relationships, meaning that usable privacy is more strongly located in the UCD domain. This is also reflected in attempts to systematize the application of UCD to privacy topics with the help of user-centered privacy frameworks [12, 16]. Accordingly, the user-centered development of privacy-friendly systems and processes requires (1) a solid understanding of the context, (2) an understanding of the stakeholder’s privacy awareness and expectations, and (3) a deep understanding and categorization of the sensitivity of the personal data processed by a system. Consequently, the underlying assumptions of these frameworks are consistent with those of the privacy engineering

frameworks [7, 15] introduced in Section 2.3. Nevertheless, user-centered privacy frameworks complement the privacy engineering frameworks, in that they propose models and workflows that incorporate HCI and usability aspects into every phase of system and process design. In this way, they support designers and developers in the selection of suitable concepts and methods. This allows the selection of user-specific privacy patterns that fulfill certain usability criteria, the implementation of protection measures that users expect, and the preparation of context-related information in the design phase.

Research on usable privacy that addresses issues under contemporary privacy law has focused almost exclusively on the needs of data subjects outside the employment context, including: (1) Examining the effectiveness and behavioral impact of transparency enhancing tools [163, 206, 207, 208] or provide the ability to intervene and consent [209, 210, 211]; (2) examining the compliance of such tools with the GDPR's demand to provide information on processing to data subjects *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language"* [108, 198, 212]; (3) examining users' perceptions of their (new) rights introduced by the GDPR [213, 214]; and (4) designing new tools that comply with both legal and user requirements [19, 208, 209, 215, 216]. The few exceptions in the employment context are presented later in Chapter 3.

#### 2.4.3 Mental models

Mental models are simplified internal representations of external reality that enable individuals to make sense of their environment [217]. People make use of (mostly simple) mental models in their everyday lives to understand complex processes and systems, without spending much time studying them in detail [218]. Essentially, such models represent a mental image of reality, which is why they are referred to as mental models. Individuals form mental models of unknown systems by trying to explain their observations and experiences through analogies from topics they are familiar with [219]. Therefore, mental models represent a person's individual view of a system that guides their action. The elicitation of mental models can provide insight into perception and sensation of individuals to better understand the reasons and influential factors of their behavior [218]. Mental models are generally considered to be vague and highly contextual representations [220]. Nevertheless, irrespective of their accuracy, mental models guide people's decision-making process in both familiar and unfamiliar situations [218, 221].

**MENTAL MODELS IN HCI** In the field of HCI, mental models are commonly used to capture the various elements of an individual's awareness and perception about theoretical concepts or specific information systems they use [222, 223]. A user's mental model is created through interaction with the target system [220]. The model is affected by a user's experience and understanding, but it does not have to be technically correct, only practical. If one now tries to elicit a user's mental model, a conceptualization of it emerges (i.e., a model of a model). The gained insights can then be used to align the target system with a user's mental model by either supporting the user or adopting the design of the target system. Conceptualized models can be used to design a system in such a way that the cognitive effort required for its use is kept to a minimum. Based on observations, the use of mental models is subject to the following restrictions [220]: Mental models are incomplete, unstable, and simple; mental models have no sharp boundaries; mental models are "unscientific" and incorrect; people's ability to use mental models is

limited. It follows from this that there cannot be one unambiguous mental model for a target system, but that, due to subjectivity, several models must always be considered. If the complexity of a target system exceeds the cognitive abilities of a human being, they depend on the use of a suitable mental model that leads to “correct” actions. This also applies to the consideration of the secrecy or disclosure of private information [224].

**MENTAL MODELS IN USABLE PRIVACY** In the field of privacy research, mental models allow modeling people’s understanding of privacy by examining “privacy” as the target system. In the context of usable security and privacy studies, mental models have been surveyed (1) to construct systems in which cognitive effort is optimized for usability [223, 225, 226], (2) to use them as a tool for effective communication between researchers, experts, and lay people [227, 228, 229, 230], or (3) to capture and explore concerns, expectations, and understandings of technology [231, 232, 233, 234, 235, 236].

Previous research has elicited mental models of privacy in general [237] and in the context of specific technical solutions, with a particular emphasis on online services [18, 225, 238, 239, 240, 241]. 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 [224] and rely on several incomplete and poorly formed sub-models [238] that drive their decision-making in privacy management.

#### 2.4.4 Privacy macro models

Privacy macro models provide conceptualizations of privacy that allow privacy to be measured. In addition, privacy macro models also allow systematizing research. In the following, we present the main models and frameworks relevant to the study of human aspects of information privacy in employment.

**EMPLOYEE PRIVACY CALCULUS** Early on, organizational privacy was strongly embedded in a value-based framework in which privacy is viewed in rational and economic terms [25, 69]. Within this framework of the “privacy calculus”, privacy can be assigned an economic value and thus becomes a tradable good. As a result, privacy becomes measurable and can be compared between individuals. Under this concept, privacy is understood as control over disclosure, whereby the withholding and disclosure of personal information follow the law of economic trade-off calculations [242]. As a result, an individual’s competing beliefs and desires are weighed against each other, and the weight of one may override the weight of the other [243, 244].

**PERCEIVED DATA SENSITIVITY** Privacy calculus is based on the notion that some personal data are more sensitive than others. As such, the “sensitivity” property is commonly defined as the perceived negative consequences or (potential) loss associated with data disclosure [245, 246]. Perceived loss is highly context-dependent, which in turn also makes the *perceived data sensitivity* context-dependent [113, 247, 248].

**WILLINGNESS TO DISCLOSE** The privacy calculus states that the trade-off results in either data disclosure or data withholding. Because it is often infeasible to observe people’s actual behavior in practice, studies often use measures of *behavioral intention* instead. According to the Theory of Planned Behavior [249], *behavioral intention* is the



strongest and most immediate antecedent to a person's actual behavior. One common gauge is people's *willingness to disclose* personal data, which has been shown to be a strong predictor of actual disclosure behavior [250, 251]. In this respect, research found that employees are generally willing to disclose personal data, but they may deliberately withhold information if they expect benefits or fear adverse consequences [118, 127]. To make their decision, employees generally assess the relevance and suitability of the requested data [66, 80]. Moreover, employees are more willing to disclose personal data if they believe they will receive adequate gratification in return [3]. Preferences for sharing (sensitive) personal data also vary by region [252, 253]. Moreover, employees' intention to disclose personal data can be partially explained by the CPM theory and privacy as Contextual Integrity (cf. Section 2.1).

**ANTECEDENTS → EMPLOYEE CALCULUS → EMPLOYEE OUTCOMES** Based on this notion, Stone and Stone [69] developed the first comprehensive model of organizational privacy that describes a causal chain of antecedents and consequences of employee privacy motivation in the form of "Antecedents → Employee calculus → Employee outcomes". This model essentially assumes that *employee calculus* is influenced by (1) individual factors such as age, gender, and personality, (2) macro factors such as social, cultural, and organizational norms, and (3) information factors such as information type, purpose of processing, and transparency [25, 69]. These influences have been confirmed in several studies [71, 76, 77, 78, 79, 80, 125]. *Employee outcome* can be behavioral, cognitive, or affective [25]. For example, *outcome* has been conceptualized as the willingness to disclose truthful data [41, 47], especially among job applicants [63, 64, 68], or as employees' acceptance and purposeful use of information systems [2, 3, 31, 35, 38, 44, 46, 254]. Furthermore, to better understand the *employee calculus*, employees' perceived invasion of privacy has often been used as a proxy to make information privacy quantifiable [43, 54, 62, 65, 67, 70, 71, 75, 77, 79]. This can include several further proxies, such as privacy beliefs, attitudes, perceptions, and concerns.

**PRIVACY CONCERNS** Privacy concerns, in particular, have become a key element of privacy research and an integral part of modern privacy macro models [112, 113, 114, 115, 116]. The construct of *privacy concern* reflects "an individual's subjective view of fairness within the context of information privacy" [255]. In practice, this refers to a person's risk beliefs, taking into account contextual norms (e.g., culture and regulatory laws) [244]. For its measurement, several scales have been developed in the literature, ranging from generic to context-specific constructs. The most widely used scales are the Concern for Information Privacy (CFIP) [256] and the Internet Users' Information Privacy Concerns (IUIPC) [255]. The scales build on several dimensions of an individual's *privacy awareness* and concern about recipients' handling of personal data, including *collection concern*, *concern for errors*, *concern for improper access*, *concern for unauthorized secondary use*. The scales' dimensions have significantly influenced the development of new and more context-dependent scales [257, 258]. Among other things, they have also been reviewed and applied to the work context [73, 259].

**ANTECEDENTS → PRIVACY CONCERNS → OUTCOMES** One of the most comprehensive and influential macro models incorporating privacy concerns is the "Antecedents → Privacy Concerns → Outcomes" (APCO) model. It can be considered an evolution of

Stone and Stone [69]’s model in that it harmonizes lessons learned from *all* contexts of past privacy research. The *APCO* model establishes privacy concerns as a systemic proxy and as an antecedent to outcome [113]. It follows the idea that privacy concerns arise from an individual’s disposition to privacy or situational clues that enable an individual to assess the consequences of disclosing information [113, 260]. As such, the basic *APCO* model is strongly anchored in privacy calculus. However, the stream of research on the privacy paradox [112, 113, 261, 262, 263], i.e., the phenomena that an individual’s privacy concerns appear to be at odds with their disclosure behavior, raised criticisms of the basic *APCO* model, arguing that it is too simplistic and promotes bias. As a result, the *APCO* model was eventually extended to include principles from behavioral economics and psychology to provide more accurate explanations for the *outcome* found in empirical research [264]. The extended *APCO* model therefore accounts for situational and cognitive constraints that influence processing effort, as well as biases and heuristics that influence behavior [264]. In addition, current research aims to establish workplace-specific antecedents to increase the contextual appropriateness of the *APCO* model to the work context [265, 266].

## 2.5 SUMMARY

In this chapter, we have set the foundation of this dissertation by placing it within the theoretical-scientific, socio-legal, and socio-technical frameworks of employee privacy.

Regarding the theoretical-scientific framework, we situated this dissertation within the broader field of workplace privacy and outlined key elements of a modern understanding of information privacy relevant to all studying on employee privacy.

Next, we elaborated on the socio-legal framework in which this dissertation is embedded and which is most relevant to both the study and implementation of employee privacy in Europe and, in particular, in Germany. To this end, we presented our working definition of information privacy in employment as employees’ right to informational self-determination. This was supplemented by a comprehensive stakeholder map and a thorough discussion of the legal framework and definitions offered by both European and German privacy and labor law, as well as the special jurisdiction to be considered.

Finally, we have laid out the main socio-technical aspects to be considered in the design and implementation of employee privacy. In particular, we outlined how privacy engineering relies on the consideration of human factors to implement effective privacy controls and privacy-friendly systems. In this context, we have pointed out that the consideration of “employee human factors” for employee privacy is inherent in the principles of *PbD*, and that privacy engineering relies on human factors in almost all systems engineering processes. This was followed by an introduction to methods and privacy macro models from *HCI* and information systems research that provide concepts, theories, and conceptualizations of privacy necessary to address human factors in employee privacy, and to achieve the goals of this dissertation, i.e., creating fundamental knowledge and employee-centric privacy controls (cf. Section 1.2).





## INFORMATION PRIVACY IN EMPLOYMENT: A LITERATURE SURVEY

---

*If I have seen further it is by standing on the shoulders of Giants.*

— Issac Newton

After having outlined the foundations of information privacy relevant to the employment context in Chapter 2, this chapter presents the current state of research and related work. For this purpose, we conducted a systematic literature review [267] on the topic of information privacy in employment. In the following, we first briefly discuss the methodology of the literature review in Section 3.1. Next, in Section 3.2, we then provide an overview of the topics covered in previous work. This is followed by a discussion on methodological, sampling, and participant biases in Section 3.3. We then demarcate this dissertation from previous work in Section 3.4, and finally conclude this chapter in Section 3.5, summarizing our literature survey findings.

### 3.1 LITERATURE REVIEW PROCEDURE

The goal of our literature review was to identify relevant work that has (1) empirically examined information privacy in the employer-employee relationship, (2) significantly contributed to the theoretical foundation of empirical research, and (3) applied methods of privacy engineering to the employment context. Although similar literature reviews have been conducted before, they are either focusing on non-employment contexts [112, 113, 114, 115, 116, 160, 161, 162, 163, 168, 268], are outdated [69], or the underlying methodology is unclear and not comprehensible [25].

To conduct our literature review, we used a three-step procedure consisting of the following steps [267]: (1) Identification of relevant articles in leading journals and conferences; (2) backward search by checking citations of previously identified articles; (3) forward search by using reference search engines. Instead of searching individual journals and conferences, we used databases of publishers and indexing services of scientific work. In accordance with recent meta studies on information privacy [4, 115, 116, 262, 269], we chose the following repositories for initial identification of relevant articles: The AIS Electronic Library, the SAGE Journals repository, the JSTOR repository, the Springer Link repository, and the Web of Science. For backward and forward searches, we additionally used Google Scholar and LENS. For an article to be considered, it had to meet the following basic requirements:

$$\begin{aligned}
 & \text{article} \ni (\text{information privacy} \wedge (\text{employee} \vee \text{worker}) \wedge (\text{workplace} \vee \text{employer})) \\
 & \wedge \text{title} \ni (\text{work}^* \vee \text{employee} \vee \text{employment} \vee \text{privacy} \vee \text{information} \vee \text{data}) \\
 & \wedge \text{abstract} \ni (\text{work}^* \vee \text{employee} \vee \text{employment} \vee \text{privacy} \vee \text{information} \vee \text{data})
 \end{aligned}$$

To include articles from engineering research areas on the topic of (usable) privacy, we used the following repositories based on previous literature reviews [163, 268]: The ACM Digital Library, the IEEE Xplore Digital Library, the USENIX Papers Search, the Sciendo search, the Springer Link repository, and the Web of Science.<sup>1</sup> However, because technical research areas tend to conceptualize “information privacy” simply as “privacy”, the articles had to meet the following basic requirements to be considered:

$$article \ni (\text{employee privacy} \wedge (\text{employee} \vee \text{worker}) \wedge (\text{workplace} \vee \text{employer}))$$

In addition, only peer-reviewed articles in English and with available full text were considered. Purely theoretical or legal discussions on information privacy, as well as studies that did not explicitly focus on the employee context, were explicitly excluded. Our final iteration took place in April 2022.

For our initial search, we translated the features described above into the query format of the respective database, resulting in a total of 785 hits. The number of relevant articles decreased to 94 after checking the title and abstract, and to 44 after reviewing the full content. After the backward and forward search, a total number of 80 articles was identified, of which 76 were available in full text.

The 76 articles were then systematized and categorized with respect to the following five characteristics: (1) The research objective and topic of study, (2) the conceptualization of privacy and its measurement used, (3) the applied study methodology, (4) the type, sample size, and nationality of participants in empirical studies, and (5) the analysis and evaluation method used. The results of our literature review are presented in the remainder of this chapter.

### 3.2 TOPICS OF EMPLOYEE INFORMATION PRIVACY

We identified a total of six topics into which we divided the existing works. In descending order, 19 papers addressed employee use of information systems, 16 papers addressed employee privacy perceptions, 15 papers addressed privacy engineering issues, 13 papers addressed job applicant privacy, 10 papers addressed workplace monitoring and surveillance, and three papers addressed workplace privacy in general. According to these characteristics, we present below the results of our literature review. We focus on the first five topics, since the latter has already been covered when we laid out the foundations in the previous Chapter 2. An overview of the different studies’ topics is also provided in Table A.1.

#### 3.2.1 *Information system use*

Work on information system use addresses the question of the extent to which information privacy perceptions influence employees’ acceptance and use of information systems in the workplace. The work covered includes topics on Enterprise Social Networks (ESNs) [31, 41, 45, 47], Bring Your Own Device (BYOD) [2, 38, 42], the use of wearables [3, 36, 44], artificial intelligence [33], and biometric systems [34, 35], as well as occupational health systems [32, 39] and employee-robot interaction [46].

<sup>1</sup> Please note that USENIX and Sciendo did not support advanced search strings and/ or the search had technical flaws, causing us to manually skim through the papers.

**FORMAL STUDIES OF BEHAVIORAL MODELS** Many of the studies on information system use have relied on formal quantitative statistical analyses of behavioral theoretical models to examine the impact of employees' privacy concerns on their intention to use an information system. Studies on this topic have heavily relied on a composition of [APCO](#), the Technology Acceptance Model ([TAM](#)) [37], and the Unified Theory of Acceptance and Use of Technology ([UTAUT](#)) [48]. [TAM](#) is designed to explain the acceptance of information technologies in the work context and was later extended with [UTAUT](#) to include moderator effects such as context and individual characteristics. For [ESNs](#), wearables, [BYOD](#), biometrics, and information systems in general, it was found that employee privacy concerns may indeed have a negative effect on the perceived usefulness, ease of use, and attitude toward the technology, which also reduces the intention to use it [2, 31, 35, 38, 42, 44]. For the [ESN](#) context, these results are supplemented by work finding that employees' trusting and risk beliefs had significant effects on their willingness to disclose information [41]. Other scholars developed frameworks that included information privacy norms and privacy calculus [45], or perceived control, data sensitivity, and perceived vulnerability [47], to explain the behavior of employees in [ESNs](#). Moreover, in the event that employers provide health record systems to their employees, Burkhard et al. [32] found that employees expected a high level of protection against unauthorized access by the employer, but also by other entities. Furthermore, Stock and Hannig [46] compared employee privacy concerns toward humans and robots in the workplace, and identified discrepancies between employees' stated privacy concerns and their intention to disclose information. They concluded that employee concerns about robots presented a paradox because they would disclose information regardless of their concerns. On another note, Lukaszewski et al. [43] found that employees would perceive the invasion of privacy by Human Resources ([HR](#)) systems to be lower if they were allowed to choose in which system their personal data are processed.

**EXPLORATORY AND EXPERIMENTAL STUDIES** In terms of qualitative and experimental studies, Badrul et al. [30] investigated government employees' privacy perceptions regarding the disclosure of work-related information in private use of Online Social Networks ([OSNs](#)). Based on [CPM](#) theory, they found that employees distinguish between private and professional boundaries, and that they want to keep their professional information separate from their private [OSN](#) when possible. Furthermore, Cardon et al. [33] applied boundary theory to the use of artificial intelligence at the workplace in order to understand how much control and transparency employees expect when their meeting records are analyzed algorithmically. They found that employees were willing to give up their privacy if it benefited the company or other employees. At the same time, though, employees made strong demands for strict guidelines on how the information was used. Moreover, Mettler and Wulf [3] explored employees' mental models of wearables at work. They found that mental models were biased by anxiety of privacy intrusions and the fear of limited self-determination. As a result, high levels of concern regarding the misuse of information by employers are reasons that hinder adoption of wearables. Simultaneously, some employees were generally willing to disclose data if they received adequate gratification in return. A recent study by Easley et al. [40] qualitatively investigated youth employees' privacy perceptions using a participatory toolkit. Aiming at a better understanding of youth employees' expectation of information disclosure in organizational email and chat, the authors report that youth employees' expectations were

strongly embedded in Contextual Integrity. As such, youth expected supervisors and co-workers to have access to communication data, but expected their communication to be generally protected from access by third-parties (e.g., advertisers, software vendors).

### 3.2.2 *Information privacy perceptions*

Work on information privacy perceptions addresses foundations of perceived privacy in the direct employer-employee relationship, without any particular technology acting as an antecedent or mediator.

**COMPANY PRIVACY POLICIES** Preliminary work in the 1980s conducted large scale surveys in the U.S. to examine whether employees were aware of their employer's data processing policies and what types of personal data they believed their employers processed [79, 80]. In examining whether these beliefs were true and whether employees perceived the use of information to be fair, it was found that for one-third of the information types surveyed, employees were either unaware or wrong. In addition, employees expected to have more control over their data than the company policies actually allowed, especially when forwarding data to external parties [79, 80]. Later studies showed that employees perceived a policy to be most intrusive and unfair when there was no way to authorize the release of personal information that would then be shared with an external recipient [75].

A study in 2008 examined further trends in U.S. employees' attitudes toward their employer's practices in handling workplace privacy after numerous reforms and laws were enacted [74]. It showed that government employees were significantly more satisfied with guidance in policies, and that employees with lower education rated communication practices as significantly worse than other employees. In contrast, employees with longer tenure and higher incomes were generally satisfied with their employers' workplace privacy management.

**SENSITIVITY OF INFORMATION PROCESSING** Apart from investigating employees' knowledge and work policy perceptions, researchers determined types of information and the purposes that employees would perceive as normative or intrusive if employers had the right to obtain the information and use it [76, 80]. They found that most financial matters, philosophical beliefs, and sexual preferences were considered private. In contrast, the majority of employees agreed that the use of demographic data, job data, pay data, medical data, drug tests, and polygraph tests were proper for personnel decisions. In certain cases, such as drug testing, it was found that employees' feelings of invasion of privacy were lower when the employer announced the drug test in advance and did not conduct it themselves [78]. In the case of appraisal systems, these were also perceived as less privacy invasive when employees accepted the system and its function [77]. However, opaque and complex appraisal systems in particular increased the perceived privacy invasiveness. Another study on organizational practices, such as drug testing, background checks, or internet monitoring, showed that an employee's ethical orientation has a direct effect on their perceived privacy invasiveness and appropriateness of such practices [71]. Thus, employees with a pronounced ethical formalism perceived a significantly lower invasiveness of privacy compared to their colleagues.

**PRIVACY PERCEPTIONS AND CONCEPTUALIZATION** Turning to the underlying impact of employees' perceived level of privacy on their levels of well-being and job performance, two studies examined the influence of privacy perceptions on intrinsic motivation and psychological empowerment [72, 125]. They revealed that these factors were indeed strongly affected by perceived informational privacy. Furthermore, Chen et al. [125] demonstrated that the strongly Western notion of privacy as control over information could be successfully applied to a Chinese sample. They also found that control over information gathering was fully mediated by control over handling, and that its effect on intrinsic work motivation was higher for males than for females.

Moreover, researchers have attempted to conceptualize and enable measurement of employees' privacy perceptions. Ball et al. [118] examined the dimensions of workplace privacy in order to distinguish information privacy from working environment privacy and solitude privacy, thereby addressing the different notions of privacy in general. Clouse et al. [73] reviewed the applicability of two scales widely used in online privacy research to measure privacy concerns for the employer-employee relationship. Recently, there have been attempts to use the theoretical foundations of these scales to further assess workplace-specific privacy concerns and to understand their determinants [259, 265]. Similarly, the same researchers developed a theoretical model to better understand the impact of inverse and direct transparency [266].

### 3.2.3 *Job application*

Research on job application privacy has similarities to studies of privacy perceptions in that it examines the extent to which social and legal norms allow companies to collect and process applicants' personal data without being perceived as invading their privacy. For organizations, this is usually about reducing information asymmetry without losing promising candidates.

**PERCEIVED PRIVACY INVASION** Early studies in the 1970s and 1980s therefore focused on identifying (1) which questions for which type of personal information job applicants perceived as being privacy invasive [66, 68], (2) how applicants' perceived level of control over personal information is related to this perception [62], and (3) which information management strategies (e.g., omitting information or lying) applicants used, to keep their privacy intact [68]. Studies after 2000 re-examined these issues from the perspective of the information era [58, 63, 64, 67], further considering the fairness and job relevance of modern selection tests using credit scores [65]. Most recently, the "Privacy and Data Security Concerns Scale" was developed and validated to assess job applicant-specific privacy and data security concerns [60].

**SOCIAL NETWORK SCREENING** The widespread use of OSNs in the 2010s resulted in employers starting to screen their applicants online. Research reacted to this development by extending the well established privacy macro model of Stone and Stone [69] to include the OSN context [59]. It was followed by studies investigating the impact of OSN screening by employers on job applicants' privacy perceptions and their feeling of attraction towards an organization [70], as well as applicants' intentions to protect information privacy when asked for login data to their OSN accounts from potential employers [61].



### 3.2.4 *Workplace monitoring and surveillance*

Employee monitoring has always been a common and accepted practice in the workplace because of its positive effect on job performance [4, 53]. However, technology-enabled monitoring raised privacy issues and led to investigations of its impact on employees.

**IMPACT OF INVASIVE AND UBIQUITOUS MONITORING** Several researchers examined the effects of increased invasiveness and ubiquity of technology-based monitoring. They found that while monitoring of Internet use and location data in the workplace is generally accepted [51, 52], particularly by U.S. citizens, ubiquitous and invasive monitoring through new technologies can have strong negative effects on employee performance [53]. For example, a perceived invasion of privacy by an employers' monitoring activities negatively affects employees' perceived procedural fairness, which can lead to an increased computer misuse by employees [54]. As a result, research on workplace monitoring typically does not focus exclusively on information privacy, but instead examines the impact of monitoring-related privacy concerns on direct determinants of job performance [4]. These include, e.g., employees' trust in management, work motivation, job satisfaction, and psychological strain and stress. With a particular focus on the latter, a number of recent studies have surveyed managers in the U.S. and Europe about the barriers they perceive to the adoption of Internet of Things in the workplace for monitoring employees' mental load and health [50, 52, 55]. They found that while managers believed the technology could help counteract stress, they generally considered its invasiveness to be an intrusion into their employees' privacy, and that the resulting privacy concerns were the main barrier to Internet of Things adoption in practice [52, 55]. They also expressed concerns about the legal basis provided by the GDPR, prompting Gauttier [50] to call for expanded controls on employee use of wearables that allow fine-grained co-determination over purposes, information types, and recipients.

**BEHAVIORAL EXPLANATIONS** In search of explanations for when employees perceive monitoring an invasion of privacy, several studies have applied CPM theory to workplace monitoring to describe the tension that employees often perceive themselves as the owners of information (e.g., work emails), but employers typically have the right to access that information anyway [49, 56, 57]. Research has shown that there is little privacy turbulence once privacy boundaries are established. Nevertheless, secret spying without the employee's knowledge, and monitoring personal matters are perceived as extremely invasive [57]. Another important concern was to examine the negative effects of perceived monitoring of computer-mediated communications in the workplace on trust in management, job commitment, and perceived fairness [49, 56].

### 3.2.5 *Privacy engineering*

Work on privacy engineering targeting the employment context may be divided into studies addressing (1) the development of guidelines and design principles for information system use [92, 93, 94], (2) the application of human-centered design for the implementation of employee and job applicant data subject rights [95, 96, 97], as well as (3) the proposal and implementation of TOMs, including the implementation of PETs [84, 85, 86, 87, 88, 89, 90, 91].

**GUIDELINES AND PRINCIPLES** With the goal of translating theoretical findings from information systems research and formal legal requirements into practical recommendations, some researchers derived design principles and guidelines for various organizational information systems. Voss et al. [93] surveyed user requirements for personalized assistance systems that respect employees' right to self-determination. Based on a persona approach, they derived eight design principles, taking into account PbD. Their principles primarily focus on making the scope and risks of personal data processing transparent to employees, but also provide for the implementation of security and identity hiding mechanisms. Yassaee [94] derived principles for the design of occupational health systems that do not inflate employees' perceived privacy risks. For this purpose, they first derived different sets of principles addressing different determinants of technology acceptance. Employees' perceived effectiveness of the different principles was then assessed using storyboards. They found that principles addressing procedural fairness (e.g., notice, consent) were valued the most. Similarly, Mannhardt et al. [92] analyzed the privacy challenges associated with the use of process mining on data collected from employees in industrial environments. Taking into account the rights and principles of the GDPR and PbD, they developed contextual guidelines for the implementation of transparency and intervention mechanisms as well as TOMs.

**EMPLOYEE DATA SUBJECT RIGHTS** A number of studies aimed at the implementation of employee data subject rights under the GDPR. Polst et al. [96] conducted two workshops with employees in Germany to investigate their requirements towards transparency and self-determination when implementing company privacy dashboards. They found that employees demanded insight into the personal data stored and the underlying permission system. They also expected their employer to handle the data in a legally compliant manner and placed high demands on the usability of the tool. The authors then derived a requirements model and a data usage model for implementing privacy dashboards, but never implemented a dashboard themselves. In contrast, Sahqani and Turchet [97] conducted a full co-design study with employees of a Finnish consulting firm to develop a "MyData" dashboard. The service provides employees with transparency and control over personal data processed for business processes and by enterprise applications. Subsequent usability testing showed that employees had a better sense of control over their personal information when using the tool than before. Furthermore, Gonçalves et al. [95] developed a GDPR-compliant document management system for the HR department to manage job applications. Employees from various enterprises' HR departments were involved in the requirements elicitation and development process, but the solution focused on GDPR compliance in terms of implementing job applicants' data subject rights.

**TECHNICAL-ORGANIZATIONAL MEASURES** In the area of system design and software engineering, we have identified several papers that address the implementation of TOMs and PETs to protect employee privacy. Regarding the tracking of employees, Lucke et al. [90] proposed a client-site semi-automatic computer vision based system to provide accurate and reliable location information while preserving employees' privacy in smart factories. Similarly, Jandl et al. [86] conducted a case study in which they developed a privacy-friendly asset tracking system for an Austrian metal parts company. After identifying issues with the architecture, control capabilities, and configurability of com-

mercially available asset tracking systems, they revised the system to incorporate PbD. Based on feedback from the company's managers and technical staff, they implemented measures to make the processing transparent and to demonstrate accountability.

Turning to privacy issues in authentication, Müller [91] proposed two methods that use either anonymous credentials or organizational measures to ensure the anonymity or pseudonymity of employee logon behavior. In weighing the risks of the two approaches for use in small and medium-sized enterprises, they concluded that there was a tradeoff between the monetary costs and employee trust. Related to this issue, scholars have investigated privacy threats raised by radio-frequency identification technology in the workplace, including information leaking, tracking, and inventorying [89]. Karger [87] further conducted a formal analysis of the privacy and security threats posed by government employee ID cards and proposed extensions to the protocol and standard to protect cardholder privacy from unintended information leakage.

Regarding the use of corporate security protection measures, Kim and Kim [88] addressed privacy risks posed by data leakage prevention systems and proposed a log anonymizing method and system architecture as a mitigation strategy. Likewise, Gudo and Padayachee [85] analyzed the threats to employee anonymity and confidentiality of private information resulting from malware scanning in organizations that have adopted BYOD. In response to the lack of privacy properties of existing solutions, they developed a malware detection framework, in which they proposed the use of multiple privacy-preserving modules for different malware detection measures. In addition, Fahrenkrog-Petersen et al. [84] addressed the hazards of using process mining on detailed log data in tech-enabled industries. They presented an event log sanitization algorithm based on t-closeness to protect employees from trace linking attacks that would reveal identity, membership, and attributes.

Last but not least, Gan et al. [270] conducted a qualitative study in which they interviewed nine employees from a Malaysian company that had implemented PETs to protect the personal data of their customers. They found that, depending on the job profile, PETs had a different impact on employees' workload and time to complete tasks. Moreover, they found that communication and data access became more systematic and replaced other communication channels. Besides, employees considered PETs useful to protect personal data and accepted both the technology and the subsequent changes to the work processes. However, their participants noticed deficiencies in the limited communication strategy by their employer, and raised concern about the PET's vendor having access to personal data and a lack of feature updates.

### 3.3 METHODOLOGIES, SAMPLING, AND PARTICIPANTS

In addition to categorizing the studies into different topics, we also divided them into six different types of methods employed, and four types of participants involved. We also identified a total of 15 different samples used in the studies. In doing so, our literature review reveals some major biases in previous studies of information privacy in the employment context. A summary of these findings is presented in Figure 3.1.



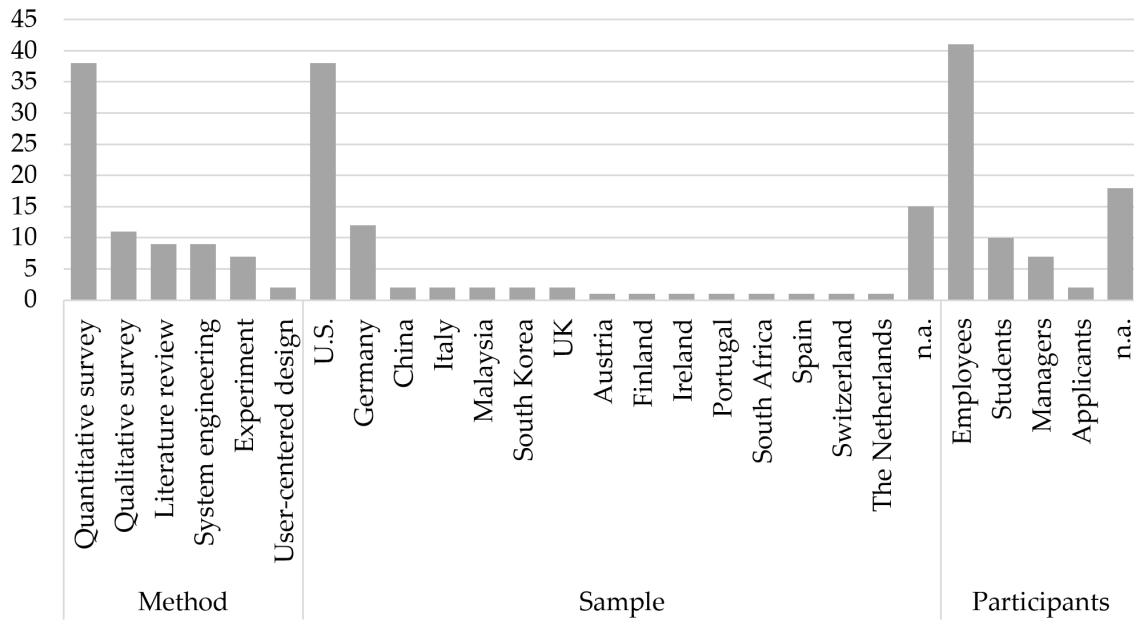


Figure 3.1: Quantification of identified methods, samples, and participants in employee privacy research. Studies are counted multiple times if there were multiple methods, samples, and participants used.

### 3.3.1 Methods

Starting with the methods, we concentrate on empirical studies that included participants. We discovered that more than half of the studies relied heavily on quantitative research methods, primarily surveys. The majority of papers that reported a quantitative survey design relied on causal modeling derived from privacy macro models and various behavioral theories. As such, their surveys were mostly based on well-defined scales to apply some form of Structural Equation Modeling (SEM) or regression analysis to test their hypotheses. This also applies to experiments that compared different treatments. Few exceptions made use of open-ended online surveys [127], and mixed methods approaches [118]. A summary of all analysis techniques identified is provided in Figure 3.2.

Furthermore, the number of qualitative studies found is much smaller (cf. Figure 3.2). Such studies were mainly based on semi-structured interviews and a form of coding inspired by either grounded theory or thematic analysis [30, 33, 259, 265, 270]. The very few studies conducted with a HCD approach or systems engineering also used requirements analysis and usability testing [95, 97].

### 3.3.2 Study samples

Regarding the samples used, we found that more than half of the studies reported using U.S. samples, while one third of the studies included samples from Europe, especially Germany [2, 3, 31, 33, 38, 39, 41, 55, 96, 259]. However, samples from other parts of the world are rarely represented. This highlights a clear bias in current privacy research towards influences from Western cultures. In addition, there is also a clear bias towards the subject of the studies (cf. Figure 3.3). U.S. samples have particularly dominated studies

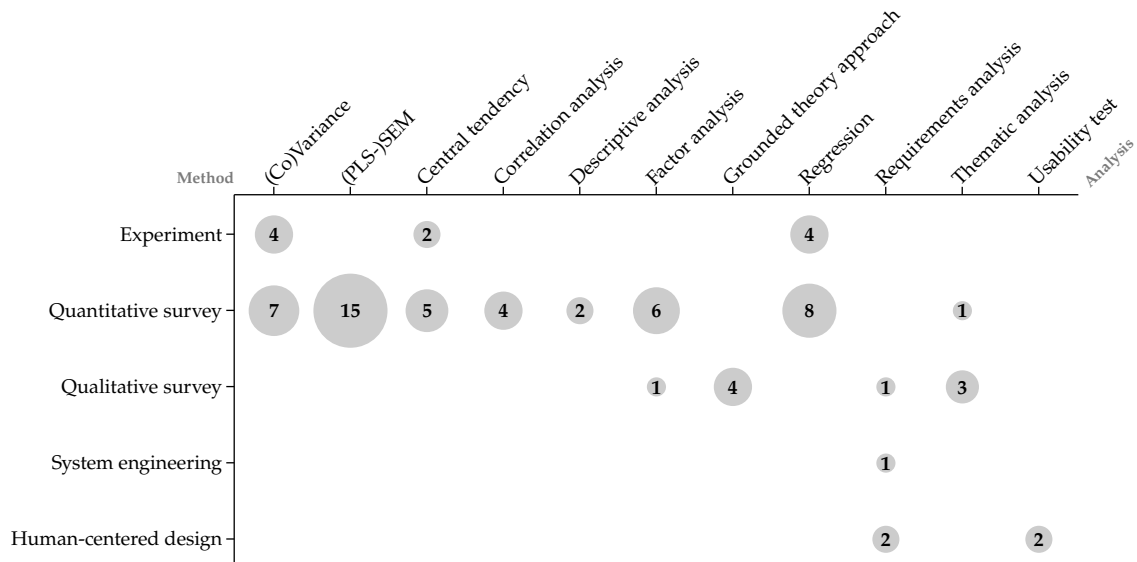


Figure 3.2: Cross table of method and analysis used in related work. Studies are counted multiple times if there were multiple analysis techniques applied. The figure excludes papers not having participants.

on job application (79%) and information privacy perceptions (60%), but are completely absent from privacy engineering studies. Studies with samples from Europe, on the other hand, have focused strongly on information system use, privacy engineering, and workplace monitoring, but have largely omitted the field of information privacy perceptions. In fact, only three studies with samples from Germany and the UK have focused on this topic. We note that the studies from Germany were published only recently, after our own research had already been completed. Consequently, today's theoretical foundations for understanding employees' perception of information privacy in employment are based almost entirely on an Anglo-American view. This bias was also reported in another recent literature review on workplace privacy [25].

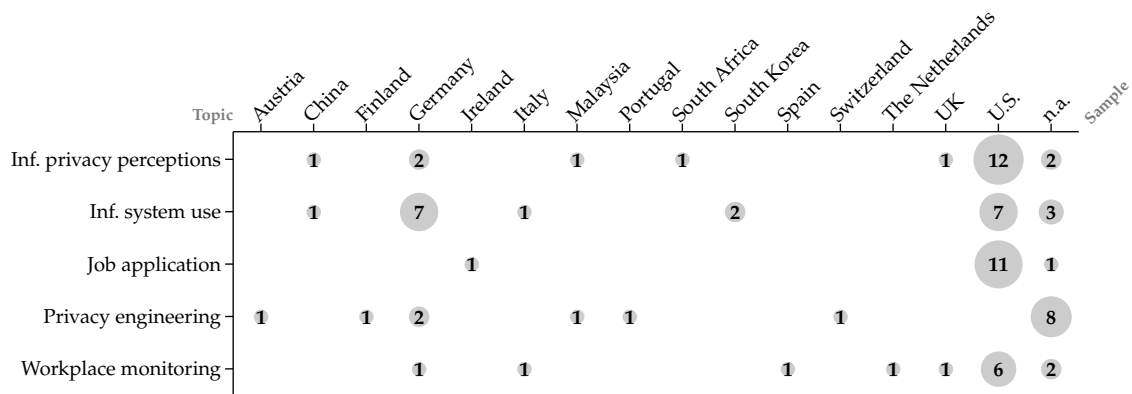


Figure 3.3: Cross table of sample and topic in employee privacy research. Studies are counted multiple times if there were multiple samples used.

### 3.3.3 *Study participants*

In terms of participants, two-thirds of the studies that involved participants included employees. Students were still present in 17% of the studies. This was particularly the case in studies on job application [58, 63, 64, 65, 68, 76]. True job applicants, on the other hand, were only found in two studies [66, 70].

## 3.4 DEMARCATION OF THIS DISSERTATION

This section summarizes how this dissertation demarcates itself from related work and topics outlined above. To this end, we have divided the topic areas into three categories that reflect the means by which employee privacy has been studied.

### 3.4.1 *Privacy as a determinant to employee acceptance*

Three themes have in common that employee privacy is studied predominantly from an organizational perspective, examining privacy as only one of many determinants that influence employee acceptance of certain policies and technologies: Work related to *information system use* is primarily concerned with examining employees' adoption of technology from a change management perspective to ensure return on investment; work related to *job application* concerns applicants' acceptance of potentially privacy-invasive screening measures employed by organizations; and work related to *workplace monitoring and surveillance* concerns employees' acceptance of potentially intrusive measures and technologies. All these topics aim to examine potential negative and adverse effects caused by employees' privacy concerns, and to identify individual privacy factors that favor employees' adoption. Thus, employees' views primarily serve as a means to an end to provide benefits to employers.

This dissertation demarcates itself from these works by taking an opposite view, considering privacy not as a factor of acceptance, but as a fundamental right to be implemented, and whose exercise by employees must be guaranteed by legal and social norms. Instead of a fragmented view of individual privacy factors, we present a holistic view of employees' conceptualizations of the right to privacy. Consequently, this dissertation complements previous work by providing missing fundamental knowledge for privacy engineering and research to holistically consider the right to privacy in systems engineering and information systems implementation. This dissertation thus contributes to the identification of additional factors of employee privacy to consider not only organizational concerns, but also legal, social, ethical, and employee requirements regarding a right to privacy that need to be taken into account.

### 3.4.2 *Conceptualizing privacy as an opt-out right*

The vast majority of research throughout all topics presented above is based on quantitative surveys and experiments that build on established theories and macro models, which in turn are based almost exclusively on studies from the Anglo-American world, where employee privacy is far less normatively protected by legal frameworks than in Central Europe [82, 83]. As a result, previous work suffers from two major issues, which

this dissertation counters. First, previous work is strongly embedded in the U.S. context well before modern privacy laws, in which privacy is framed as *the right to freedom from intrusion* [81]. According to this view, the processing of employee personal data is always allowed, unless employees prove an expectation of privacy for a specific processing operation, which, however, is rarely recognized in practice [82, 83]. As a result, privacy is conceptualized as an “opt-out right”, in which privacy is shaped by laws or court decisions that explicitly prohibit certain processing. Obviously, this view is diametrical opposed to the view of privacy as the fundamental right to informational self-determination, which conceptualizes privacy as an “opt-in right”. The Anglo-American view thus strictly contradicts the principle of “prohibition with subject of permission” in Central Europe and Germany (cf. Section 2.2.4). Thus, previous work is subject to different legal and social norms, and its application to Germany and Europe would contradict the principles of both information privacy (cf. Section 2.1) and privacy engineering (cf. Section 2.3). Consequently, previous work does not reveal how employees conceptualize the design of a “right” to privacy in the first place. As a result, previous works’ results, in particular those related to the topic *employee privacy perceptions*, are simply not applicable to the implementation of employees’ right to privacy under the right to informational self-determination.

This dissertation addresses these issues by providing preliminary fundamental knowledge of theoretical and abstract concepts of employee privacy, taking into account modern and European perspectives. In this vein, we present the first conceptualizations of employees’ right to informational self-determination and in-depth empirically derived findings on employees’ privacy perceptions. These findings lay the foundation for future research and privacy engineering processes of *knowledge management*, *risk management*, *stakeholder needs and requirements*, and both *system* and *architecture definition* (cf. Section 2.3).

### 3.4.3 Privacy implementation

In general, all approaches to guidelines and principles, as well as most approaches to *PETs*, suffer from the fact that their design is based on knowledge outside the employment context and that the actual stakeholders, i.e., employees, were not involved. As such, the results lack an empirical foundation that does justice to the contextual nature of privacy (cf. Section 2.1) and conflict with the requirement to respect contextual factors in privacy engineering (cf. Section 2.3). Our work proves that contextual differences exist, but also provides missing contextual, empirical insights about employees’ conceptualizations of privacy that were lacking.

In addition, work on *PETs* has focused on privacy-by-architecture approaches from a purely technical-legal point of view, neglecting the socio-technical nature of privacy. Work that focused on the implementation of data subject rights neglected the limited self-determination rights of employees. Our work complements previous approaches by being the first to focus on the key role of data processing employees for employee privacy protection and providing the first privacy pattern for employee personal data management resulting from a *UCD* study. The findings support researchers and privacy engineers, especially in the processes of *knowledge management*, *architecture definition*, and *design definition* (cf. Section 2.3).

### 3.5 SUMMARY

In this chapter, we have presented the current state of research on information privacy in employment. We have shown that most of the research emphasis is on investigating (adverse) behavioral effects. Although the topics covered are complementary to our own research objectives (cf. Section 1.2), they often reside in theories that primarily aim to identify and address issues of technology acceptance and organizational compliance.

Moreover, previous work is subject to an enormous cultural bias, especially through U.S. samples and conceptualization of privacy that are deemed incompatible with European views of privacy. Therefore, previous results must be regarded with caution when being applied today. Our research addresses this issue by providing preliminary and holistic insights on employees' perceptions in Europe under the right to informational self-determination.

In addition, most work on privacy engineering has focused on ensuring employee anonymity in log data, or developing remediation strategies, either in the form of design principles or through PETs. However, only two studies have employed a comprehensive UCD approach and actually developed and tested a prototype with employees. Our work complements previous work in that we provide fundamental knowledge useful to design employee data subject rights. We also extend previous efforts by broadening the view to include data processing employees in the protection of employee privacy and providing the first privacy pattern specific to this stakeholder group, emerging from a UCD process.



## PROBLEM STATEMENT AND RESEARCH QUESTIONS

---

*Problems are not stop signs,  
they are guidelines.*

— Robert H. Schuller

Our review of available work on information privacy in employment, presented in Chapter 3, revealed some major biases and limitations in terms of its applicability to the implementation of employees' right to privacy. Particularly striking is the lack of insights on employees' conceptualizations of a right to privacy in a European context, which is urgently needed for the necessary privacy engineering process to implement employee-centric privacy controls. Another shortcoming is the focus on [PETs](#) that ignore employees' perspectives, or on [PETs](#) that solely target employees in their role as data subjects. These shortcomings prevent the implementation of effective privacy measures, i.e., measures that preserve employees' freedom and exercise of rights, under the foundations set forth in Chapter 2; either, because lacking fundamental knowledge prevents privacy engineering processes being performed correctly, or because restrictions of employees' rights under employment hinder them from protecting their own privacy to an extent known from other contexts. In the following, we discuss both shortcomings and, in particular, highlight the resulting research questions that are addressed in this dissertation. In Section 4.1 we focus on issues related to the generation of fundamental knowledge regarding employees' conceptualizations of privacy in a European context. We then address issues related to the lack of consideration of data processing employees in Section 4.2. Finally, we conclude this chapter in Section 4.3 with a summary of the identified problem areas and research questions.

### 4.1 EMPLOYEES' CONCEPTUALIZATIONS OF MODERN AND EUROCENTRIC PRIVACY

In laying out the foundations of this dissertation in Chapter 2, it was shown that with the [GDPR](#) coming into force in 2018, the European understanding of privacy has dramatically influenced the discourse on privacy protection worldwide with numerous jurisdictions following the regulation's lead. Thus, the core principles associated with recognizing informational self-determination as a fundamental right in an information society will also have a significant impact on how privacy is shaped in employment contexts, both today and in the future. Our literature review in Chapter 3 revealed, however, that the current state of research on employee privacy does not reflect this development. Instead, it remains within a historically U.S.-influenced framework, which tends to define privacy in terms that are incompatible with the European and German conception of privacy (cf. Section 3.4.2). Thus, for the implementation of employee privacy under the right to informational self-determination, there is simply a lack of indispensable fundamental knowledge to do justice to the nature of privacy as a socio-technical and not a purely technical-legal matter (cf. Section 2.3 & Section 2.4). According to the state of the art



and best practices in privacy engineering and usable privacy [8, 9, 12, 13, 15, 16, 23, 24], fundamental knowledge required in essential systems engineering processes, such as *knowledge management*, *risk management* or *stakeholder needs and requirements*, refers to a stakeholder-specific understanding of factors including, but not limited to, privacy needs, awareness, concerns, and capabilities, as well as theoretical and abstract privacy concepts, such as mental processes related to privacy issues and perceptions of personal data. To summarize, what is essentially required is fundamental knowledge of how employees conceptualize (the right to) privacy. Indeed, our literature survey in Chapter 3 revealed a lack of holistic evidence on employee privacy perceptions in relation to contemporary and Eurocentric concepts of privacy (cf. Section 3.4.2), which is in stark contrast to research on user privacy in the online context [208, 213, 214, 271, 272]. We argue that such efforts must be extended to the employment context to generate insights that contribute to a modern understanding of privacy in employment relationships and have high practical relevance for the effective implementation of employees' right to privacy. To address this concern, we divide our research on this topic into the broader conceptualization of the right to informational self-determination in employment and the conceptualization of the perception of personal data.

#### 4.1.1.1 *Internal conceptualizations of informational self-determination*

The broader challenge of employee-centric privacy design is to develop processes, systems, and privacy controls that meet both legal requirements and business needs, but also the (privacy) needs, requirements, capabilities, and concerns of employees (cf. Section 2.3). In particular, legally mandated privacy controls that employers must implement and guarantee can only protect privacy in employment to the extent that they align with employees' awareness and perceptions of personal data processing as well as their privacy rights and obligations. In HCI methodological terms, the challenge is therefore to match employees' "mental models" of information privacy with the legal and organizational framework's "conceptual model" of the "target system" information privacy (cf. Section 2.4.3). In the presence of distortions, appropriate corrective actions must be taken to develop privacy controls that are deemed effective, efficient, and satisfactory.

A lack of alignment is likely to render privacy controls ineffective, either because employees are unable to exercise their rights, or because they perceive a violation of their privacy, as the controls do not meet their expectations. This would not only render the principles of the GDPR and the right to informational self-determination absurd, but also mean that employers do not fulfill their accountability to uphold these principles (cf. Section 2.2). Additionally, known adverse effects in the employer-employee relationship may occur, such as declining trust in employers, misuse of information systems, declining work performance, or falsification of personal data [3, 4, 31, 49, 53, 54, 56, 64, 70, 77].

To address these issues and fill existing knowledge gaps, we explore employees' conceptualization of privacy to provide deep insights into employees' understanding of the right to privacy, data processing, data flows, expected safeguards, and threat models. This leads to our first research question:

**RQ1** "What are employees' internalized conceptualizations of the privacy framework under the right to informational self-determination in employment?"

Answering this question addresses research gaps of a theoretical nature by complementing previous work that has focused only on the conceptualization of privacy through privacy macro models for the purpose of measurement [73, 125, 259, 265], and separated the dimension of information privacy from other dimensions [118]. The answer to the question is also of practical importance, as it makes the system “privacy in employment” tangible and lays the foundation for both HCD and privacy engineering in the employment context under usable privacy aspects [12]. In particular, gained insights are useful to build knowledge repositories with high contextual validity, determine employment-specific risk probabilities and threats, elicit and define stakeholder and system requirements, and assess and select appropriate architectures (cf. Section 2.3). Furthermore, answering this question helps researchers, designers, and engineers to grasp what understanding and needs underlie the elicitation of requirements in earlier user-centered approaches [96, 97] and how their concrete transformation into system requirements can succeed (cf. Section 2.4.3).

#### 4.1.2 *Privacy perceptions of personal data*

An essential element in the conceptualization of privacy is the concept of personal data it contains, which is thus also of great relevance for privacy engineering and human-centric privacy research [9, 12, 15, 16, 143]. As laid out in Section 2.2, employees have limited ability to decide on the nature and extent of personal data processing because laws or employers' interests outweigh employees' privacy interests. Yet, most of these data are perceived by users as highly sensitive in the online and marketing contexts [271, 273, 274]. In addition, numerous studies on online environments, smart device use, and marketing show that different types of personal data are also perceived differently by users in terms of sensitivity [245, 246, 271, 273, 274, 275, 276, 277, 278, 279, 280]. In contrast, knowledge on perceived data sensitivity in the employment context is strictly limited to work from the U.S. prior to 2000 [66, 79, 80, 281]. However, the extent to which the mandatory disclosure of much personal data affects employees' perceptions of data sensitivity and willingness to disclose data has not been studied, despite the increase in disclosure. This is complicated by the fact that privacy is known to be a contextual concept [26, 27, 28], making it infeasible to generalize results from other research areas and cultures with different social norms to the employment context in Europe and Germany in particular. Consequently, the current situation prevents the effective application of usable privacy design strategies.

**DIFFERENCES IN PERCEPTIONS OF PERSONAL DATA** In the absence of insights, practitioners today have no choice but to adhere to formal classifications of data sensitivity prescribed by applicable standards and legal texts (cf. Section 2.2.3). This imposes a purely technical-legal view that ignores socio-technical aspects, in that it is unclear whether formal classifications of personal data are consistent with employees' perceptions of what constitutes sensitive data and their willingness to disclose truthful data. As a result, essential prerequisites of user-centric privacy engineering are not fulfilled, which then leads to unfounded conclusions for the implementation of privacy controls and system architectures [15, 16]. This increases the risks of provoking a perceived invasion of privacy for employees and unnecessarily straining the employer-employee

relationship [9]. Employees may also perceive privacy controls as useless because they do not receive the control or information they expect.

For these reasons, privacy research in other domains has aimed to explore perceptions of personal data and identify different groups of data to better understand and design data processing activities [251, 271, 273, 274, 278, 282]. We argue that similar efforts need to be made for the employment context in order to provide designers and engineers with contextual and empirically derived results. This leads us to the formulation of our second research question:

**RQ2** “How do personal data differ in terms of their perceived sensitivity and willingness to disclose by employees?”

Research further suggests that perceived data sensitivity and willingness to disclose are influenced by numerous antecedents (i.e., factors related to privacy) studied in privacy macro models (cf. Section 2.4.4) [69, 245, 246, 274, 276]. Our literature review in Chapter 3, however, revealed gaps in the understanding of these determinants; numerous antecedents have been examined solely in the context of the intention to use a particular information system or to accept organizational procedures. Unlike previous research, we seek to understand which antecedents affect employees’ perceptions of personal data and how this relates to different types of personal data. We also aim to understand how employees’ conceptualization of privacy affects these antecedents. We thus formulate our third research question:

**RQ3** “Which antecedents influence employees’ perceptions of personal data?”

Answering these questions fills glaring gaps in research on theoretical and abstract concepts of employee privacy [25]. At the same time, the results (1) provide the missing fundamental knowledge for privacy engineering to create employee-centric data taxonomies [16] and translate them into effective privacy strategies as part of a risk management process [10, 99], (3) to develop employee-centric privacy controls [16], and (4) to understand privacy spheres in employment and derive appropriate solutions [15, 20].

**EMPLOYEE GROUPS AND CLUSTERS** Privacy research has made enormous efforts to account for individual differences by categorizing people into groups. Segmentations of people are found useful (1) to assess the willingness to disclose in marketing settings [283], (2) to study the impact of service features on different users [284], (3) to serve developers and service providers in developing products [285], and (4) to help resolve the privacy paradox [286]. Most attempts classify people based on their privacy concerns [280, 283, 285, 286, 287, 288, 289, 290, 291, 292]. Fewer attempts are based on people’s perceived data sensitivity, willingness to disclose, and behavior [251, 293, 294, 295, 296]. For the employment context, however, our literature review revealed that no comparable approaches to segmentation have been pursued to date. Indeed, little attention has been paid to the element of uniqueness in employees’ privacy perceptions overall. Yet, the high level of diversity among employees is unlikely to allow for a uniform model of privacy perceptions. We expect that privacy engineering for employee privacy would therefore benefit from considering the uniqueness of privacy perceptions in the manner described above. Consequently, we formulate our fourth research question:

**RQ4** “Can employees be categorized based on different perceptions of personal data?”

Addressing this issue contributes to filling existing research gaps [25], and is also timely and important as more and more data about employees are collected and processed. Answering this question can be leveraged for the design of user-centric *PETs* and *TETs*, by understanding which data are perceived as sensitive by employees and what differences exist among employees.

#### 4.2 DATA PROCESSING EMPLOYEES AS LEVERS FOR EMPLOYEE PRIVACY

Turning towards practical issues of implementing employee privacy in organizations, our literature review in Chapter 3 illustrates clearly that current efforts focus on either data minimization through anonymization, or to apply techniques of *HCD* to implement data subject rights. While these are essential contributions for the preservation of employee privacy, this state does not do justice to the fact that employee personal data are often required for numerous business processes in a non-anonymized form, and that employees are often obliged to disclose personal data while the legal framework restricts rights to data correction (cf. Section 2.2.5). The preservation of employee privacy therefore depends to a large extent on both the correct implementation of *TOMs* by employers and the correct application of *TOMs* by data processing employees, i.e., the entities who process other employees' personal data on behalf of the employer.

For this to succeed, *TOMs* must incorporate usable privacy criteria and thus be designed human-centered to meet the needs of data processing employees [12, 16]. Privacy research, however, has so far ignored this stakeholder group and its unique responsibility for protecting employee personal data. Instead, *TOMs* have been viewed almost exclusively from the perspective of data subjects [19] and from the perspective of organizations [297]. With regard to the latter, research has focused on the overall *GDPR* readiness of organizations and focused exclusively on the perspective of employees in management positions. While there have been *HCD* approaches to privacy policy management tools, these have also focused only on the perspective of managers [98]. To summarize, the requirements and perspectives of data processing employees as a key user group of *TOMs* have simply been neglected. In terms of privacy engineering of *TOMs* under aspects of *HCD*, this means that there is a lack of foundations, such as privacy patterns and *PETs* for implementing *PbD* principles. This situation clearly contradicts the fact that the implementation of *PETs* has been shown to cause workflow disruptions and unintended side effects, such as increased workload for data processing employees [270].

As a result, we argue that the effective implementation of *TOMs* necessitates user-centric approaches for those who process employee personal data, as they occupy a fundamental position when it comes to putting data protection goals into practice. This view is consistent with calls from the security and privacy research community to expand the scope beyond data subjects to include, e.g., administrators and developers [298]. Accordingly, this leads us to the following research question:

**RQ5** “How can data processing employees be effectively, efficiently, and satisfactorily supported in the data protection compliant processing of employee personal data?”

Answering this question not only fills research gaps, but also has practical significance for the design of employee personal data processing. By understanding stakeholder requirements, the results facilitate the effective consolidation of business processes, data management processes, and data protection processes to meet key principles of *PbD*,

such as *privacy as the default*, *privacy embedded into design* and *full functionality - positive sum, not zero-sum* (cf. Section 2.3.1). In addition, we expect that usable TOMs promote privacy-compliant handling of personal data by data processing employees, thereby reducing the risks of data breaches and supporting employers in their accountability obligations. The insights gained also contribute to deriving principles and patterns for the implementation of TOMs, which can then support privacy engineering in *architecture definition* and *design definition* processes (cf. Section 2.3). Employers, developers, and researchers are thus given the opportunity to address further aspects in the future design of TOMs for employee privacy.

#### 4.3 SUMMARY

In this chapter, we defined our problem statement and derived our research questions based on the foundations presented in Chapter 2 and our literature review laid out in Chapter 3. The problem statement breaks down into two problem areas. The first is to lay important foundations for employee-centric privacy engineering, i.e., privacy engineering that incorporates human factors and takes into account employees' views, expectations, and capabilities. To this end, we derived four research questions that aim to generate fundamental knowledge about employees' conceptualizations of privacy, taking into account factual privacy law and the specifics of the employment context. More specifically, **RQ1** targets to understand employees' conceptualizations of (the right to) privacy in employment, while **RQ2 - RQ4** aim to understand the conceptualizations and perceptions of employee privacy in relation to personal data in particular.

Second, we complement previous attempts to enforce employee privacy rights by shifting the focus to data processing employees and their responsibility for employee privacy due to employees' limited self-determination rights. To this end, we derived research question **RQ5** that focuses on developing usable solutions for data processing employees to assist them in handling employees' personal data in a privacy-compliant manner and, as a consequence, to support employers in their accountability obligations.

## STUDY I — EMPLOYEES’ CONCEPTUALIZATIONS OF THE RIGHT TO INFORMATIONAL SELF-DETERMINATION

---

*A conceptual model is an explanation, usually highly simplified, of how something works. It doesn’t have to be complete or even accurate as long as it is useful.*

— Donald A. Norman

In this chapter, we address the current lack of understanding about employees’ internal conceptualization of the right to privacy under **RQ1**, derived in Section 4.1. To this end, we explored potential issues by conducting a semi-structured interview study with 27 employees in Germany and elicited mental models of the right to informational self-determination. Based on our publications [100, 101], this chapter provides insights into employees’ (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. The resulting findings provide valuable input for the design and engineering of employee-centric privacy controls, privacy-friendly systems, and privacy-friendly processes

The remainder of this chapter is structured as follows: First, we present the background and research model in Section 5.1. This is followed by details on our procedure and methods for designing and conducting our study, along with details on ethical consideration and data analysis in Section 5.2. Next, we present employees’ perceptions of categories of data in Section 5.3, followed by employees’ conceptualizations of the right to informational self-determination in Section 5.4, and insights on employees’ perceptions and awareness of personal data processing in Section 5.5. Afterwards, we discuss our results’ implications in Section 5.6, and discuss limitations of our study in Section 5.7. We finally conclude this chapter, summarizing our findings in Section 5.8.

### 5.1 BACKGROUND AND RESEARCH MODEL

To address **RQ1** “*What are employees’ internalized conceptualizations of the privacy framework under the right to informational self-determination in employment?*” we subdivided our research into three key research topics, as detailed in the following subsections.

#### 5.1.1 Perceptions of categories of data and terminology

The right to informational self-determination stipulates different rules for the processing of different categories of data (cf. Section 2.2.3). Legal texts use different terms both to refer to such categories and to express rules for processing. In practice, employees are often confronted with both legal and non-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, we found that privacy policies in office clouds use terms interchangeably or add non-privacy related terms, and even use the same terms to describe access rights (e.g., “private” document or calendar) without considering the exact legal meaning [106]. To date, it is unknown how employees perceive these terms and the implied legal meanings. Since legislation obligates employers to “provide any information [...] using clear and plain language” (Art. 12 GDPR), identifying potential misconceptions is of high practical relevance. To provide preliminary insights on employees’ perceptions and familiarity with these terms, we derive the following sub-research question:

**RQ1<sub>a</sub>** “What are employees’ conceptualizations of different categories of data under common terminology found in practice?”

#### 5.1.2 *Concepts of informational self-determination*

As outlined in Section 2.2, the employment context grants extensive information rights to employees, but only limited intervention. 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 generally be audited by DPOs and employee representatives. To reveal employees’ conceptualizations of the current organizational and legal framework, as well as their requirements for transparency and intervention, which they derive from their right to privacy, we derive the following sub-research question:

**RQ1<sub>b</sub>** “What are employees’ internalized conceptualizations of the right to informational self-determination in employment?”

#### 5.1.3 *Awareness and perception of personal data processing*

Past studies revealed that people have a poor understanding of the data flow and infrastructure of information systems they use every day [232, 299]. However, adequate awareness of these aspects is vital in drawing accurate conclusions regarding security and privacy [12, 23, 300, 301]. In the case of the processing of personal data, according to Art. 13 and Art. 14 GDPR, this also includes being aware of when and how personal data are disclosed. In this regard, the legislator has clarified 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). To date, however, it remains largely unknown how employees’ privacy awareness is shaped. Although employees are known to expect their personal data to be protected [35], it remains unknown what employees believe with respect to which precise safeguards are implemented, and which threat models exist. Similarly, there is a lack of insights into what privacy invasions by employers employees actually anticipate. To investigate employees’ perceptions of personal data processing, including their perceptions on safeguards and threat models, we derive the following sub-research questions:

**RQ1<sub>c</sub>** “How do employees perceive the process of self-disclosure?”



**RQ1<sub>d</sub>** “What are employees’ awareness of data processing with respect to data storage and data flow?”

**RQ1<sub>e</sub>** “What are employees’ conceptualizations of implemented safeguards to protect privacy in employment?”

**RQ1<sub>f</sub>** “What are employees’ conceptualizations of threat models to privacy in employment?”

**RQ1<sub>g</sub>** “What potential invasions of privacy by employers are employees aware of?”

## 5.2 METHODOLOGY

To answer our research questions, we conducted a mental model study based on semi-structured interviews with 27 employees from Germany during the period July until September 2019, and in August 2020. We chose a mental model approach, because mental models themselves represent the conceptualizations we aim to identify and because mental models have been used before to answer similar research questions (cf. Section 2.4.3). In the following, we discuss how we addressed ethical considerations in Section 5.2.1, followed by details on the applied methodology in Section 5.2.2, the interview guidelines in Section 5.2.3, the study procedure in Section 5.2.4, the participants’ recruitment in Section 5.2.5 and demographics in Section 5.2.6, and on the evaluation and data analysis in Section 5.2.7.

### 5.2.1 *Ethical considerations of the study*

We made sure to minimize potential harm to the employees participating in our interview study by adhering to 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, and was approved by the works council and/ or the management of organizations we contacted for recruitment. All participants were informed of the basic content and objectives of the study, and were asked to provide informed consent. After the interview was completed, we disclosed full information on the background of the study. We collected data anonymously when possible or when not possible, pseudonymized or anonymized the data after the interviews. In particular, we removed all direct identifiers from the transcripts. Any contact information was stored separately and was not linked to the participants’ responses. 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.

### 5.2.2 *Method selection*

The elicitation of mental models requires the extraction of subjects' internal representations and can be done either directly or indirectly [302]. 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 [223]. 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 [303]. 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 [304]. In order to overcome the limitations, a combination of at least two elicitation techniques is common [225, 227, 299]. Thus, we chose to conduct our interviews using both verbal and graphical elements, as given that informational self-determination is a highly abstract concept.

### 5.2.3 *Interview 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 the right to informational self-determination. Thus, to design an appropriate interview guideline, we adopted an expert model approach [305], as it has been proven to be valuable in eliciting mental models on computer security and privacy [240]. 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 and a diagrammatic summary of the development process is available in Figure 5.1. We derived interview guidelines from the model and revised them with three researchers experienced in conducting interviews. We also conducted three pilot interviews with employees to fine-tune the questions and wording. Our interview guidelines are available in Appendix B.1.

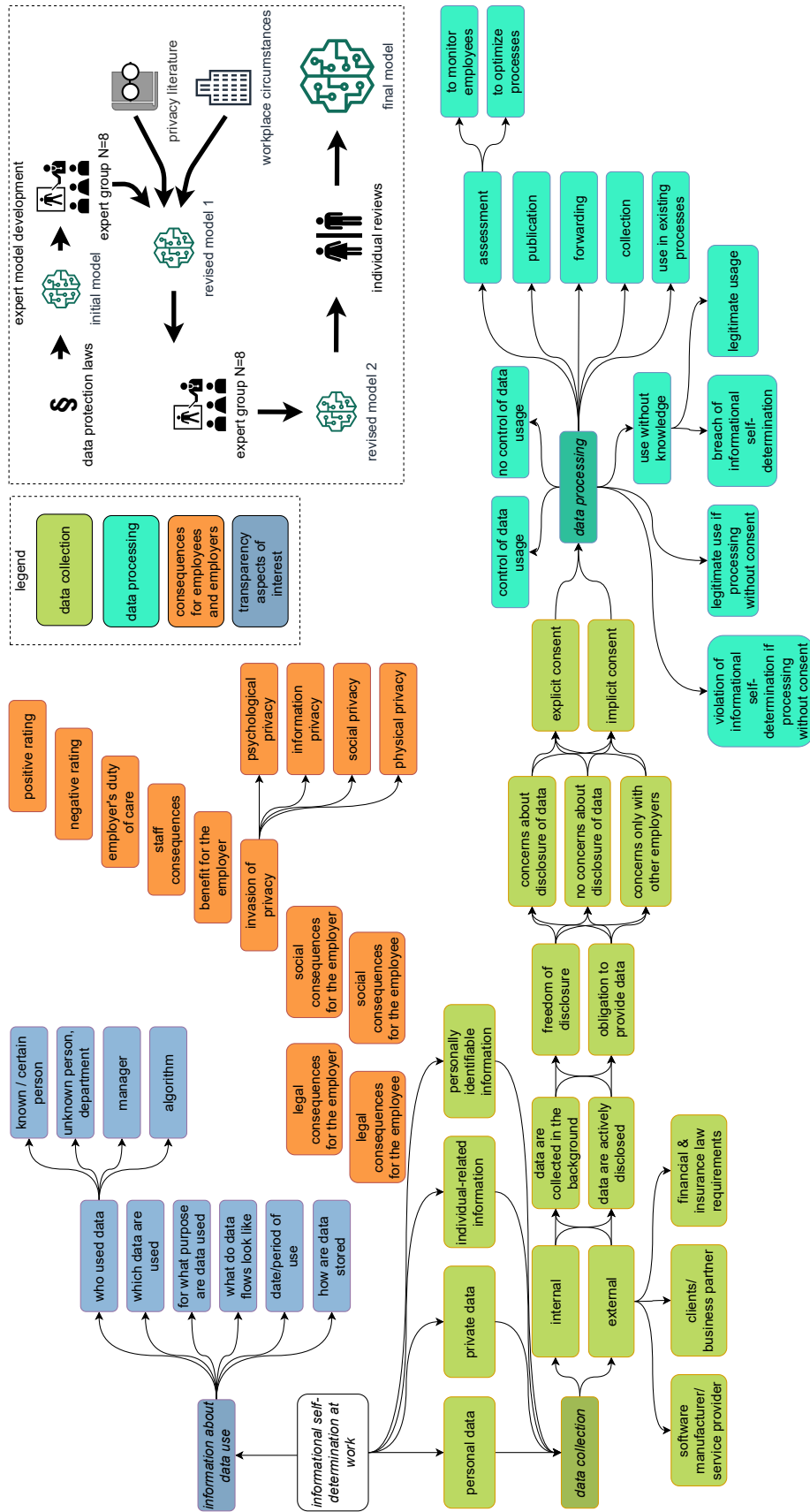


Figure 5.1: Expert model of the right to informational self-determination in employment.

#### 5.2.4 Study 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.

To examine **RQ1<sub>a</sub>** *“What are employees’ conceptualizations of different categories of data under common terminology found in practice?”*, we presented the following six terms for categories of data in a random order to our participants: “Data” (German: “Daten”), “information” (German: “Information”), “personal matters data” (German: “Persönliche Daten”), “personal data” (German: “Personenbezogene Daten”), “personal identifiable data” (German: “Personenbeziehbare Daten”), and “private data” (German: “Private Daten”). We then asked them to give definitions and examples of the terms, taking into account their employment and the previously mentioned working tools.

Next, to address **RQ1<sub>c</sub>** *“How do employees perceive the process of self-disclosure?”* and **RQ1<sub>g</sub>** *“What potential invasions of privacy by employers are employees aware of?”*, we discussed various topics of control and transparency over personal data with our participants. We asked them to explain their abilities and liberties in disclosing data to employers, and encouraged them to discuss ways in which their privacy could be violated. To examine **RQ1<sub>b</sub>** *“What are employees’ internalized conceptualizations of the right to informational self-determination in employment?”*, we then asked for explanations of the concept of informational self-determination and its relevance to the employment relationship. We concluded the discussion with the question *“what is informational self-determination in employment?”*

Following that, we used a drawing task to examine employees’ conceptualizations of safeguards, threat models, and data processing under **RQ1<sub>d-f</sub>**. To this end, we presented our participants a sheet with the different data types “bank details”, “salary”, “private address”, and “telephone records” printed on it. Next, we asked our participants 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.

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.

Please note that referring to payroll preparation is a common choice to examine privacy related issues in employment relationships [306]. Employees are familiar with this processing, and it involves the sharing of sensitive personal data, including the social security number, name, address, birth date, marital status, religious affiliation, child allowance, handicap allowance, and account number. In contrast, other types of data, such employees’ or their children’s birth certificates, are often times inaccessible to employers unless there are special regulations. 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 with TOMs. Lastly, processing of pay-

roll information serves as a good proxy for studying awareness, because it restricts the intervention, but not the transparency properties of the right to informational self-determination.

#### 5.2.5 *Participant recruitment and enrollment*

Since demographic variables correlate to different privacy perceptions [307], 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 works council 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 to 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 employees directly to participate in the study if their demographic details matched our recruitment target. To counteract demographic imbalance, we also contacted employees 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.

#### 5.2.6 *Participant demographics*

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, six worked in micro companies (< 10 employees), seven in medium companies (< 250 employees), and 14 in large organizations ( $\geq 250$  employees). Typical for office workers, the level of education in our sample was relatively high, as 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 com-

prised 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 compilation of all participants' demographic information is available in Table 5.1.

### 5.2.7 *Evaluation and data analysis*

We conducted a qualitative analysis of our interview data by carrying out both deductive and inductive coding. We chose this approach because it expanded the coding topics covered by our expert model to include topics generated from the content of the interview itself. For coding, we followed established guidelines and common practices for semi-structured interviews [308, 309]. 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.

For deductive coding, the previously created expert model was used as the codebook. Both coders independently coded a randomly selected 50% subset of the interviews. In a subsequent revision step, a "negotiated agreement approach" [308] was used to discuss disagreements and resolve coding differences by revising the categories and coding scheme in order to avoid interpretation bias. Afterwards, the same two coders coded all interviews. Gwen's Gamma ( $AC_2$ ) [310] was used as a measure of the quality of the Inter-Rater Agreement (IRA) as it takes into account the kappa-paradox, a problem where low kappas occur despite a high percentage of agreement [311]. For the results' interpretation, only codes with at least moderate agreement ( $IRA_{AC_2} > 0.74$ ) were respected.

To generate themes using inductive coding, the principal investigator [308] coder A (the author of this dissertation) 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 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 [308]. 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.

For the reporting of the results in this dissertation, we translated relevant statements of our participants' from German into English, applying a forward-backward translation procedure with native speakers.

Table 5.1: Participant demographics

ID	Age	Sex	Education	Profession	Employment (years)		Org. <sup>3</sup> Size	Ind <sup>4</sup>
					Total	Current		
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	Edu
P02	56-65	f	Academic degree	Administrative employee	26-30	0-5	L	Edu
P03	46-55	m	Academic degree	Team leader	16-20	6-10	L	Edu
P04	46-55	f	UEQ <sup>1</sup>	Administrative employee	26-30	6-10	L	Edu
P05	46-55	f	Sec. school & higher	Administrative employee	31-35	31-35	L	Edu
P06	56-65	f	Academic degree	Team leader accounting	26-30	0-5	L	Edu
P07	46-55	m	Academic degree	Project controller	20-25	6-10	L	Edu
P08	46-55	m	Academic degree	Purchasing employee	20-25	6-10	L	Edu
P09	26-35	f	Sec. school & higher	Clerk	16-20	16-20	L	Edu
IT & software developer (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
P11	36-45	m	UEQ <sup>1</sup>	IT Administrator	20-25	11-15	S	IT
P12	26-35	m	Apprenticeship	Application developer	6-10	0-5	S	IT
P13	18-25	m	Academic degree	Software developer	0-5	0-5	M	IT
P14	26-35	f	Academic degree	Software developer	11-15	11-15	M	IT
P15	26-35	m	Academic degree	Software engineer	6-10	6-10	M	IT
P16	36-45	f	Academic degree	Software developer	20-25	11-15	M	IT
P17	46-55	m	Academic degree	Mgmt. software dev.	16-20	0-5	M	IT
P18	36-45	m	Academic degree	Res. software dev.	11-15	6-10	L	Res
P19	18-25	m	Academic degree	Res. asst. software dev.	0-5	0-5	L	Res
P20	36-45	f	Academic degree	Res. asst. software dev.	20-25	11-15	L	Res
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
P22	46-55	f	Apprenticeship	Sales employee	31-35	11-15	S	IT
P23	46-55	f	Academic degree	Architect	20-25	6-10	S	Const
P24	18-25	f	UEQ <sup>1</sup>	Civil engineer	0-5	0-5	M	Const
P25	26-35	f	Apprenticeship	Media designer	11-15	6-10	M	Mktg
P26	26-35	f	Academic degree	Teamlead O&P media <sup>2</sup>	11-15	0-5	L	NPO
P27	26-35	m	Academic degree	Media consultant	6-10	0-5	L	Mktg

Note.

<sup>1</sup> UEQ: University entrance qualification

<sup>2</sup> O&P: Owned and paid media

<sup>3</sup> S: Micro (< 10 employees), M: Medium (< 250 employees), L: Large (≥ 250 employees)

<sup>4</sup> Edu: Education, IT: IT-service, Res: Research, Const: Construction, Mktg: Marketing, NPO: Non-profit



### 5.3 PERCEPTIONS OF CATEGORIES OF DATA

In this section, we present the results obtained in relation to **RQ1<sub>a</sub>** *“What are employees’ conceptualizations of different categories of data under common terminology found in practice?”* More specifically, we present the employee definitions for the data categories in Section 5.3.1, followed by the identified themes in Section 5.3.2 and a discussion of our findings in Section 5.3.3. 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.

#### 5.3.1 Employees’ definitions of categories of data

First, we present the definitions and examples we received from participants for the various terms.

##### ▷ **Data** (German: “Daten”)

We identified two distinct themes for the term “data”. The first theme provided by one third of the participants was that “data” can be treated as an **umbrella term**: *“Data is a very general term, [...] actually everything consists of data”* (P16). Furthermore, participants noted that “data” is a *“generic concept [that describes] all kinds of things”* (P04). While participants were not asked to identify a meaningful structure among the different data categories, they tended to arrange or **describe hierarchies**: *“I’m going to make it a little bit hierarchical, so first of all everything is ‘data’. ‘Data’ is at the top”* (P15). The second theme to be found deals with the close relation between “data” and “information”. Two nuances emerged in this context: (1) While participants tried to identify separate meanings at first, they often ended in merging their meanings at some point. (2) Other participants’ explanations emphasized on the generic property of data to express information: *“Data are different items out of all this information [...], the single items that you can divide these [other] categories into”* (P20). Only a few participants provided concrete examples, highlighting the term’s perceived abstractness. Except from master data, examples were rather concrete and include account statement, gender, and date of birth.

##### ▷ **Information** (German: “Informationen”)

Our participants agreed that their every working life is full of data and information. Hence, just like “data”, “information” was generally seen as an **umbrella term**. Yet, we found different associations. Participants with an IT background described information as being **data linked together**: *“So data is very raw and the information that is when you put the data together in context that you can then derive information from it”* (P14). Moreover, we found that IT and administrative professionals linked mere factual knowledge **without personal reference** to “information”, whereas other participants referred to data **with a clear personal reference** relevant to the job (e.g., customer data) when describing “information”.

##### ▷ **Personal data** (German: “Personenbezogene Daten”)

Overall, we found the greatest confirmation that personal data were perceived to **directly relate to and uniquely identify** an individual: *“[Personal data are] anything that only concerns me, that only I am, with which one could prove that this is my*

*identity*" (P22). The majority of our participants primarily assigned all types of master data (e.g., name) to this term. Examples mentioned by our participants included work-related data, such as skills, education, and religious affiliation, but also sexuality, and creditworthiness. IT-staff also linked biometrics and passwords to personal data. Software developers were also particularly aware that they generate personal data in the course of their normal work, e.g., when maintaining a code repository, using the company's chat, or when their actions are stored in log files. Furthermore, our participants were aware that personal data become available to a **wide range of internal and external recipients**. Very few participants expressed the need to protect personal data from employers.

▷ **Personal identifiable data** (German: "*Personenbeziehbare Daten*")

Half of our participants identified the **implicit personal reference** of personal identifiable data. But few participants were able to provide holistic explanations: "[Personal identifiable data] is information and data where it is not yet possible to find out exactly who they belong to, but by combining this information and data one could draw conclusions about certain persons" (P02). Moreover, all of our participants also identified a **close relationship** between "personal identifiable data" and "personal data", or argued that there is **no difference** at all. A third of participants expressed difficulties describing both these terms. While most explanations come to a similar conclusion, many of them seem to be based on **assumptions rather than knowledge**. Half of our participants stated that they did not know the meaning of the term and simply assumed that it was likely to refer to indirect personal information as compared to "personal data". Examples mentioned included master data (e.g., education, date of birth), but also fingerprints, passwords, and body size.

▷ **Personal aspects data** (German: "*Persönliche Daten*")

We encountered the **most non-uniform explanations** for this term. Half of our participants described personal aspects 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 aspects data were **absolutely confidential**. A third of participants claimed that "personal aspects data" was a synonym for "personal data". The collected statements took fundamentally **contradictory positions** on a continuum between the extremes of personal reference: One quarter reported that personal aspects 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 aspects data simply as "*information that is not personal at all*" and without reference to an individual, but "*which are subject to [their] personal access*." The responses of the remaining participants are distributed along this continuum of contradicting positions, providing more balanced explanations: "*Personal aspects data may have some sort of [...] personal reference, but do not necessarily have to*" (P15). Despite these differences, our participants agreed that personal aspects data somehow belong to a person and that access may be restricted: "*Personal aspects 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 aspects data **serve business purposes** and must be available to employers. Still, personal aspects data must only be **accessible by a small circle** of people or an individual. Few participants indicated that personal aspects data were worth protecting

and should stay confidential. In total, our participants provided 16 examples of personal aspects data, which mainly fall into the categories of master data (e.g., name) and special categories of personal data (e.g., diseases, blood type, dating activities).

▷ **Private data** (German: *“Private Daten”*)

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”* (Po2). 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”* (Po1) by and from employers. Examples given by our participants include all types of master data, but also diary entries, type of disability, illnesses, video recordings, pets, or the vacation spot.

### 5.3.2 Identified themes of categories of data

We identified recurring themes in the coding of our participants' explanations, which we arranged into four thematic groups. The results of the coding are shown in Figure 5.2 and are explained in more detail below.

The first group (G1) we identified describes a data category's *relation to a person*. Overall, for five of six terms, we found conflicting views on whether a term refers to data for which a personal reference exists, and how that data relate to a person. 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 (cf. Section 2.1), 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.

Based on accumulated answers, our coding suggests that participants distinguished between **three broader concepts**: (1) The first concept arises from “data” and “information”, and largely **lacks privacy related attributes**, contains no personal reference, but is of high relevance for daily work; (2) the second concept arises from “personal data” and “personal identifiable data”, and symbolizes data with **clear personal references** that either uniquely identifies a person or from which the identity of a person can be inferred; (3) the third concept is defined by “private data” and symbolizes **data with no**

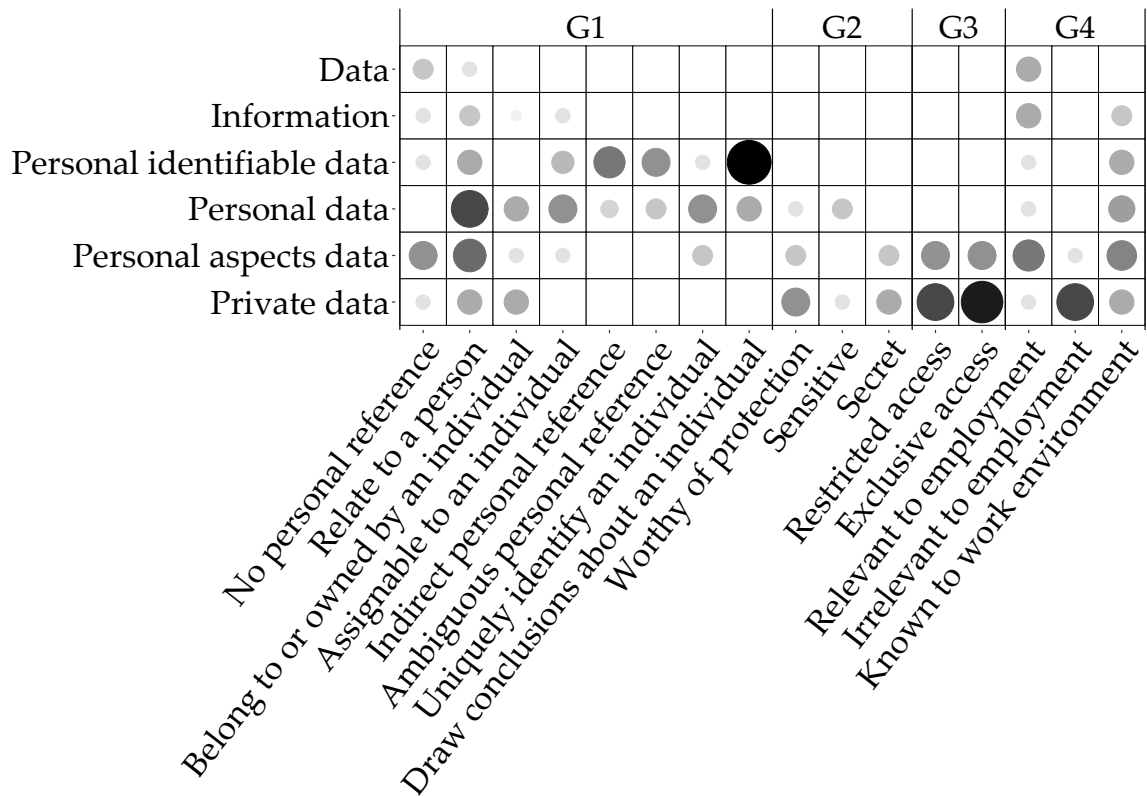


Figure 5.2: Identified coding themes of categories of data: (G1) Relation to a person; (G2) data sensitivity; (G3) access to data; (G4) relation to work. Circle size and saturation are proportional to the number of mentions.

**business relevance and strong access restrictions.** According to our coding, the term “personal aspects data” is in turn overloaded and cannot be assigned to any of these concepts.

### 5.3.3 Discussion

Our examination of employee perceptions of data and terminology reveals somewhat ambivalent results. On the one hand, the answers we received indicate that the terms under question evoke adequate associations in a broader sense. 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 [312].

Furthermore, we identified elements of CPM theory in our participants’ answers (cf. Section 2.1). 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 expecta-

tions 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, employees’ 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 become fuzzy [126]. Also, lack of familiarity with the terms’ legal meanings favors *boundary rule mistakes* because employees do not understand the associated privacy rules [126]. For example, data processing employees may access and process certain data without authorization, or the data subject employees may mistakenly assume that no processing is taking place.

#### 5.4 CONCEPTUALIZATIONS OF INFORMATIONAL SELF-DETERMINATION

To address **RQ1<sub>b</sub>**, “What are employees’ internalized conceptualizations of the right to informational self-determination in employment?”, we discussed various topics of self-determination and transparency over personal data with our participants and concluded with the question “what is informational self-determination in employment?”. 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, explaining that informational self-determination was 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.”

Based on our coding, we divided the aspects discussed by our participants into four thematic categories. We report on *objectives* of informational self-determination in Section 5.4.1, importance of *self-determination* in Section 5.4.2, value of *transparency* in Section 5.4.3, and practical *restrictions* and *issues* in Section 5.4.4. We then provide clusters of different mental models in Section 5.4.5 and discuss our findings in Section 5.4.6. 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. The codebook underlying this coding is shown in Figure 5.3.

##### 5.4.1 Objectives

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.

### 5.4.2 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**. Po6 explained it this way: *"[Inquiry 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 or to 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.

### 5.4.3 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).

### 5.4.4 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** [244]. Participants noted that the disclosure of personal data was indispensable, especially in service-oriented professions.



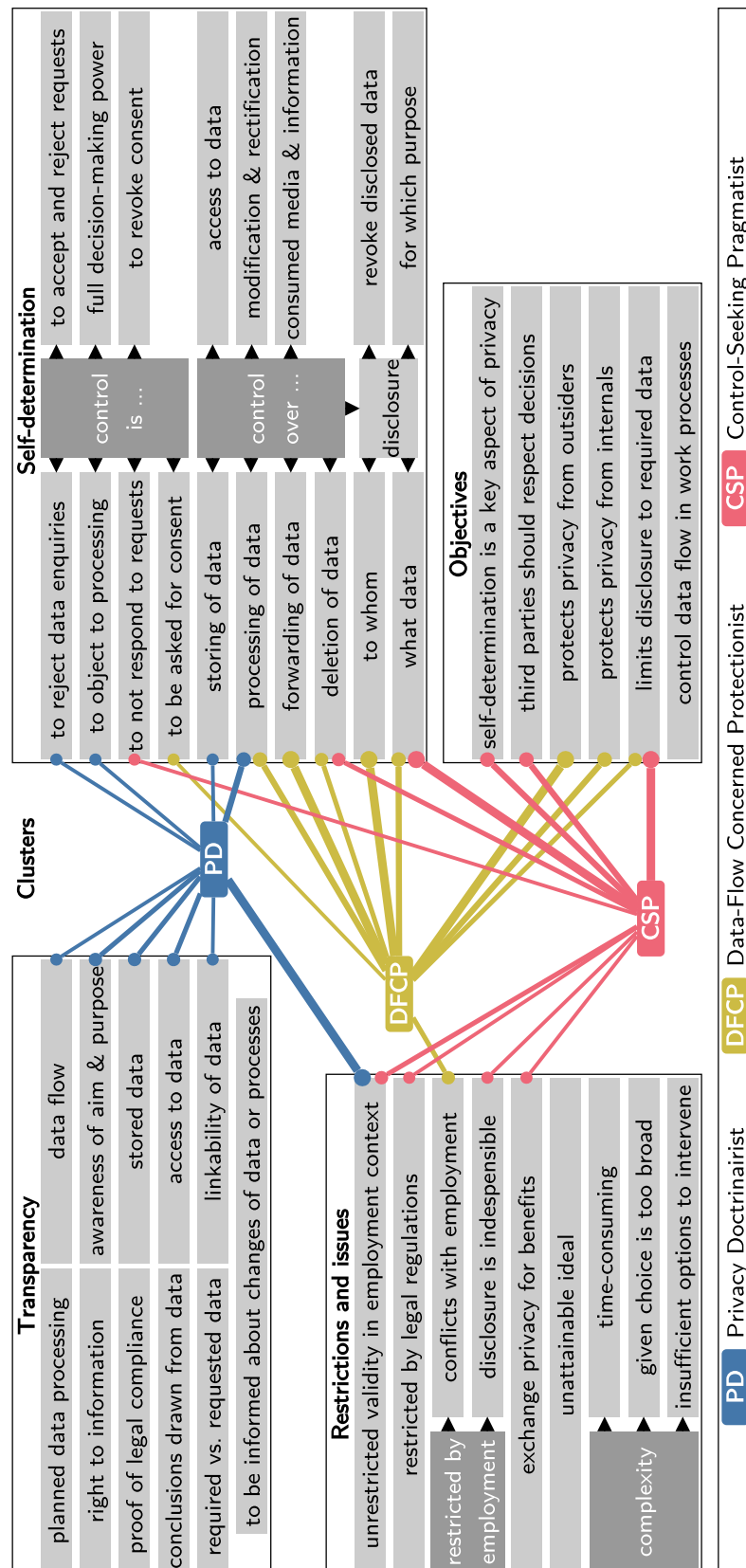


Figure 5.3: Identified themes of informational self-determination in employment arranged by code groups and hierarchies. For each identified cluster, the top ten codes are linked together. The line width symbolizes the code frequency in a cluster.



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."*

#### 5.4.5 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. We used multidimensional-scaling to build a case map, followed by hierarchical clustering (Unweighted Average Linkage). We compared the resulting feature vectors for two, three, and four 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. Figure 5.3). To better distinguish between the three clusters, we assigned them names that reflect the themes they encompass. In the following, we present and describe the different clusters identified.

##### ▷ Privacy Doctrinairist (PD)

We identified a group of eight employees (five IT, two others, one administrative) who put forward very strong claims for far-reaching transparency and ultimate control abilities over personal data. They emphasized the **universal validity of informational self-determination** in employment and did not accept any weakening of it. For them, transparency is tantamount to knowledge about *what* data are stored and *who* has access to data. These employees were the only ones in our sample who elaborated on the **importance of transparency** and discussed its complex dimensions. They were also looking for **assurances of data collection's legitimacy**. In addition, participants in this cluster also partially recognized the value of ex post control, demanding a right to **withdraw consent or to object** to data processing.

##### ▷ Control-Seeking Pragmatist (CSP)

We further identified a group of ten employees (five administrative, three others, two IT) for whom 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**. Therefore, they also claim for **far-reaching control** mechanism over their personal data, but **omit**

**transparency** completely. Instead, they look for “self-determination” as the key element of privacy. In particular, there are strong claims to control *which* of their personal data are disclosed or restrained. Strong emphasis was put on employers to respect decisions on avoidance of data disclosure. Also, these participants demanded abilities to delete and correct data. Nevertheless, employees **agreed upon several limitations and restrictions** to their privacy in employment. These include legal regulations that force them to disclose certain personal information and to be pragmatic about privacy. Showing traits of a privacy calculus [244], they accept such restrictions by weighing off the benefits of employment against perfect privacy. While they seek for control, they look for guidance and organizational support to protect their privacy in respect to legal and workplace boundaries.

▷ **Data-Flow Concerned Protectionist (DFCP)**

We identified a third group of nine employees (four IT, three administrative, two others) who have 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 the transmission** of data and to *whom* their personal data are disclosed to. 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**. Consequently, **DFCPs** expect to be asked for explicit consent most of the time before employers disclose their data to either internal or external recipients. They also share the **PD's** demand for extensive control over *what* happens to data in general, and claim that their privacy is severely restricted due to the employment context.

#### 5.4.6 Discussion

Our investigation of the right to informational self-determination reveals that privacy in employment 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 in employment [125], 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 in employment, 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 in employment, which is compensated for by considering the moment of disclosure as the most important control point for pri-

vacy 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 the right to privacy in employment.

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 [231, 235], 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 this regard, issues on the voluntariness when using consent in employment appear to be intensified by an overall negativity bias regarding privacy management.

Nevertheless, our findings show that privacy paternalism conflicts with the notion of self-determination, being deeply rooted in mental models. It is noteworthy that legislation generally enforces self-determination in non-employment 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 [213]. Since our sample includes employees 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 in employment 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 TETs (cf. Section 2.3.3), 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 in employment.

Moreover, by comparing the descriptive characteristics of the three clusters of mental models we identified with the descriptive characteristics of personas known from online privacy research, we identified minor similarities with Morton's *information controller* and *organizational assurance seeker* [313], and with Schomaker's and Westin's *privacy pragmatist* [283, 287]. Different, though, our clusters emphasize the various interpretations of the right to privacy in employment instead of online privacy concerns. In line with the criticism of online privacy personas not serving well in other than the original context [314], we expect our clusters to highlight privacy perceptions that are particular to the employment context. Unlike online privacy personas, our results do not indicate unconcerned employees either, which questions the applicability of approaches such as

Westin's unconcerned persona to the employment context. We consider this a consequence of the overall high value of the topic of data protection in Germany.

## 5.5 PERCEPTIONS AND AWARENESS OF PERSONAL DATA PROCESSING

To complement the exploration of employees' conceptualization of the right to informational self-determination above, we now address employees' perceptions and awareness of everyday data processing. In line with our research questions **RQ1<sub>c-g</sub>**, we first present perceptions of self-disclosure in Section 5.5.1, followed by perceptions of data flow in Section 5.5.2. We then explore our participants' beliefs about privacy safeguards in Section 5.5.3 and threats in Section 5.5.4, and discuss aspects of potential privacy intrusions by employers in Section 5.5.5. We then discuss our findings in Section 5.5.6. 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.

### 5.5.1 Self-disclosure

Aiming to understand employees' perceptions of self-disclosure under **RQ1<sub>c</sub>** "*How do employees perceive the process of self-disclosure?*", we asked our participants how their employers obtain personal data from them, and how they agree to the processing.

The vast majority of our participants responded that they **actively disclose** their personal data to their employers "*systematically within the scope of data entry forms.*" Participants were particularly conscious about the data they provided during the recruitment process. In this regard, one participant pointed out that it is generally difficult to know who has access to documents (e.g., resumes) and who is in possession of which kind of information. Moreover, P15 considered himself to be a kind of data provider who has control over what data are shared: "*[I don't think that my employer] actively obtains data from me, instead I rather believe that I provide data.*"

When we asked our participants how they agreed to the processing of their personal data by their employer, participant P22 responded: "*Not at all. Or simply by providing them - it was tacit consent.*" The majority of respondents gave similar explanations and characterized their consent therefore as **implicit**. P13 further explained that the consent "*is not stated in my employment contract, [instead] this is done here on a basis of trust.*" Participants emphasized that **implicit consent is not necessarily a loss of control**. Instead, active data disclosure was seen as a form of "*indirect approval*" because one is "*still conscious of [disclosing] data.*" However, there were also participants who admitted not to "*remember if there was a consent form back then*" (Po4). In such cases, employees stated that they really do not mind their data being processed anyway.

Half of the participants declared that they **explicitly consent** and claimed to have actually signed a corresponding data protection statement at the beginning of their employment, which is ultimately valid. Moreover, implicit and explicit consent are by no means dichotomous, but the type of consent "*depends on the type of data, [...] for many [data] there do exist privacy declarations stating that the data can be used*" (Po7) and that one usually signs at the beginning of an employment. Consent for subsequent data disclosures, however, occurs implicitly: "*But then there is also a lot of data, which is naturally produced as you work. Which means, of course, that there is no need for separate approval.*"

### 5.5.2 Personal data flow

We now turn to employees' perceptions of personal data processing, related to **RQ1d** *"What are employees' awareness of data processing with respect to data storage and data flow?"* The results are based on the drawing exercise, in which our participants explained how and where different data are stored, and outlined the path of the data flow.

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"* (Po7) 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 internet service provider 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).

### 5.5.3 Privacy safeguards

To examine **RQ1e** “What are employees’ conceptualizations of implemented safeguards to protect privacy in employment?”, we extracted the safeguards described by our participants in the drawing exercise to protect their personal data. In total, we identified three different themes for safeguards that our participants referred to in their explanations: (1) The *organizational* theme, (2) the *technical* theme, and (3) the *physical* theme. A summary of the different safeguards is provided in Figure 5.4.

Irrespective of the professional background, nine participants explicitly stated that they were **completely unaware** of the extent to which safeguards existed for protecting their personal data. They 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). Still, the vast majority of participants (N=19) identified a **functioning authorization concept** in the form of Role-Based Access Control (**RBAC**) within their organization as the most important safeguard. Technical lay participants 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” (Po6). Yet, they also believed that IT administrators could still access data anytime, anywhere. IT experts, in turn, assumed that **RBAC** was applied at the

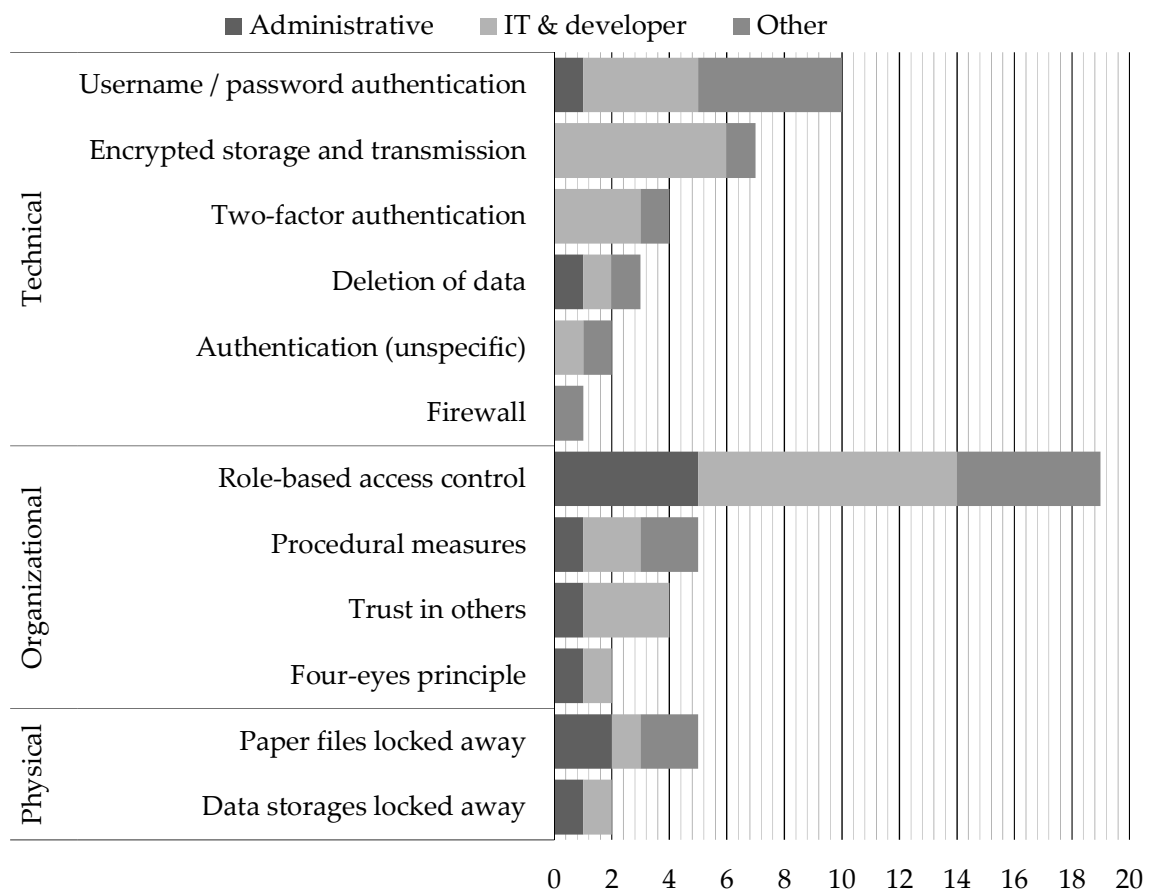


Figure 5.4: Conceptualizations of identified safeguards for employee privacy, sorted by theme and number of participants.



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**.

#### 5.5.4 Privacy threats

Next, we present our findings related to **RQ1f** *“What are employees’ conceptualizations of threat models to privacy in employment?”* In general, our participants differentiated between different attack vectors and adversaries in their explanations. A summary of the different threats identified is provided in Figure 5.5.

First, 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 (five 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.



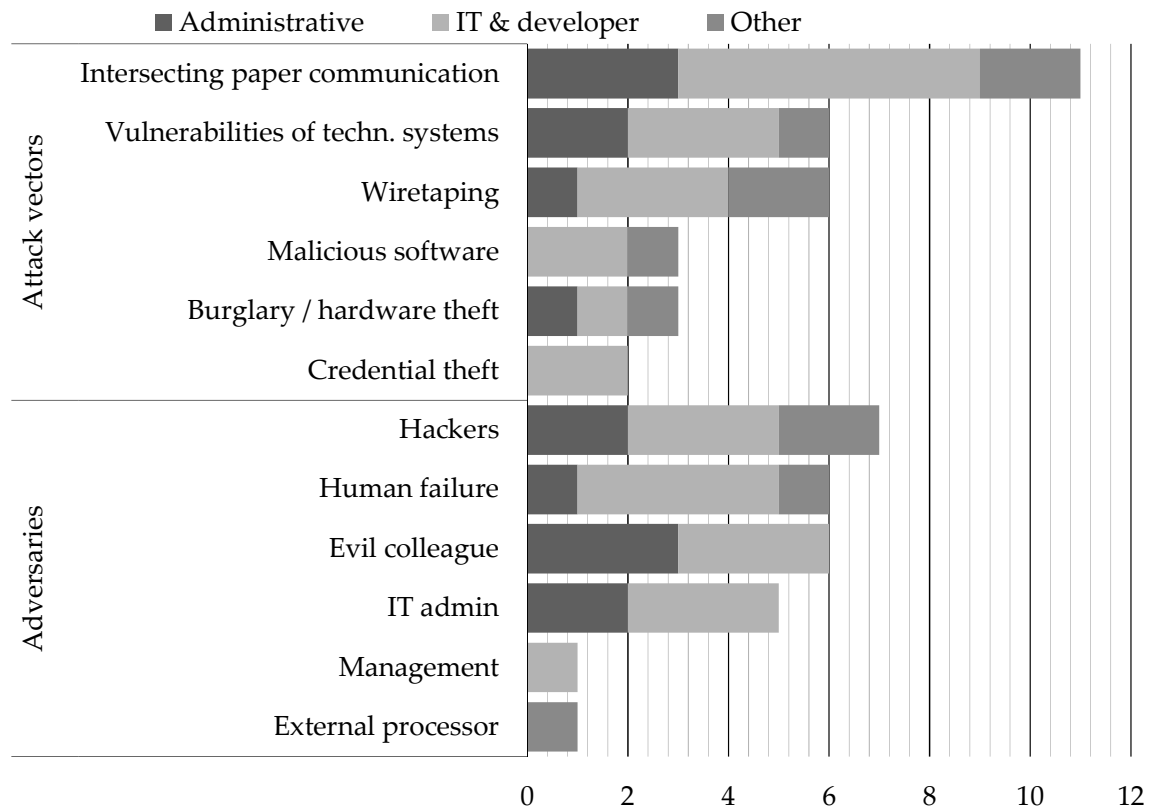


Figure 5.5: Conceptualizations of identified threat models for employee privacy, sorted by theme and number of participants.

#### 5.5.5 Invasion of privacy

To investigate **RQ1<sub>g</sub>** “What potential invasions of privacy by employers are employees aware of?”, we asked participants to discuss aspects and situations that would violate their privacy in employment. We specifically asked participants about their thoughts and judgment on their data being processed without their knowledge, and also asked for practical examples of data misuse.

Overall, our participants reported to be **generally unconcerned** when disclosing personal information, justifying their attitudes with strong trust beliefs. Po4 expressed that “in the course of digitization and Facebook and no idea what else there is [...] I can already imagine that more can happen with the data [...] But I would say that my employer doesn’t do that.” In line with this view, various participants justified their lack of concern by referring to the law, claiming that their employer “will of course adhere to the applicable data protection regulations” as “this is top priority” to the organization and its employees. A manager emphasized the appropriateness of the types of data collected: “Employers do not record eye color, nose length or shoe size, but record the data necessary for the contractual relationship and payroll accounting” (P17), concluding that there is no reason to be concerned or worried about. Few participants feared the **loss of control** and **uncertainty** going along with the disclosure of **sensible personal data** to employers: “In the worst case, it could even be used against me at some point.” (P15)

Regarding the unwitting processing of personal data by employers, the vast majority of participants expressed **no concern**, arguing that the data were not sensitive or that the

purpose was probably legitimate. Likewise, P16 also questioned the need to be informed about data forwarding because *“otherwise [the employer] would have done it.”* In contrast, few participants considered the **linkage** of working times and ticket systems or the interpretation of financial and health data as potential invasions of privacy. For example, P15 expressed concern about handling sick notes that must be sent to the employer but may contain hidden references to illness: *“Then it goes on to the headquarters, and then you just don’t know what conclusions they draw from it.”* Overall, the misuse of data, according to our participants beliefs, had to be generally related to some form of **commercial interests of the employer** (i.e., selling employee data). One participant further speculated that employers could be *“passing on data to advertising agencies in order to place targeted advertisements to enforce certain behavior at work the employer benefits from.”*

#### 5.5.6 Discussion

Our investigation of employees’ perceptions and awareness of personal data processing yields a wide range of insights. First, looking at our participants’ perceptions of self-disclosure, we found that they generally perceived themselves as a data source who can consciously decide whether or not to release personal data to the employer. In this sense, the conscious release of personal data was perceived as tacit consent to their processing. This kind of consent was apparently also considered sufficient for disclosure in day-to-day business. In contrast, explicit consent was considered a one-time issue at the time of recruitment. However, even though our participants perceived self-disclosure and the basis for processing as a result of a conscious act, they were unaware of what personal data were actually available to their employers or third parties, even though they themselves claimed to have actively provided the data. Indeed, our results suggest that awareness is characterized only by superficial knowledge. For instance, we asked our participants at the beginning of the interview for what purposes their employers process their personal data, whereupon the vast majority mentioned payroll. But when we confronted them with follow-up questions, we often found little to moderate factual knowledge. In fact, our participants were also often surprised at the extent of their own ignorance. Accordingly, it is probably fair to conclude that our sample’s overall awareness of personal data processing was rather low.

Furthermore, our participants’ mental models appear to be biased by their job-specific experiences in their respective work environments. 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 regard 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.

However, we further found that advanced technical knowledge is not necessarily beneficial. 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 simply run the risk of overestimating the safeguards implemented. 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. Non-IT 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. Such strong trust beliefs may be explained by the fact that, unlike in the U.S., there were no reports on leaked payroll data in the German media at the time of the interviews. 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.

Regarding the misuse of personal data by employers, our results show that this topic exceeds the boundaries of our participants' mental models. This was expressed in particular by drawing analogies from other contexts, especially the online context. For example, the majority of our participants stated that employers could misuse employees' personal data primarily by selling them to third parties. This finding supports our participants' statements that they trust their employer to handle and protect their personal data properly. In contrast, internal attackers, such as colleagues, were considered a major threat to privacy, reflecting the desire to control personal data flow inside the organization (cf. Section 5.4).

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 [315]. For example, research attributes actions under uncertainty a significant contribution to the privacy paradox [262]. Our results show that ignorance poses a serious risk to fall into a (dis)illusion about personal data processing in employment relationships. Furthermore, we found that some participants expressed concern about being uncertain, since there was a lack of transparency about which data were available to employers. In particular, permanent data storage was perceived as a potential privacy invasion because the employers might use the data against employees in the future. Similar to previous findings [118, 127], these participants perceived unwitting processing of personal data as a violation, since they feared negative consequences.

## 5.6 IMPLICATIONS

The Legally mandated privacy controls and data subject rights that employers must implement and guarantee can only protect privacy in employment to the extent that they are consistent with employees' conceptualizations with the right to informational self-determination. In this context, our examination of 27 employees' mental models under **RQ1** "*What are employees' internalized conceptualizations of the privacy framework under the right to informational self-determination in employment?*" reveals a variety of issues with employees' perceptions, concepts, and awareness of this right and associated concepts. The most obvious boundaries are the one-dimensional views of privacy as mere ex

ante control, and the lack of awareness of personal data processing. The latter appears reasonable with regard to the ignorance of transparency. The identified gap between the mental models of informational self-determination and the fundamental objectives of this right (cf. Section 2.2) has several implications for the design and implementation of effective privacy controls, and for future work. In the following, the results are discussed in terms of both their theoretical and practical implications.

#### 5.6.1 *Notice and transparency*

We found overall awareness among our participants that many different personal data, including less conspicuous data (e.g., usage data), are collected and processed in the employment context. However, employees seem to struggle to identify the presence of such data in their work environments. We further found that no processing is expected for personal data with no assumed business relevance. Employees may draw incorrect conclusions, however, because they appear to have no or limited knowledge of which purposes exist in the first place. Awareness of data processing also seems to be more likely when employees actively disclose personal data. Consequently, 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 could not provide clear and consistent definitions of common terms. Prior work showed that employees create “*implicit rules [...] by implied meanings and understandings*” for ownership and control [127]. Our results demonstrate this strategy’s susceptibility to error. The use of common terms is likely to leave employees in an uninformed state, since they are unaware of the rights and obligations that actually apply to “private data”, for example. The identified conflicting interpretations in this study 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. 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. 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. Mitigation efforts should also aim to counteract any inconsistent use of the terms in software, in privacy statements, or by employees and employers.

Moreover, the mental models identified in this study are also generally characterized by inexperience with any form of privacy-by-policy in the employment context; even basic properties of notice did not seem to be part of our participants’ practical experience. This finding is complementary to other work that examined what information about personal data processing employees would like to receive [96]. Mental models following the idea that employers would probably notify their employees if they had to, highlights the need to support employees in internalizing transparency not as a nice gesture from the employer, but as a fundamental right they own.

### 5.6.2 *Control and intervention abilities*

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 employment context allow. Only the cluster of PDs is likely to associate a small increase in informational self-determination if the design of privacy controls strictly complies with the law. 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 employees 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. Looking at these results from a usability perspective, it appears that privacy-by-architecture approaches may be a relief to employees compared to privacy-by-policy [15] (cf. Section 2.3.3).

To further 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. Our results further indicate that “one-size-fits-all” solutions should be discouraged in this regard. For example, the demand for excessive involvement in every disclosure process by CSPs may be perceived as annoying to other employees. Contrary, ex post privacy controls do not align with the self-determination demands of DFCEPs. To further address usability aspects, new forms of data inquiry incorporating the notion of implicit consent and denial of data processing should be considered, since our participants perceived such implicit controls useful in managing self-disclosure. Nevertheless, 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 possibly even perceive it to be less burdensome in comparison to ex ante control.

### 5.6.3 *Awareness*

As far as the protection of personal data is concerned, our investigation suggests that employers appear to enjoy the trust of their employees. In fact, the mental models retrieved are characterized by trust and unawareness to such an extent that our question of potential misuse scenarios of personal data by employers exceeded their limits. We therefore assume that our participants have never encountered personal data misuse by employers before. Accordingly, employers have a great responsibility to do justice to this leap of faith. In the event of a privacy breach, this trust relationship runs the risk of being severely disrupted.

Moreover, it should be in employers' best interest to enhance their employees' mental models of personal data processing to prevent disillusionment, counteract uncer-

tainty, and further strengthen the trust culture. The current state of unawareness and the tendency to overestimate safeguards hinders employees from drawing reasoned conclusions about risks to their privacy. Our results indicate that reducing uncertainty may also lower privacy concerns, because employers' future actions become more predictable to employees. 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.

#### 5.6.4 *Implications for research*

Previous studies on privacy in employment often consider the employers and cyber criminals to be the only intruders that impact employees' privacy perceptions [3, 35]. 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 employees' privacy perceptions.

### 5.7 STUDY LIMITATIONS

Although the study design intends to capture general mental models of informational self-determination in employment, 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 [247], 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 [247]. Findings may vary for employees from other organizations, because privacy perceptions correlate to the organization type [316]. 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 [112, 247]. 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 [232]. However, our participants may in fact had relatively advanced



mental models of informational self-determination; indeed, 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.

## 5.8 SUMMARY

In this chapter, we have presented the results of a semi-structured interview study with 27 employees in Germany, in which we elicited employees' mental models of the right to informational self-determination to examine **RQ1** *"What are employees' internalized conceptualizations of the privacy framework under the right to informational self-determination in employment?"* According to our literature review in Chapter 3, our results provide the first insight into employees' privacy conceptualizations that are Eurocentric and non-Anglo-American. To this end, we provide fundamental knowledge on: (1) Employees' conceptualizations of different categories of data and common terminology; (2) employees' conceptualizations of the right to informational self-determination, dividing into different objectives, demands for self-determination and transparency, and issues; and (3) employees' awareness of personal data processing, data flow, safeguards, threat models, and misuse scenarios. Our results illustrate the ambiguity and obscurity of common terminology to describe (personal) data, even for data processing employees and managers. Meanwhile, our findings provide guidance on the use of terminology and indicate factors that should be considered to fulfill the legal requirements for clear and plain language in the employment context. We also identified three types of mental models that differ in their expectations of privacy controls. These may serve to understand employees' specific privacy needs and capabilities, and provide guidance on which biases to consider when designing or implementing privacy controls. Furthermore, we found ignorance among participants about actual personal data flow, processing, and safeguard implementation in employment. Instead, our participants' mindsets were shaped by their faith in the employer and TOMs to protect privacy.

The results of this study lay the foundation for a knowledge repository that provides stakeholders involved in privacy engineering, such as employers, researchers, designers, and software engineers, with fundamental knowledge for follow-up systems engineering processes to, e.g., assess risks, elicit requirements, or make architectural decisions (cf. Section 2.3 & Section 2.4). In particular, this study contributes to knowledge about the types of privacy controls desired by employees and the challenges to be considered in designing and creating usable control and transparency mechanisms in the employment context. As such, findings on data processing employees influenced our own UCD study presented in Chapter 7. For researchers, new aspects emerged for future studies, some of which influenced our quantitative study, which we present in the upcoming Chapter 6.



## STUDY II — DETERMINANTS AND DIFFERENCES OF EMPLOYEES' PERCEPTIONS OF PERSONAL DATA

---

*What can be asserted without evidence  
can be dismissed without evidence.*

— Christopher Hitchens

In this chapter, we complement our findings presented in Chapter 5 on the conceptualization of the right to privacy by investigating employees' perceptions of personal data, focusing on the research questions **RQ2** - **RQ4** derived in Section 4.1. Based on [102], we present the results of a cross-sectional survey study with 553 employees from Germany. The survey provides multiple insights into the relationships between employees' perceived data sensitivity and their willingness to disclose personal data in the employment context. The study contributes to the general body of knowledge in privacy research by providing new insights into privacy in employment. It further highlights differences between contexts and makes an important contribution to balancing the existing one-sided focus of research on both private contexts and U.S.-centric views.

The remainder of this chapter is structured as follows: We introduce our research model and hypotheses in Section 6.1. This is followed by details on the procedure and methods for designing and conducting our study, along with details on ethical concerns and data analysis in Section 6.2. Next, we present details on employees' perceived data sensitivity and willingness to disclose in Section 6.3, followed by an examination of employees' perceptions of different groups of personal in Section 6.4. We then present the results of an in-depth analysis of determinants of *perceived data sensitivity* and *willingness to disclose* in Section 6.5, and reveal different clusters of employees in Section 6.6. Afterwards, we discuss our results' implications in Section 6.7, and discuss limitations of our study in Section 6.8. We finally conclude this chapter, summarizing our findings in Section 6.9.

### 6.1 BACKGROUND AND RESEARCH MODEL

In this section, we elaborate on our research questions by deriving specific sub research questions and hypotheses guiding our research. Specifically, Section 6.1.1 addresses **RQ2**, Section 6.1.2 addresses **RQ3**, and Section 6.1.3 addresses **RQ4**. A summary of our research objectives mapped to the different research questions is shown in Figure 6.1.

#### 6.1.1 Differences in the perception of personal data

In the following, we set out our research model to address our research question **RQ2** “How do personal data differ in terms of their perceived sensitivity and willingness to disclose by employees?” and to divide its scope into smaller, yet more concise, sub-research questions.

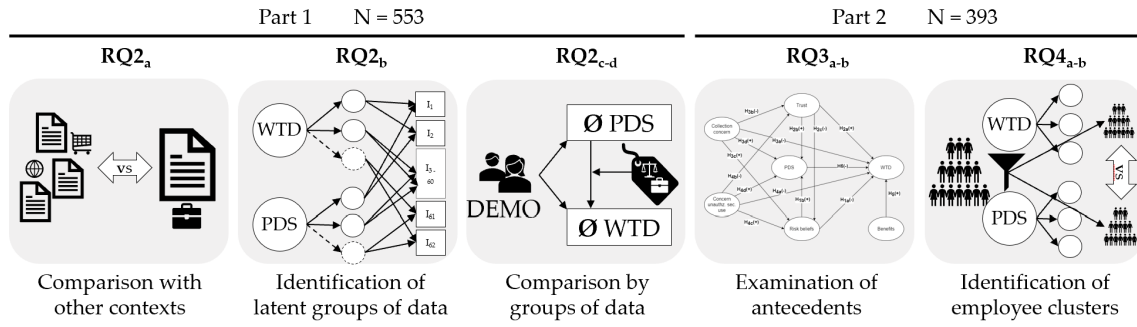


Figure 6.1: Summary research objectives and research questions in Study II.

**CONTEXTUAL DIFFERENCES** As explained in Section 2.4.4, people's perceptions of (personal) data sensitivity are generally considered to be highly context-dependent [113, 247, 248]. However, recent studies in the marketing and online context show that perceived data sensitivity seems unaffected by slight context changes. In more detail, different studies have been conducted with samples from the USA and Brazil [274], from Germany [271], and from Saudi Arabia [273]. All found that the ranking of various personal data by perceived sensitivity was largely unaffected by differences in culture and context. This raises the question whether a global consensus for a ranking of personal data by perceived sensitivity can be reached [271, 274]. We take up this proposition and examine whether perceived data sensitivity differs significantly between the employment context and the online and marketing contexts examined in [271, 273, 274]. This leads to the formulation of our first sub-research question:

**RQ2<sub>a</sub>** "Does the employment context alter the ranking of personal data by *perceived data sensitivity* compared to other contexts?"

**GROUPS OF PERSONAL DATA** Legislation and international standards distinguish between different groups of personal data based on their sensitivity properties. A common, yet simple distinction is that between "personal data" and "sensitive personal data". Based on the comprehensive list of different definitions provided in Section 2.2.3, we aim to provide updated insights into employees' perceptions of groups of personal data by examining whether employees' perceived data sensitivity matches legal distinctions. To further assist in the employee-centric design of privacy controls and privacy-friendly systems, we are investigating whether we can identify context-specific groups of personal data that emerge directly from the perceptions of employees' perceived data sensitivity and willingness to disclose in employment. Such "latent" groups of personal data would be characterized by the fact that, in contrast to previous work, they allow holistic inferences and do not merely represent evaluations of individual types of data. By comparing these groups of personal data to other groups based on legal definitions, we are the first to examine and compare the magnitude of the (expected) negative correlation between *perceived data sensitivity* and *willingness to disclose* for different groups of data. As such, we derive the following sub-research questions:

**RQ2<sub>b</sub>** "Can latent groups of personal data be identified in the employment context based on employees' *willingness to disclose* and *perceived data sensitivity*?"

**RQ2<sub>c</sub>** “Do the *perceived data sensitivity* and *willingness to disclose* differ between groups of personal data?”

**RQ2<sub>d</sub>** “Is the magnitude between *perceived data sensitivity* and *willingness to disclose* affected by the group of personal data?”

### 6.1.2 Antecedents and causal model

Our research question **RQ3** “Which antecedents influence employees’ perception of personal data?” tackles the current lack of studies focused on investigating the determinants of *perceived data sensitivity* and *willingness to disclose* personal data in the employment context [25]. We therefore review the applicability of antecedents used in other contexts [113, 247, 262] to the employment context, using the APCO model (cf. Section 2.4.4). Moreover, our mental model study in Chapter 5 strongly suggests that employees’ personal disposition toward a right to privacy influences their privacy perceptions. We therefore derive the following two sub-research questions:

**RQ3<sub>a</sub>** “How do common antecedents affect employees’ *perceived data sensitivity* and *willingness to disclose* data in employment?”

**RQ3<sub>b</sub>** “Are common antecedents affected by employees’ personal disposition toward a right to privacy?”

For the studying of **RQ3<sub>a</sub>**, we lay out our causal model below by describing the various antecedents examined in this study. To this end, we derive and formulate our hypotheses **H1** – **H6**. The causal model is depicted in Figure 6.2.

**RISK BELIEFS AND TRUST** *Risk beliefs* refer to the uncertainty that the disclosure of personal information could lead to some kind of material or non-material loss [244, 247]. Thus, *risk beliefs* negatively influence *willingness to disclose* personal data [244, 255]. Since employees were found to withhold personal information when they fear adverse consequences [118, 127], we hypothesize the following:

**H1<sub>a</sub>**: Employees’ *risk beliefs* are negatively associated with their *willingness to disclose* personal data.

**H1<sub>a</sub>**: Employees’ *risk beliefs* are positively associated with their *perceived data sensitivity*.

*Trust* has an opposite effect to *risk beliefs* [73] and refers to the degree to which employees believe their employer is dependable in protecting employee personal data [255]. The results of Study I in Chapter 5 indicate that employees in Germany appear to trust their employers to process their personal data in a fair and data protection compliant manner. We thus hypothesize the following:

**H2<sub>a</sub>**: Employees’ level of *trust* in employers is positively associated with their *willingness to disclose* personal data.

**H2<sub>b</sub>**: Employees’ level of *trust* in employers is negatively associated with their *perceived data sensitivity*.

**H2<sub>c</sub>**: Employees’ level of *trust* in employers is negatively associated with their *risk beliefs*.

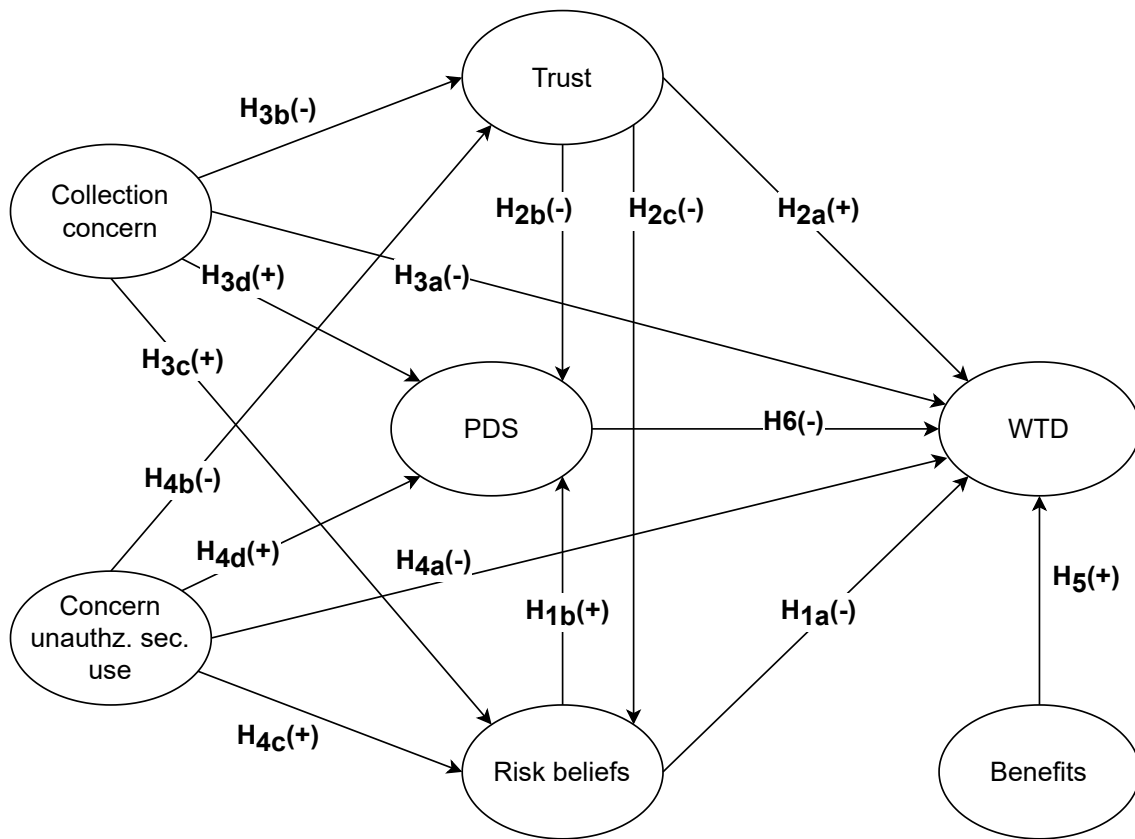


Figure 6.2: Anticipated causal model of antecedents for Perceived Data Sensitivity (PDS) and Willingness to Disclose (WTD) in the employment context. For each hypothesis (H1 - H6), we indicate the expected direction of effect (positive (+) or negative (-)).

**PRIVACY CONCERNS** *Privacy concerns* cover a wide range of beliefs (cf. Section 2.4.4) and have indirect effects on people's privacy behavior by substantially influencing their *willingness to disclose* [112, 250, 262]. Previous work anticipates that this relationship also applies to the employment context [73]. Given that employees are required to disclose large amounts of potentially sensitive personal information to their employers, we hypothesize that this translates into a particular level of concern by employees that employers are collecting too much data about them over time. Based on this notion, we formulate the following hypotheses related to employees' *collection concern*:

**H3<sub>a</sub>**: Employees' concern about the extensive *collection* of personal data by employers is negatively associated with their *willingness to disclose*.

**H3<sub>b</sub>**: Employees' concern about the extensive *collection* of personal data by employers is negatively associated with their overall level of *trust* in employers.

**H3<sub>c</sub>**: Employees' concern about the extensive *collection* of personal data by employers is positively associated with their *risk beliefs*.

**H3<sub>d</sub>**: Employees' concern about the extensive *collection* of personal data by employers is positively associated with their *perceived data sensitivity*.

Moreover, because in our mental model study we found that employees expressed concerns that some of their personal data could have negative consequences if used for

purposes other than those intended (cf. Chapter 5), we expect similar effects for employee concerns about employers' *unauthorized secondary use* of personal data. In this regard, we formulate the following hypotheses:

**H4a:** Employees' concern about the *unauthorized secondary use* of personal data by employers is negatively associated with their *willingness to disclose*.

**H4b:** Employees' concern about the *unauthorized secondary use* of personal data by employers is negatively associated with their overall level of *trust* in employers.

**H4c:** Employees' concern about the *unauthorized secondary use* of personal data by employers is positively associated with their *risk beliefs*.

**H4d:** Employees' concern about the *unauthorized secondary use* of personal data by employers is positively associated with their *perceived data sensitivity*.

**BENEFITS AND PERCEIVED DATA SENSITIVITY** Previous studies suggest that employees assess the relevance and suitability of personal data when requested to disclose in the employment context [66, 80]. In addition, our results of Study I in Chapter 5 suggest that some employees' conceptualizations of the right to privacy take *benefits* as a tradeoff for the restriction of self-determination. Consequently, employees' willingness to disclose personal data may increase if they believe to receive adequate gratification (i.e., *benefits*) in return [3]. Moreover, while several studies have examined *perceived data sensitivity* outside the employment context, it has rarely been examined as a predictor of *willingness to disclose*. We therefore derive the following hypotheses:

**H5:** Employees' perceived *benefits* of self-disclosure to employers are positively associated with their *willingness to disclose*.

**H6:** Employees' *perceived data sensitivity* is negatively associated with their *willingness to disclose*.

**EMPLOYEES' DISPOSITIONS TO A RIGHT TO PRIVACY** For the studying of **RQ3b**, we derive and formulate our hypotheses **H7 – H10**. Given that the research question is exploratory in nature, drawing directly from Study I in Chapter 5, a causal modeling is deemed infeasible for its studying. Instead, we are interested in finding out whether and which dispositions of employees for privacy have an effect.

The first disposition studied is employees' perception of having a right to privacy. *Privacy as a right* has hardly been studied before, yet, people tend to perceive the right to privacy differently, which has also an effect on their privacy beliefs [113, 288]. Our findings in the mental model study in Chapter 5 revealed that employees' beliefs about having a right to informational self-determination influence their attitudes toward how data should be used or how much data should be disclosed. As a result, we examine its impact on other antecedents surveyed in this study.

Furthermore, the mental model study also revealed that employees tend to perceive the managing of privacy as complex and challenging. We therefore investigate whether the perceived *complexity of privacy protection* has an effect on common antecedents. Similarly, our mental model study indicates that employees have only artificial knowledge of privacy law, if any, but at the same time trust that the legal framework will guide employers to protect their data. We therefore also include *knowledge about privacy law* and employees' *satisfaction with privacy law* in our examination of potential effects on antecedents. As a result, we derive the following hypotheses:

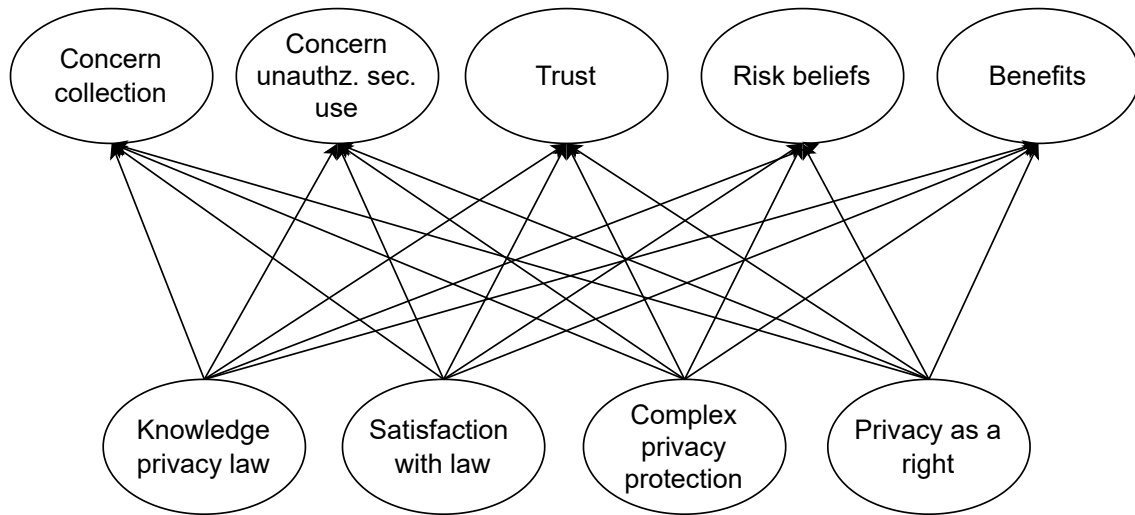


Figure 6.3: Model for examining effects of employees' dispositions to a right to privacy on privacy antecedents.

**H7:** Employees' level of perceiving *privacy as a right* has significant effects on other antecedents of personal data disclosure.

**H8:** Employees' level of perceiving the *complexity of privacy protection* has significant effects on other antecedents of personal data disclosure.

**H9:** Employees' level of *knowledge about privacy law* has significant effects on other antecedents of personal data disclosure.

**H10:** Employees' level of *satisfaction with privacy law* has significant effects on other antecedents of personal data disclosure.

### 6.1.3 Employee groups and clusters

To address our research question **RQ4** "Can employees be categorized based on different perceptions of personal data?", and thus consider the element of uniqueness of individuals' privacy perceptions, we examine differences among employees based on *willingness to disclose* and *perceived data sensitivity*. We choose these attributes, because we believe they are the most relevant for employers when attempting to process truthful data. As a result, we derive the following sub-research questions:

**RQ4a** "Can employees be classified into groups according to *willingness to disclose* and *perceived data sensitivity*?"

**RQ4b** "Do these groups differ in terms of demographic factors or privacy attitudes?"

## 6.2 METHODOLOGY

To examine our research questions and hypotheses, we conducted a cross-sectional online survey with 553 employees in Germany between July 2020 and March 2021. The data were analyzed quantitatively using appropriate statistical methods. In what follows, we



first discuss how we addressed ethical concerns in Section 6.2.1, followed by details on the measurement instrument used in Section 6.2.2, the survey's procedure in Section 6.2.3, the participants' recruitment in Section 6.2.4, our participants' demographics in Section 6.2.5, and the data analysis in Section 6.2.6.

### 6.2.1 *Ethical considerations of the study*

We ensured to minimize potential harms from our study by adhering to the Code of Ethics of the German Sociological Association and the Standards of Good Scientific Practice of the German Research Foundation. Our study design was also independently approved by two DPOs at our institutions. Employees participating in our study were informed about the data collected at the beginning of the survey. After consenting to participate, they could leave the survey at any time and delete their responses. In addition, we collected data anonymously whenever possible. If this was not possible, the data were stored separately from the response data and deleted after the survey was completed. All data were stored on encrypted hard drives.

Participants recruited through online panels were paid according to minimum wage in Germany (€9.60/h) adjusted to the median completion time. Participants recruited via other channels were not paid, but invited to participate in a raffle of shopping vouchers. We pointed out the conditions of participation at the beginning of the study. When we contacted organizations to recruit their employees, we provided extensive information about the study and surveys for review. We assured participating organizations that they could not be identified. One organization required approval through employee representation. We assured representatives and employees that we would not share information about participation with their respective employers. Last but not least, we explicitly referred to voluntary participation in our invitation emails and, after consultation with the organizations, explained whether the study may be completed during or outside working hours.

### 6.2.2 *Measurement instrument*

Where available, we used validated measurement items from the literature to design our survey and adapted them as needed. For privacy antecedents, we used items from [255, 256] to elicit *trust*, *risk beliefs*, *collection concern*, and *unauthorized secondary use*. Because no matching items for *benefits* were found, we created them ourselves. To elicit employees' dispositions to privacy, we used items from [288] to elicit *privacy as a right*, and statements from [287] to elicit *complexity of privacy* as well as *satisfaction with privacy law*. All constructs were measured with three to four items using a six-point scale. An exception is *satisfaction with privacy law*, which was a single item measured on a six-point scale. To elicit *knowledge about privacy law*, we used five multiple choice questions. To design the questions, we either adapted questions from the "Online Privacy Literacy Scale" [317], or we created new questions and items targeting the employment context. Furthermore, to measure *perceived data sensitivity* and *willingness to disclose*, we used a set of 62 items representing various personal data. Participants rated *perceived data sensitivity* on a six-point scale and *willingness to disclose* on a four-point scale, respectively. The set of 62 personal data items is composed of the results of a series of workshops conducted in 2019 as part of the preparation of this study. The workshops targeted at



eliciting employees' requirements for PETs. In the workshops, participants were asked to list personal data that are frequently disclosed in employment or that they believe should be protected. Details on the workshops are available in [96]. For our survey, we combined the responses from four workshops with a total of 30 participants from four research institutions and one private company in Germany. Workshop participants included works councils, administrative staff, IT professionals, and researchers from the fields of ergonomics, data protection law, and human-computer interaction. From the responses, we created a consolidated list of personal data with 50 unique items. Given the expertise of our workshop participants, we consider the list to reflect a fair representation of personal data relevant for the purpose of our study. To address potential bias through participant recruitment, we have completed the list with items from studies on privacy in the online and marketing context [271, 274]. Some items were omitted, if they have a different meaning in the German-cultural space or if no equivalent exists. The full questionnaire is available in Appendix C.1. The final list of personal data items is available in Figure 6.4 and in Appendix C.4.

### 6.2.3 Study procedure

Our survey requires participants to respond to a total of 183 items. As a result, the length of the questionnaire and the associated workload may influence employees' willingness to participate, leading to fatigue near the end of the survey, and increasing the risk of unbalanced responses [318]. We have therefore created a two-part questionnaire to make the survey more appealing to employees, easier to complete, and to avoid quality loss due to excessive and repetitive question design. The first part (Part 1) is composed of three sub-parts: (1) Demographics related to employment, (2) ratings of *perceived data sensitivity* and *willingness to disclose* 62 personal data items, and (3) remaining demographics and survey feedback for part one. The second part (Part 2) comprises questions on the variables of our causal model and survey feedback for part two.

### 6.2.4 Participant recruitment and enrollment

We recruited our participants via the two online panels Prolific (N = 351) and Respondi (N = 111), as well as via mailing lists of organizations we contacted (convenience sampling), and through social media of the local Chamber of Commerce and Industry (N = 133) (N<sub>total</sub> = 595). The reason for distributing the survey across multiple channels was to reach a larger number of participants and to reduce demographic bias from individual channels, as response rates via Prolific were low for some demographic groups. First, we invited participants to complete Part 1, and then reinvited them to Part 2 two days later. To avoid methodical artifacts, we screened participants to ensure that they were employed in Germany and spoke German. After survey completion, we linked the responses from both parts by merging the data from the surveys. For the online panels, we used user identifiers provided by the panels. For all other recruitment channels, we used passcodes generated by the participants themselves. Passcodes were created in the first survey and had to be re-entered in the second survey. Neither the user identifiers nor the passcodes allow us to identify the natural persons. Furthermore, we have removed participants from the data based on timing, the number of missing responses ( $\geq 10\%$ ), and participants' self-assessed quality of the responses, consisting

of ratings for honesty and seriousness. We additionally checked the data for multivariate outliers and straightlining response patterns. Response times averaged 11.7 minutes (median = 9.8) for Part 1 and 12.8 minutes (median = 11.6) for Part 2.

#### 6.2.5 Participant demographics

In total, we have accepted 553 responses as valid for Part 1, and 393 responses for Part 2. The sample demographics are summarized in Table 6.1. Overall, our sample is slightly biased in favor of younger male participants as there is a small positive correlation between sex and age ( $\rho = .17$ , Confidence Interval (CI)<sub>95</sub>: [.08, .25]). Nevertheless, participants' ages spanned the typical period of employment ( $x \in [18, 67]$ ,  $\bar{x} = 39.6$ ,  $sd = 12.3$ ). At the time of the survey, half the respondents had been employed by their current employer for at least six years ( $x \in [0, 46]$ ,  $\bar{x} = 8.77$ ,  $sd = 9.5$ ). Three-quarters had permanent employment, and half of the participants regularly processed personal data as part of their job. In addition, our sample includes employees from 18 different industries and 12 different occupational groups. The distribution of industries among the top five industries was balanced, but a bias toward the service sector was observed among professional groups. Compared to the overall population of employees in Germany [319], however, our sample is biased toward younger employees with a university degree who work for large organizations, have a slightly shorter job tenure, and higher income. Our participants also primarily worked in the fields of IT, science, business, law, and education. Details on the industries and professional groups, and a separate presentation of the demographics of Part 1 and Part 2, as well as a comparison with the population of employees in Germany, can be found in Appendix C.3.

#### 6.2.6 Evaluation and data analysis

To answer **RQ2<sub>a-d</sub>**, we analyzed the data from Part 1 because it contained responses to *perceived data sensitivity* and *willingness to disclose*. To test the hypotheses **H1** – **H10** under **RQ3** and to investigate **RQ4**, we used the subsample of Part 2, as it contained responses to the latent constructs (i.e., antecedents and privacy beliefs). All analyses were performed using R. The packages used are reported in Appendix C.2. In the following, we will explain how we proceeded to answer our research questions.

##### 6.2.6.1 Comparison between contexts

To compare differences in perceived data sensitivity across different contexts under **RQ2<sub>a</sub>** “Does the employment context alter the ranking of personal data by perceived data sensitivity compared to other contexts?” we created an intersection of examined data items from our study and the three other studies considered [271, 273, 274]. The items were then ranked according to their mean scores per study. We then compared the pairwise Spearman rank correlation coefficients ( $\rho$ ) between all studies to verify whether the ranking of the items remain constant. Next, we examined whether the pairwise correlations between our German sample (employment context) and the German sample in [271] (online context) differed by running tests for differences in overlapping correlations. Significance was determined using the percentile bootstrap method of Rousselet et al. [320] at the 95% confidence interval (CI<sub>95</sub>,  $n_{boot} = 2000$ ).

Table 6.1: Participant demographics summary.

Description	Part 1	Part 2	Germany [319]
Participants	N: 553	N: 393	
Sex	%	%	%
Diverse	0.2	0.0	<i>n. a.</i>
Female	39.6	41.7	46.5
Male	59.7	58.3	53.5
Age (years)	%	%	%
$\leq 24$	8.7	9.9	1.3
25 – 34	32.4	3.5	22.1
35 – 44	27.1	29.0	21.9
45 – 54	14.6	14.0	23.6
55 – 64	16.5	15.8	29.9
$\geq 65$	.7	.8	1.2
Job tenure (years)	%	%	%
$\leq 4$	47.3	46.6	27.6
5 – 9	24.1	24.4	19.1
$\geq 10$	28.6	29.0	44.3
Org. size (num. employees)	%	%	%
< 10	8.0	7.1	18.0
10 – 249	34.4	32.8	38.0
250 – 999	25.7	26.7	44.0
$\geq 1k$	31.6	33.1	
Net income (€ / month)	%	%	%
< 1k	9.2	12.2	13.0
1k < 2k	36.7	31.6	42.0
2k < 3k	36.9	36.4	29.0
3k < 4k	11.4	12.7	10.0
$\geq 4k$	5.8	7.1	6.0
Other	%	%	%
University degree	58.2	58.3	16.9
Permanent employment	75.8	75.6	<i>n. a.</i>
Multiple jobs	7.6	7.6	5.4
German nationality <sup>1</sup>	88.2	86.0	87.5
Regular processing of personal data	<i>n. a.</i>	52.2	<i>n. a.</i>

Note. Part 1  $\supset$  Part 2; Full demographics are reported in Appendix C.3.

### 6.2.6.2 Latent structure analysis

For the examination of **RQ2<sub>b</sub>** “Can latent groups of personal data be identified in the employment context based on employees’ willingness to disclose and perceived data sensitivity?”, different options are available. A common approach is subdividing personal data according to the *perceived data sensitivity* using conventional clustering methods [271, 273, 274]. Such clusters differ in average perceived sensitivity, but are often difficult to interpret in terms of semantic meaning. In contrast, factorization approaches revealed latent groups of personal data with increased interpretability [251, 278, 282]. We therefore opted for the latter and conducted an Exploratory Factor Analysis (EFA) on the participants’ responses. We also ran a Confirmatory Factor Analysis (CFA) on *willingness to disclose* and *perceived data sensitivity* to validate the identified structure. We chose common factor analysis over principal component analysis, because research suggests that people’s willingness to disclose and perceived data sensitivity are influenced by latent variables, such as contextual norms [27, 248]. For analysis, we followed guidelines for EFA and CFA with ordinal data [321, 322, 323]: First, we removed personal data items with nonresponse rates  $\geq 10\%$  [323] and tested for univariate and multivariate normality to assess the suitability of the data for further analysis. Next, we examined the possibility of imputing missing data by testing for missing patterns using Little’s test. We also visually examined the data if we expected biased results due to violations of the multivariate normal assumption. To conduct EFA and CFA on different datasets, we split the data in half at random ( $N_{\text{EFA}} = 277$ ,  $N_{\text{CFA}} = 276$ ) and verified that the demographic properties were similar. Next, we examined the basic factorability assumption using the Kaiser–Meyer–Olkin measure of sampling adequacy, the Kaiser–Meyer–Olkin criterion, and Bartlett’s test of sphericity. To account for the ordinal nature of the data, we used polychoric correlations [324, 325]. We then removed items with high ( $|r| \geq .8$ ) or very low ( $|r| < .3$ ) pairwise correlations. The number of factors to retain was determined on the basis of multiple recommended criteria [321, 326]: Parallel analysis, Velicer’s Minimum Average Partial, and post-hoc model fit indexes, i.e., the Akaike Information Criterion and the Bayesian Information Criterion. The estimators for EFA were selected based on recommendations to recover weak factors in rather small samples or when multivariate normality is violated [321, 322], including Minimum Residuals, Unweighted Least Squares, and Principal Axis Factoring. We then compared the resulting solutions to each other, in order to ensure that the results replicated for the different estimators [322]. We used oblique rotation to address the expected correlations between emerging factors. After deciding on a factor solution, we have refined it iteratively using Hair et al. [323]’s three-step procedure. The latent factors identified from EFA were validated with CFAs using the robust estimator Weighted Least Square Mean and Variance Adjusted (WLSMV) [327]. First, we fitted a model to the EFA-subsample to detect severe model misspecification [327]. We then fitted a second model for the CFA-subsample to verify the latent structures’ validity and reliability for both *willingness to disclose* and *perceived data sensitivity*. Discriminant validity was validated using the Fornell-Larcker criteria and the Heterotrait-Monotrait Ratio of Correlation (HTMT) ( $< .85$ ) [328].

### 6.2.6.3 Comparison of groups of personal data

To compare groups of personal data under **RQ2<sub>c</sub>** “Do the perceived data sensitivity and willingness to disclose differ between groups of personal data?” and **RQ2<sub>d</sub>** “Is the magnitude

between perceived data sensitivity and willingness to disclose affected by the group of personal data?", we have created four groups according to the distinctions made in legal texts and standards discussed in Section 2.2.3: (1) The group *ALL* includes all 62 personal data items surveyed; (2) the group *GDPR* represents special categories of personal data under Arts. 9 & 10 GDPR [133]; (3) the group *IDENT* represents secure personal identifiers (e.g., Passport No.) [144]; and (4) the group *MASTER* refers to employee master data (e.g., contact details). The detailed item mapping is available in Appendix C.4. For each group, we have created subscales for Perceived Data Sensitivity (*PDS*) (i.e., *PDS<sub>ALL</sub>*, *PDS<sub>GDPR</sub>*, *PDS<sub>IDENT</sub>*, *PDS<sub>MASTER</sub>*) and for Willingness to Disclose (*WTD*) (i.e., *WTD<sub>ALL</sub>*, *WTD<sub>GDPR</sub>*, *WTD<sub>IDENT</sub>*, *WTD<sub>MASTER</sub>*). We also created additional subscales for groups of personal data identified in the latent structural analysis described above. Using these scales, we performed a regression analysis to compare the different groups, using *PDS* as the predictor and *WTD* as the outcome. *PDS<sub>ALL</sub>* and *WTD<sub>ALL</sub>* served as the baseline for comparisons. Violations of independence for the outcome variables were addressed by including random intercepts for participants and random slopes for *PDS* in Linear Mixed-effects Models (*LMMs*) and its robust variants. We have verified that the inclusion of random effects increased the model fit using likelihood-ratio tests. Verification of normality and homoscedasticity assumptions for residuals failed by visual inspection and using Levene test. All models were therefore fitted using robust *LMMs*. Significance checks were done using the robust *LMM*'s *t* value and the Satterthwaite approximations [329] of degrees of freedom of the corresponding regular *LMM* (cf. [330, 331]).

#### 6.2.6.4 Causal model analysis of antecedents and covariates

To examine **RQ3a** "How do common antecedents affect employees' perceived data sensitivity and willingness to disclose data in employment?", we analyzed the causal model depicted in Figure 6.2 using Structural Equation Modeling (*SEM*). Based on expected effect sizes in the range  $[.2 \leq |\beta| \leq .85]$  [262] and based on common rules of thumb, we decided that  $N_{\text{obs}} = 393$  was acceptable ( $N_{\text{obs}} \geq 300$ ,  $N_{\text{obs}}/N_{\text{var}} \geq 10$  [323, 332]). The validity of the measurement model and structural model as well as the constructs' reliability were assessed following guidelines in [323]. The variables *trust*, *risk beliefs*, *collection concern*, *unauthorized secondary use*, and *benefits* were modeled as reflective constructs. In contrast, *perceived data sensitivity* and *willingness to disclose* were modeled using composite scores. The reason behind this is that we test both latent groups of personal data identified using factor analysis, but also non-latent groups of personal data predefined in legal texts and standards. However, for the non-latent groups of personal data, the theoretical basis for modeling these as reflective constructs is missing. For example, the group *ALL* includes all 62 surveyed items and the group *GDPR* represents special categories of personal data that are predefined and which do not take into account latent aspects.

Furthermore, if fit indices of the fitted models indicated inadequate fit, we checked the variables' items for low factor loadings and ran an *EFA* with Principal Axis Factoring and oblimin rotation to identify items with high crossloadings. Identified items were then marked for deletion. After our measurement model achieved satisfactory fit, we modeled the causal *SEM* structure *a-priori* based on our hypothesized causal model outlined in Figure 6.2 above. To check for demographics differences, we also fitted a second model including our participants' demographics as control variables on *perceived data sensitivity* and *willingness to disclose*.

Next, for the studying of privacy specific covariates under **RQ3<sub>b</sub>** “Are common antecedents affected by employees’ personal disposition toward a right to privacy?”, we ran a multivariate regression analysis. For this purpose, we set up a Multiple Indicators and Multiple Causes (MIMIC) SEM model (cf. Figure 6.3). For the two latent variables *privacy as a right* and *complex privacy protection*, we performed the same checks for reliability and validity as for the other latent variables in our causal model. These were also modeled as reflective constructs, whereas *knowledge about privacy law* and *satisfaction with privacy law* were modeled as formative constructs. We also fitted a second model, including our participants’ demographics as control variables.

#### 6.2.6.5 Identification of employee groups

For answering **RQ4<sub>a</sub>** “Can employees be classified into groups according to willingness to disclose and perceived data sensitivity?” and **RQ4<sub>b</sub>** “Do these groups differ in terms of demographic factors or privacy attitudes?”, we performed Latent Class Analysis (LCA) to identify groups of employees based on their response patterns of *willingness to disclose*. LCA is a type of finite mixture modelling that determines classes (“clusters”) based on subpopulations with different sets of attributes. Observations are assigned probabilities belonging to each class. Here, classes are assumed to be unobserved categorical (latent) variables. We determined the optimal number of classes by first estimating a one-class model and then iteratively adding classes up to a maximum of five, as we expected group sizes similar to those in previous studies in other contexts [251, 283, 287, 288]. We evaluated model fit using various fit indices, with a focus on the Bayesian Information Criterion due to its superiority in LCA class selection [333]. To avoid local maxima, we ran 500 replications.

We have fixed participants’ class memberships based on posterior probabilities after deciding on the number of classes. To improve the posterior probabilities and reduce estimation attenuation [334], we ran latent class regression analysis with demographic covariates as dichotomous and attitudes as ordinal (three bins) variables. Before extracting the classes, we ensured that the entropy was greater than .8, indicating a low classification error. We then compared the fit of a constraint to the fit of an unconstrained multigroup SEM to test for differences between the extracted classes. If the likelihood-ratio test was significant, we performed distal outcome analysis for privacy antecedents using a MIMIC model and logistic regression for demographic variables.

### 6.3 EMPLOYEES' PERCEIVED DATA SENSITIVITY AND WILLINGNESS TO DISCLOSE

This section presents our findings related to research question **RQ2<sub>a</sub>** “Does the employment context alter the ranking of personal data by perceived data sensitivity compared to other contexts?” We first report the descriptive results in Section 6.3.1, followed by correlation and rank analysis in Section 6.3.2, and conclude with a discussion in Section 6.3.3.

#### 6.3.1 Descriptive results

The average scores for Perceived Data Sensitivity (PDS) and Willingness to Disclose (WTD) are plotted in Figure 6.4. Detailed scores are available in Appendix C.4. Consistent with the results of previous work in the online and marketing context, our results show that also in the employment context, *passwords* were perceived as the **most sensitive** data



type, whereas *hair color* was perceived as the **least sensitive** data type. It is striking that eight of the ten items with the lowest **PDS** can be clearly assigned to employee master data. The ratio of personal data types with a score for **PDS** < 5 and data types with a score for **PDS** > 5 is 21:41. This means that two-thirds of the data types were rated as rather sensitive information. Half of the data types have scores for **PDS** ≥ 6. The proportion of data types with scores for **WTD** < 5 and scores for **WTD** > 5 is 32:30, and is therefore balanced. The **lowest WTD** was found for *online dating activities*, closely followed by *passwords* and *DNA*. On the other hand, participants were **most willing** to disclose their *profession*, *education*, and *language skills* to employers. The ten items with the highest **WTD** are all directly related to employment.

### 6.3.2 Contextual differences

A visual comparison of the **PDS** scores from this study in Figure 6.4 with the **PDS** scores from previous studies conducted in the online and marketing contexts [271, 273, 274] reveals **differences in the rating of perceived data sensitivity**. With a few exceptions, the scores for less sensitive data are lower in this study than in other studies, whereas scores for more sensitive data are almost always higher in this study.

When comparing the rank order of the personal data items based on *perceived data sensitivity* between the different studies as described in Section 6.2.6.1, we found that the items in our study deviate on average 6.5 positions from the rank order of other studies [271, 273, 274]. We found particularly large differences ( $|\delta| \geq 10$ ) for *political opinion*, *religious affiliation*, and *GPS location*, which were perceived considerably **more sensitive in the employment context**. At the same time, *home address*, *health insurance No.*, *account No.*, and *social security No.* were perceived considerably **less sensitive in the employment context**. This trend also holds true when comparing only the results of the two German samples, i.e., our study with that of Schomakers et al. [271] (cf. Figure 6.5). For the German cultural context, we find that seven out of eight personal data items belonging to the special categories of the **GDPR** are ranked higher in the employment context (our study) than in the online context (Schomakers et al. [271]'s study). In contrast, seven out of ten data items belonging to employee master data are ranked lower than in the online context. No or minimal changes in the rank were observed for *passwords*, *private license plate*, *IP address*, *income level*, *number of children*, and *body size*.

Our comparison further reveals that the ranks between Schomakers et al. [271]'s study only deviate by an average of 2.6 ranks compared to the other two studies conducted in the online and marketing contexts [273, 274]. This implies that **personal data items were ranked similarly in previous studies despite the different contexts** (i.e., online vs marketing) and **despite cultural differences** (i.e., Germany vs. Saudi Arabia vs. Brazil vs the U.S.). This assumption is fostered by the pairwise scatter plots of the rankings from the different studies depicted in Figure 6.6. They reveal a clear linear relationship between the ranked **PDS** scores across all studies except for our study. A detailed comparison of *perceived data sensitivity* between the different studies using correlation analysis confirms the visual impression in terms of the high correlation coefficients for studies from the online and marketing contexts. Here, the scores determined in Schomakers et al. [271]'s study for the German sample have the highest correlation coefficients of all studies conducted. With values close to or greater than .9, these are very strong correlations. In contrast, the ranking of **PDS** scores in our study correlates only moderately to weakly



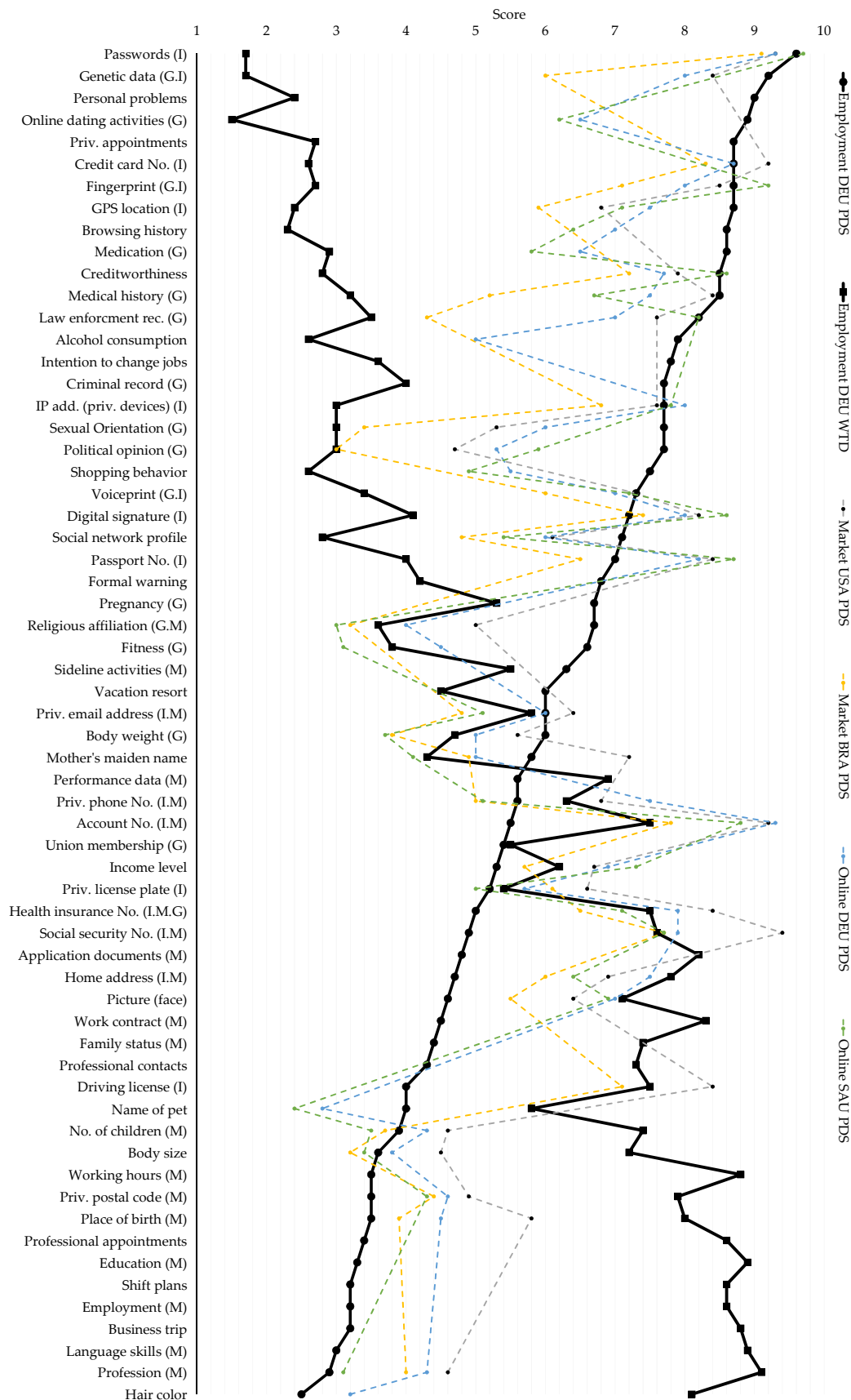


Figure 6.4: Mean values for PDS (dots) and WTD (square) of 62 personal data items, sorted by PDS (this study). Adjusted PDS scores from studies in other contexts and cultural backgrounds are included for comparison. Missing assignments indicate that the item was not surveyed in the corresponding study. "M" marks employee master data, "I" marks secure identifiers, and "G" marks data under GDPR.

with the ranking in previous studies. The pairwise comparisons between the pairwise differences further confirm that the **differences between the correlation coefficients** of our study and those of Schomakers et al. [271] are **significant in all cases** (cf. Figure 6.6). This suggests that the perceived sensitivity of personal data in the employment context differs significantly from the perception in other contexts.

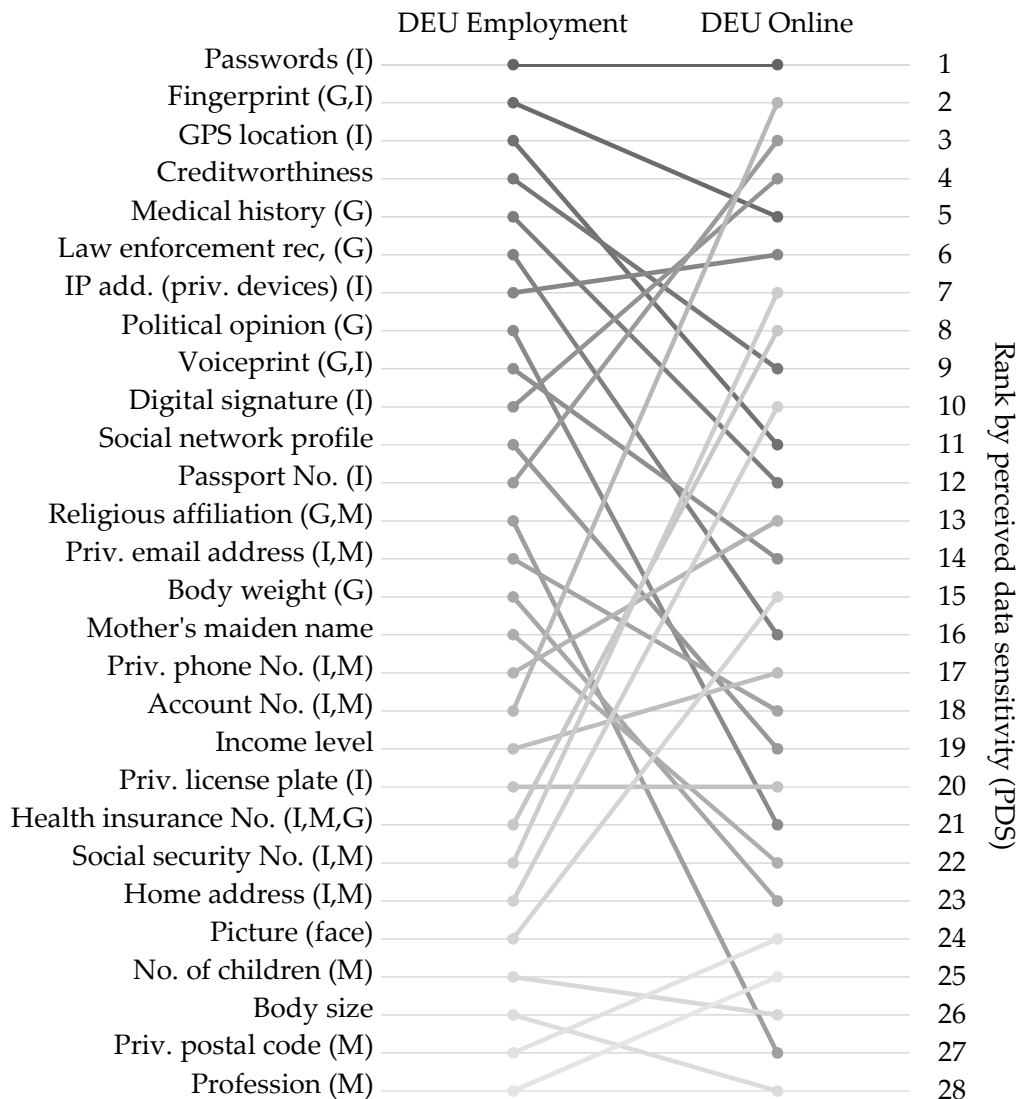
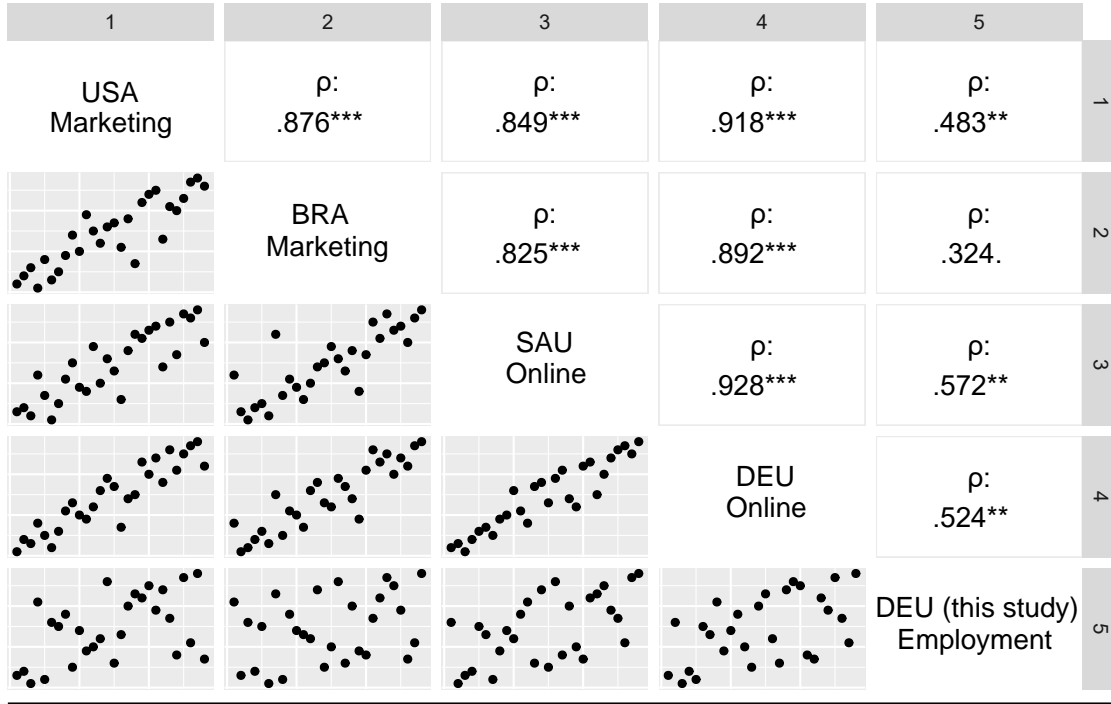


Figure 6.5: Changes in the rank order of personal data, ranked by *perceived data sensitivity* in the employment context (this study) versus the online context [271] for the German cultural area. Sorted from the most sensitive data type (rank 1) to the least sensitive data type (rank 28) according to this study's results. Personal data items are limited to the uniform set of data studied in all studies [271, 273, 274]. Average changes in rank are 6.7 positions.



Pairwise comparisons between this study and the study of Schomakers et al. [271]:

$\delta_{USA}$	$\rho_{4,1} - \rho_{5,1} = .43$	$CI_{95}: [.13, .80]$
$\delta_{BRA}$	$\rho_{4,2} - \rho_{5,2} = .57$	$CI_{95}: [.24, .94]$
$\delta_{SAU}$	$\rho_{4,3} - \rho_{5,3} = .35$	$CI_{95}: [.12, .65]$

$\therefore p < .1$  \*:  $p < .05$  \*\*:  $p < .01$  \*\*\*:  $p < .001$

Figure 6.6: Pairwise rank correlations (Spearman) of *perceived data sensitivity* of the same set of personal data items investigated in different studies with varying contexts and cultural backgrounds. The lower part shows pairwise comparisons between our study and the study in [271], both with samples from Germany. (USA: [274], BRA: [274], SAU: [273], DEU [271])

### 6.3.3 Discussion

Referring to **RQ2a** “Does the employment context alter the ranking of personal data by perceived data sensitivity compared to other contexts?”, our analysis revealed that scores for *perceived data sensitivity* in the employment context did indeed lead to a significant change in the ordering of the data items studied. First, our analysis shows that *perceived data sensitivity* varied more between the employment context and all other contexts than between online and marketing contexts. Second, our analysis also shows that even when cultural factors are taken into account, perceptions in the employment context still differ significantly from other contexts. Although we identified differences between previous studies from the online and marketing contexts that are likely attributable to cultural factors, our analysis shows that the employment context led to a 2.5 times stronger effect when comparing our results to another sample from Germany of similar size in the online context ( $N_{[271]} = 592$ ). Consequently, we find that other authors’ assumption of a global consensus regarding people’s personal data sensitivity perceptions (cf. “Con-

*textual differences*” in Section 6.1.1) seems to be supported for the online and marketing contexts, but becomes obsolete when results are compared to the employment context. This supports our assertion that privacy in the employment context deserves dedicated consideration, and that further research is needed to investigate such differences.

Furthermore, with respect to Contextual Integrity, our analysis clearly shows that the contextual norms that apply to the employment relationship differ from those that apply in other contexts. The differences were expressed specifically by the relative increase in perceived sensitivity of personal data items belonging to the special categories under the GDPR. In contrast, employers' access to all forms of master data, and in particular unique identifiers (e.g., passport number), appears to be compatible with contextual norms. In comparison with work from the U.S., it appears that the employees surveyed in our study, unlike U.S. employees (cf. Section 3.2.2), also regard medical data as inappropriate. At the same time, the results are similar in that employees consider religious and philosophical beliefs inappropriate, although employers in Germany usually process this information about their employees in the case of members of Christian churches. This could mean that current (legal) practice violates contextual norms and that employees would prefer not to have to disclose this data. It is also possible that our sample counts few church members.

#### 6.4 GROUPS OF PERSONAL DATA

Having described and compared our dataset in terms of perceived data sensitivity and willingness to disclose with other work in the previous section, we now turn to research questions **RQ2<sub>b-d</sub>**. First, we report the results of the EFA and the CFA applied on our participants' responses to identify latent groups of personal data in Section 6.4.1. We then report our comparative analysis of our participants' willingness to disclose and perceived data sensitivity of different groups of data in Section 6.4.2. We conclude this section with a discussion of our results in Section 6.4.3.

##### 6.4.1 Identification of latent groups of personal data

In the following, we report the results of our latent structure analysis outlined in Section 6.2.6.2 above to examine **RQ2<sub>b</sub>** “Can latent groups of personal data be identified in the employment context based on employees' willingness to disclose and perceived data sensitivity?” Our tests for univariate and multivariate normality of our participants' responses indicated violation of the normality assumption. Furthermore, based on insignificant results of Little's test ( $\chi^2(2196) = 1784.212$ ,  $p > .99$ ) and visual inspection of the data, we concluded that data were missing completely at random. We have therefore imputed missing data using the non-parametric method *missForest* suitable for ordinal data [335]. Next, the basic factorability assumption was confirmed by all items having acceptable values for the Kaiser–Meyer–Olkin measure of sampling adequacy ( $\geq .85$ ) and by the Kaiser–Meyer–Olkin criterion ( $\geq .91$ ) indicating “meritorious” factorability of the correlation matrix. The Bartlett's test of sphericity was also significant ( $\chi^2(1830) = 8394.02$ ,  $p < .001$ ), implying that the correlation matrix was appropriate for factor analysis.

Since all variables loaded with wide communality ( $> .5$ ) and we had a large variable-to-factor ratio, we deemed our sample size to be adequate for further analysis [336]. Factor retention criteria suggested retaining between three and six factors, which is con-

Table 6.2: Latent groups of personal data and results of the Confirmatory Factor Analysis (CFA) for Willingness to Disclose (WTD) and Perceived Data Sensitivity (PDS).

	WTD	PDS
Model fit		
Scaled fit indices		
$\chi^2(\text{df})$ , ***: $p < .001$	(129): 207.9***	(98): 188.9***
Comparative Fit Index (CFI)	.98	.99
Goodness of Fit (GFI)	.99	.99
Root Mean Square Error of Approximation (RMSEA)	.05	.06
Recommended values [323]: CFI > .94, GFI > .95, RMSEA < .7		
Identified latent constructs and their items		
<i>SENS</i>	$\lambda$	$\lambda$
Genetic data	.87 $\alpha$ .83	.59 $\alpha$ .81
Personal problems	.71 $\omega$ .84	.68 $\omega$ .82
GPS location	.70 AVE .58	AVE .58
Medication	.73	.83
Creditworthiness	.74	.77
Medical history	.82	.90
<i>NOTSENS</i>	$\lambda$	$\lambda$
Hair color	.82 $\alpha$ .74	.90 $\alpha$ .70
Body size	.83 $\omega$ .77	.74 $\omega$ .73
Body weight	.73 AVE .63	AVE .68
<i>PII</i>	$\lambda$	$\lambda$
Home address	.80 $\alpha$ .81	.87 $\alpha$ .90
Social security No.	.80 $\omega$ .82	.91 $\omega$ .91
Health insurance No.	.82 AVE .63	.89 AVE .78
Account number	.77	.86
<i>WORK</i>	$\lambda$	$\lambda$
Employment	.87 $\alpha$ .79	.86 $\alpha$ .91
Profession	.85 $\omega$ .81	.85 $\omega$ .92
Professional appointments	.72 AVE .61	.86 AVE .76
Shift plans	.77	.89
Business trip	.67	.90
Recommended values [323]: $\lambda \geq .7$ , $\alpha \geq .7$ , $\omega \geq .7$ , AVE $\geq .5$		

sistent with the range of dimensions of personal data proposed in previous work on different contexts [66, 246, 251, 271, 274, 278, 282]. Due to the high number of items, the skewed data, and the sample size, we focused particularly on avoiding bias towards overfactoring [337], i.e., identifying too many factors. After comparing different factor solutions, a **four factor solution** using Principal Axis Factoring and Promax rotation achieved the best partitioning in terms of acceptable loading height ( $> .45$ ), low number of cross-loadings (relative magnitude of variance [323]), acceptable commonality ( $\geq .5$ ), and interpretability of the factors. Iterative refinement resulted in a set of 18 items. The final CFAs with the second half of the participants, conducted to confirm the four identified factors, showed good to acceptable model fits. All indicators for construct reliability were in acceptable range and discriminant validity has been confirmed. The results of the analysis, including details on model fit, reliability, validity, and factor loadings, are reported in Table 6.2.

To better distinguish the latent groups of personal data in further analysis, we have assigned them names to reflect the groups' characteristics of sensitivity and context. The first factor *SENS* comprises six personal data items. It represents personal data considered to be **sensitive and private**, as they are generally not related to the employment relationship (e.g., genetic data) or could have negative consequences if they become known to employers (e.g., medical history). The second factor *NOTSENS* contains three personal data items and represents the **least sensitive** data. Nevertheless, the data still belong an employee's private sphere, since they are generally not directly related to the employment relationship (e.g., hair color). In contrast to *SENS* though, they are not expected to have any negative consequences. The third factor *PII* comprises four personal data items, and contains data types belonging to **personal identifiers** and which must usually be disclosed for employment (e.g., social security number). The fourth factor, *WORK*, contains five personal data items that represent types of data directly **resulting from work** or employment (e.g., profession).

#### 6.4.2 Differences in sensitivity and willingness to disclose

After we have successfully identified latent groups of personal data from our participants' responses, we now compare different groups of personal data with regard to differences in the relationship between *PDS* and *WTD*. To examine **RQ2<sub>c</sub>** "Do the perceived data sensitivity and willingness to disclose differ between groups of personal data?" and **RQ2<sub>d</sub>** "Is the magnitude between perceived data sensitivity and willingness to disclose affected by the group of personal data?", we used a set of eight groups of personal data. The set comprises the **four latent groups** *SENS*, *NOTSENS*, *PII*, and *WORK*, as well as the **four predefined non-latent groups** *ALL*, *GDPR*, *IDENT*, and *MASTER*. A summary of all the data groups examined is provided in Table 6.3.

The eight groups were compared to each other using *LMMs* as described in Section 6.2.6.3. We found that the models' fit significantly increased when including random effects ( $\text{Fit}_{\text{PDS}}: \chi^2(1) = 462.28, p < .001$ ;  $\text{Fit}_{\text{WTD}}: \chi^2(2) = 457.5, p < .001$ ). The results of regression analysis are reported in Figure 6.7 and Table 6.4, respectively. We found that *PDS* and *WTD* were significantly different across all eight groups of personal data studied. For one thing, the assessed scores deviated significantly from the baseline *PDS<sub>ALL</sub>* and *WTD<sub>ALL</sub>*. Second, Tukey post-hoc analysis further revealed that *PDS* and *WTD* differed also significantly among all groups of personal data studied ( $p < .001$ ). The only exceptions



Table 6.3: Groups of personal data examined.

Data group	Set of personal data items contained
Predefined groups (cf. Appendix C.4)	
<i>ALL</i>	All 62 items
<i>GDPR</i>	Special categories under Arts. 9 & 10 GDPR [133]
<i>IDENT</i>	Secure personal identifiers (e.g., Passport No.) [144]
<i>MASTER</i>	Employee master data (e.g., contact details)
Latent groups (cf. Table 6.2 or Appendix C.4)	
<i>SENS</i>	Sensitive data types from the private sphere not related to employment and potentially harmful
<i>NOTSENS</i>	Least sensitive data types from the private sphere and not related to employment
<i>PII</i>	Personal and secure identifiers, usually disclosed to employers in Germany
<i>WORK</i>	Data types arising directly from employment

were the two groups *MASTER* and *PII*, between which no significant difference was found. Furthermore, for groups of personal data clearly related to employment, i.e., *PII*, *MASTER*, and *WORK*, we found significantly lower *PDS* scores compared to the baseline *PDS<sub>ALL</sub>*. Likewise, scores for *WTD<sub>PII</sub>*, *MASTER*, *WORK* were significantly higher than *WTD<sub>ALL</sub>*. For other groups of (mostly non-employment-related) personal data, this effect was reversed: Scores for *PDS<sub>GDPR</sub>*, *IDENT*, *SENS* were significantly higher than *PDS<sub>ALL</sub>*, and scores for *WTD<sub>GDPR</sub>*, *IDENT*, *SENS* were significantly lower than *WTD<sub>ALL</sub>*. This finding **confirms the context-dependence** that underlies people's intention to disclose (cf. Section 2.4.4). A notable exception is the group *NOTSENS*, which comprises non-employment-related data but behaved like employment-related data groups. Contrary to intuition, *PDS<sub>NOTSENS</sub>* was even much lower compared to *PDS<sub>PII</sub>* and *PDS<sub>MASTER</sub>* (cf. Table 6.4). This highlights that *NOTSENS* represents personal data of **very low sensitivity**. In contrast, however, *WTD<sub>NOTSENS</sub>* was also significantly lower compared to *WTD<sub>PII</sub>* and *WTD<sub>MASTER</sub>*.

Moreover, taking a closer look at the observed effects for latent and non-latent groups of personal data, we note that the latent group *SENS* reflects personal data **considerably more sensitive** than the non-latent group *GDPR*. Indeed, the effects of *PDS<sub>SENS</sub>* and *WTD<sub>SENS</sub>* are almost twice as strong as those of *PDS<sub>GDPR</sub>* and *WTD<sub>GDPR</sub>* (cf. Table 6.4). Likewise, the latent group *WORK* also reflects personal data **considerably less sensitive** than the non-latent group *MASTER*. Again, the effect for *PDS<sub>WORK</sub>* is almost twice as strong as that of *PDS<sub>MASTER</sub>*.

Examining the magnitude between *perceived data sensitivity* and *willingness to disclose*, we found that *PDS* had a notable **significant negative effect** on *WTD* for all data groups studied. However, visual inspection of the regression lines (cf. Figure 6.7) reveals that this magnitude is significantly steeper for the *NOTSENS* group. Tukey post-hoc analysis confirmed this observation ( $p < .001$ ). In summary, this indicates that mild changes in the level of *PDS<sub>NOTSENS</sub>* lead to significant larger changes in *WTD<sub>NOTSENS</sub>* than is the case for



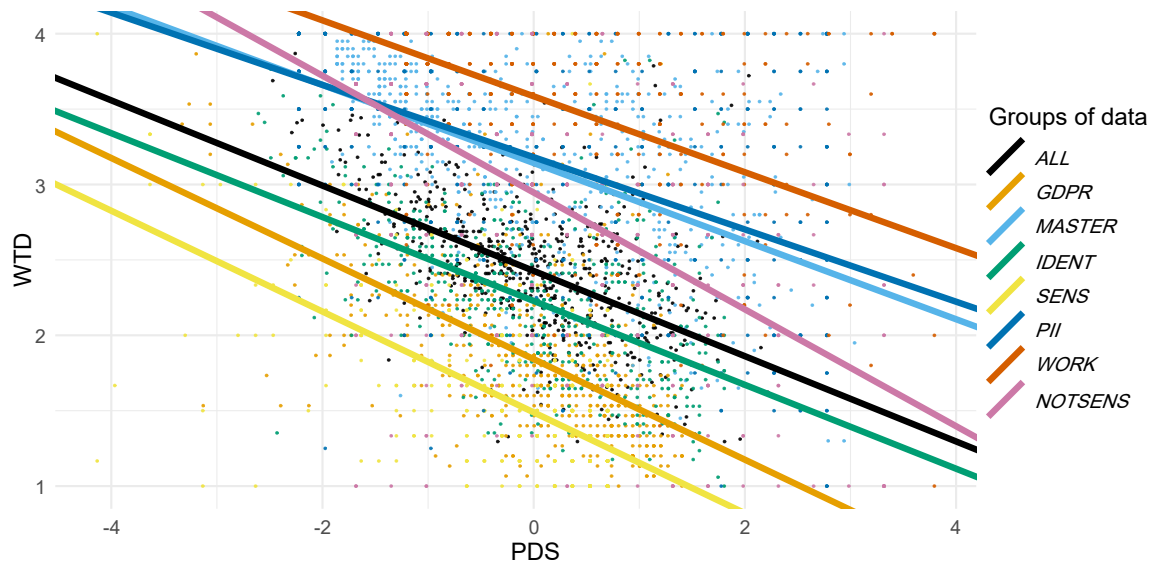


Figure 6.7: Robust LMM's fixed effects between Willingness to Disclose (WTD) and Perceived Data Sensitivity (PDS) for different groups of personal data.

all other groups of personal data. The analysis also revealed that the magnitudes for the groups *GDPR* and *SENS* are steeper than for *PII* ( $-.09$ ,  $CI_{95}[-.15, -.03]$ ). Apart from these exceptions, however, the relationship between *perceived data sensitivity* and *willingness to disclose* appears to be largely **constant among different groups of personal data**.

Table 6.4: Results robust LMMs with random effects by participants. The different groups of personal data are compared with the group *ALL* as a baseline.

Predictors	Perceived Data Sensitivity (PDS)		Willingness to Disclose (WTD)	
	Est.	$CI_{95}$	Est.	$CI_{95}$
(Intercept)	3.78***	[ 3.69, 3.88 ]	2.43***	[ 2.43, 2.46 ]
<i>GDPR</i>	.84***	[ .72, .96 ]	-.59***	[ -.63, -.54 ]
<i>MASTER</i>	-.85***	[ -.97, -.73 ]	.72***	[ .67, .76 ]
<i>IDENT</i>	.43***	[ .31, .55 ]	-.20***	[ -.24, -.16 ]
<i>SENS</i>	1.58***	[ 1.46, 1.70 ]	-.94***	[ -.98, -.89 ]
<i>PII</i>	-.68***	[ -.80, -.56 ]	.75***	[ .71, .80 ]
<i>WORK</i>	-1.68***	[ 1.80, -1.55 ]	1.16***	[ 1.11, 1.20 ]
<i>NOTSENS</i>	-1.18***	[ 1.30, -1.06 ]	.52***	[ .48, .56 ]
$PDS^c$			-.28***	[ -.32, -.24 ]
$NOTSENS \times PDS^c$			-.10***	[ -.15, -.06 ]
$R^2_m / R^2_c$	.458 / .586		.749 / .843	

Note. N = 553

\*\*\*:  $p < .001$

$R^2_m$ : marginal;  $R^2_c$ : conditional <sup>c</sup>centered

### 6.4.3 Discussion

In this section, we have concentrated on answering research questions **RQ2<sub>b-d</sub>** that focused on identifying and comparing groups of personal data based on employees' perceptions of data sensitivity and willingness to disclose.

Starting with **RQ2<sub>b</sub>** "*Can latent groups of personal data be identified in the employment context based on employees' willingness to disclose and perceived data sensitivity?*", we identified four latent groups of personal data using factor analysis. The four groups emerged directly from our participants' response patterns and represent distinct dimensions of employees' perceptions for the employment relationship. Thereby, the four groups seem to differ primarily along the dimensions of contextual relevance and sphere. Accordingly, taking into account general social and political norms, data elements in the *SENS* and *NOTSENS* groups are not usually explicitly disclosed in an employment context. In fact, much of the processing of data in the *SENS* group for the purposes of an employment relationship is prohibited by law (cf. Section 2.2.4). In contrast, data under the groups *WORK* and *PII* are required for the employment context in Germany for formal or organizational reasons. Their disclosure is therefore backed by common social and political norms. Regarding the further categorization along the second dimension, the latent groups of personal data are connected to different proportions with intimate, private, and social spheres (cf. Section 2.2.1). Accordingly, data from the *SENS* group can be located between the outer intimate and inner private sphere, since their disclosure to employers threatens employees' autonomy and personal development. The group *NOTSENS*, on the other hand, can be placed between the outer private and the (public) social sphere, since employees can hardly avoid disclosing these types of personal data in their daily interactions with other subjects. Next, data of the group *WORK* are to be assigned fully to the (public) social sphere in the scope of an employment relationship, since they result directly from the relationship itself. In terms of *CPM* theory, personal data in this group are co-owned by both employee and employer, in the sense of an organizational privacy boundary. In contrast, the last group *PII* is mostly located in the employees' private sphere, making employees the owners of the data, while employers become only co-owners. Nevertheless, the boundary linkage between the employees' private sphere and the employer is strong and well-coordinated because employees usually disclose data under *PII* systematically.

Furthermore, our investigation of **RQ2<sub>c</sub>** "*Do the perceived data sensitivity and willingness to disclose differ between groups of personal data?*" revealed that employees perceive different groups of personal data as having different levels of sensitivity, and that their willingness to disclose also differs significantly by group. In line with the categorization of personal data based on their contextual relevance, we found that data more related to the employment context had significantly lower perceived data sensitivity as well as significantly higher willingness to disclose. However, our examination of **RQ2<sub>d</sub>** "*Is the magnitude between perceived data sensitivity and willingness to disclose affected by the group of personal data?*" found that in some cases, significantly lower perceived data sensitivity is not necessarily associated with an equivalently significantly higher willingness to disclose. For instance, although data under *NOTSENS* have no reference to the employment context, the group was perceived as significantly less sensitive than work-related data under the latent group *PII* as well as under the non-latent group *MASTER*. However, willingness to disclose was significantly lower for *NOTSENS* than for *PII* and *MAS-*

TER. A viable explanation would be that the two dimensions' contextual relevance and sphere have different effects on perceived data sensitivity and willingness to disclose. Based on our observation, it seems that perceived data sensitivity is primarily influenced by sphere, whereas willingness to disclose is primarily affected by contextual relevance. Based on this assumption, *PII* and *MASTER* were perceived as more sensitive than *NOTSENS*, because they are located in the private sphere of an individual, whereas *NOTSENS* is located in the (public) social sphere. At the same time, though, the high contextual relevance of *PII* and *MASTER* makes employees disclose the data anyway, whilst missing contextual relevance for *NOTSENS* leads to much lower willingness to disclose. Apart from this special case, however, the magnitude between perceived sensitivity and willingness to disclose seems to be largely stable.

Moreover, comparing the latent data groups from factor analysis with the definitions of non-latent data groups drawn from the literature and law, we find that in some cases latent groups represent much more homogeneous forms of non-latent groups. For example, the latent data group *PII* and the non-latent data group *MASTER* had similar scores for perceived sensitivity and willingness to disclose. Likewise, the magnitude and direction of effects between perceived data sensitivity and willingness to disclose were identical for the latent data group *SENS* and the non-latent data group *GDPR*, as well as for the latent data group *WORK* and the non-latent data group *MASTER*. These results emphasize that these respective tuples of data groups' share strong similarities.

## 6.5 ANTECEDENTS AND CAUSAL MODEL

After having identified latent groups of personal data and contrasting differences in employees' perceptions of data sensitivity and willingness to provide, we now tackle the current lack of studies focused on investigating the determinants of these perceptions in the employment context. To examine research question **RQ3** "*Which antecedents influence employees' perception of personal data?*", we first present our analysis of determinants of perceived data sensitivity and willingness to disclose in Section 6.5.1. We then explore different effects of employee privacy disposition on these determinants in Section 6.5.2 and discuss our results in Section 6.5.3. The basic descriptive statistics of all variables used for analysis are summarized in Table 6.5.

### 6.5.1 Determinants of data sensitivity and willingness to disclose

For investigating **RQ3a** "*How do common antecedents affect employees' perceived data sensitivity and willingness to disclose data in employment?*" we applied Structural Equation Modeling (SEM) analysis as outlined in Section 6.2.6.4 above. An initial CFA of the measurement model indicated overall adequate fit, and an EFA revealed clearly emerging factors. However, we removed an item for *risk beliefs* that cross-loaded onto *trust*. We also removed an item for *collection concern* with  $\rho > .9$  on multiple items of *risk beliefs*, as well as an item for *benefits* with a particular low loading. While this relaxed the variance shared between the constructs, their correlation remained strong. Nevertheless, the adjusted measurement model had acceptable fit ( $\chi^2(81) = 202.15$ ,  $p < .001$ , CFI = .98, GFI = .99, RMSEA = .062), and indicators for construct reliability and validity were in acceptable range (cf. Table 6.6). In addition, all subsequent SEM analyses also showed adequate model fit. The detailed analysis results for the non-latent groups of personal

data are reported in Table 6.7 and Figure 6.8a, whereas analysis results for the latent groups of personal data are reported in Table 6.8 and Figure 6.8b, respectively. Results for antecedents are reported in Table 6.9.

**ANTECEDENT EFFECTS** SEM analysis **confirmed** significant moderate ( $.3 \leq |\beta| \leq .5$ ) **negative effects** of *perceived data sensitivity* on *willingness to disclose* for **all groups of personal data**. In contrast, our hypotheses regarding the **effects of antecedents** on *willingness to disclose* were confirmed only for **some groups but not for others**. For the anticipated positive effect of *trust* on *willingness to disclose*, we found small ( $|\beta| \leq .3$ ) significant

Table 6.5: Summary of variables used in SEM analysis.

Willingness to disclose					Perceived data sensitivity				
Variable	$\bar{x}$	SD	Median	Scale	Variable	$\bar{x}$	SD	Median	Scale
ALL	2.44	0.42	2.43	4 pt	ALL	3.79	0.82	3.80	6 pt
GDPR	1.87	0.49	1.73	4 pt	GDPR	4.58	0.91	4.67	6 pt
IDENT	2.25	0.48	2.24	4 pt	IDENT	4.22	0.97	4.29	6 pt
MASTER	3.17	0.53	3.25	4 pt	MASTER	2.98	1.18	2.85	6 pt
NOTSENS	2.87	0.80	3.00	4 pt	NOTSENS	2.70	1.23	2.67	6 pt
PII	3.18	0.78	3.25	4 pt	PII	3.23	1.74	3.25	6 pt
SENS	1.53	0.53	1.50	4 pt	SENS	5.30	0.90	5.67	6 pt
WORK	3.59	0.55	3.80	4 pt	WORK	2.20	1.16	2.00	6 pt

Antecedents					
	Variable	$\bar{x}$	SD	Median	Scale
Benefits	BFTS	3.48	1.33	3.50	6 pt
Collection concern	COLL	2.57	1.24	2.33	6 pt
Concern unauthorized secondary use	UNAU	5.39	0.79	5.67	6 pt
Risk beliefs	RSKB	2.04	1.01	2.00	6 pt
Trust	TRST	5.07	0.90	5.25	6 pt

Employee dispositions to privacy					
	Variable	$\bar{x}$	SD	Median	Scale
Complexity privacy protection	CPLX	3.17	1.23	3.00	6 pt
Privacy as a right	PRGT	4.08	1.18	4.00	6 pt
Satisfaction privacy law	SATL	4.29	1.21	4.00	6 pt
Knowledge	KNWL	1.66	0.76	1.00	3 pt <sup>1</sup>

Note. N = 393

<sup>1</sup>Measured with n = 5 multiple choice questions and converted to a 3-point scale with  $f(n_{\text{correct}} \leq 3) = 1$ ,  $f(n_{\text{correct}} = 4) = 2$ ,  $f(n_{\text{correct}} = 5) = 3$ .

Table 6.6: Construct reliability measures, validity measure, and correlations.

Var	$\alpha^a$	$\omega^a$	1. <sup>b</sup>	2.	3.	4.	5.	6.	7.	$\lambda^a$ (final selection only)	Sources
1. BFTS	.69	.8	<b>.67</b>	.03	0	0	.02	0	.02	1.00 .591	[255, 338]
2. COLL	.82	.83	.06	<b>.68</b>	.62	.47	.01	.19	.2	.835 .774 .857	[255, 338]
3. RSKB	.75	.79	.00	.79	<b>.63</b>	.5	.00	.07	.24	.745 .852 .779	[255, 338]
4. TRST	.88	.89	.11	-.69	-.7	<b>.75</b>	.00	.04	.26	.916 .756 .890 .886	[255, 338]
5. UNAU	.74	.77	-.15	.08	0	.04	<b>.63</b>	.21	.00	.810 .795 .772	[255, 338]
6. PRGT	.75	.76	-.03	.44	.26	-.2	.46	<b>.56</b>	.02	.809 .663 .768	[288]
7. CPLX	.75	.77	.11	.44	.49	-.51	-.04	.13	<b>.56</b>	.777 .672 .800	[287]

Note. N = 393

<sup>a</sup>: Recommended values [323]:  $\lambda \geq .7$ ,  $\alpha \geq .7$ ,  $\omega \geq .7$ , Average Variance Extracted (AVE)  $\geq .5$

<sup>b</sup>: lower triangle: inter-construct correlation ( $\rho$ ), bold diagonal: AVE, upper triangle:  $\rho^2$

Discriminant validity (Fornell-Larcker) requires  $\rho^2 < \text{AVE}$

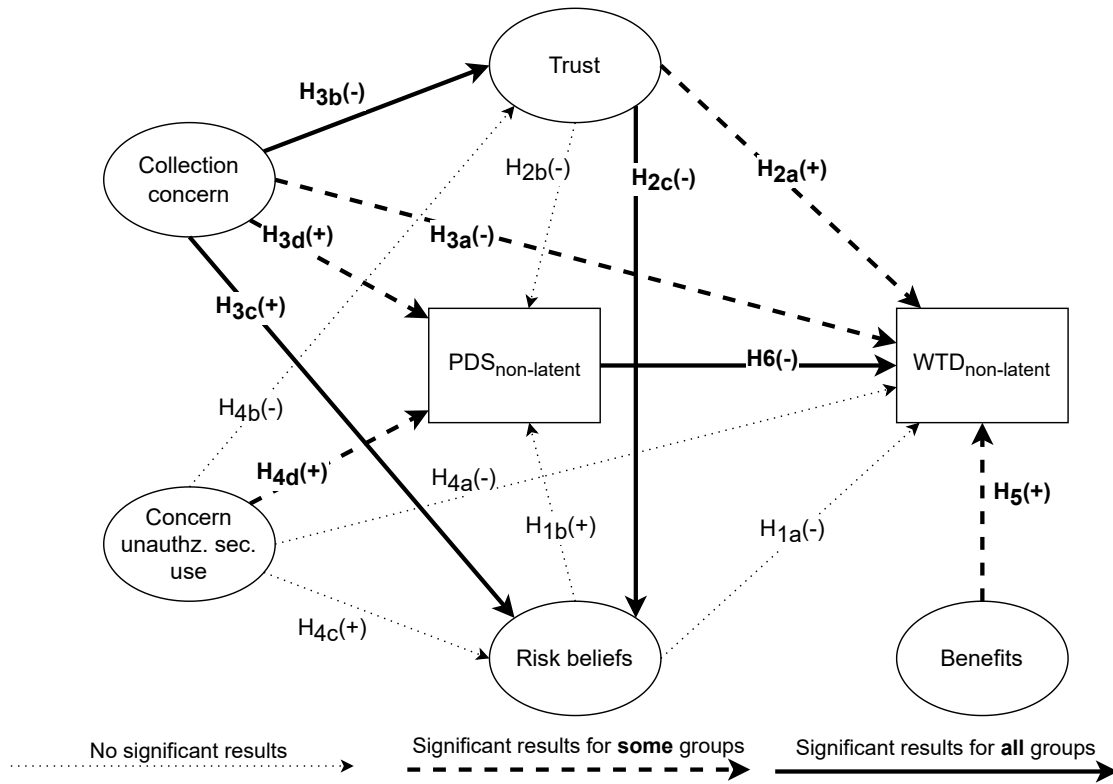
effects for  $\text{WTD}_{\text{ALL}}$  and  $\text{WTD}_{\text{GDPR}}$ . We also found a small significant negative effect of *collection concern* on  $\text{WTD}_{\text{SENS}}$ , as well as a small significant negative effect of *unauthorized secondary use* on  $\text{WTD}_{\text{IDENT}}$ . In terms of employees' perceived *benefits*, we found small significant positive effects on all non-latent groups, i.e.,  $\text{WTD}_{\text{ALL, GDPR, IDENT, MASTER}}$ , as well as on one latent group, i.e.,  $\text{WTD}_{\text{WORK}}$ .

Regarding effects on *perceived data sensitivity*, we found a small significant negative effect of *risk beliefs* on  $\text{PDS}_{\text{GDPR}}$ , and several significant small to moderate positive effects of *collection concern* on the four non-latent data groups, i.e., on  $\text{PDS}_{\text{ALL, GDPR, IDENT, MASTER}}$ . There were also small significant effects of *unauthorized secondary use* on  $\text{PDS}_{\text{ALL, GDPR, IDENT}}$ . In summary, we find that privacy concerns primarily had small to positive significant effects on *perceived data sensitivity*, but hardly any effect on *willingness to disclose*. In addition, except for *perceived data sensitivity*, virtually all of the antecedents studied showed **effects exclusively for non-latent groups** of personal data.

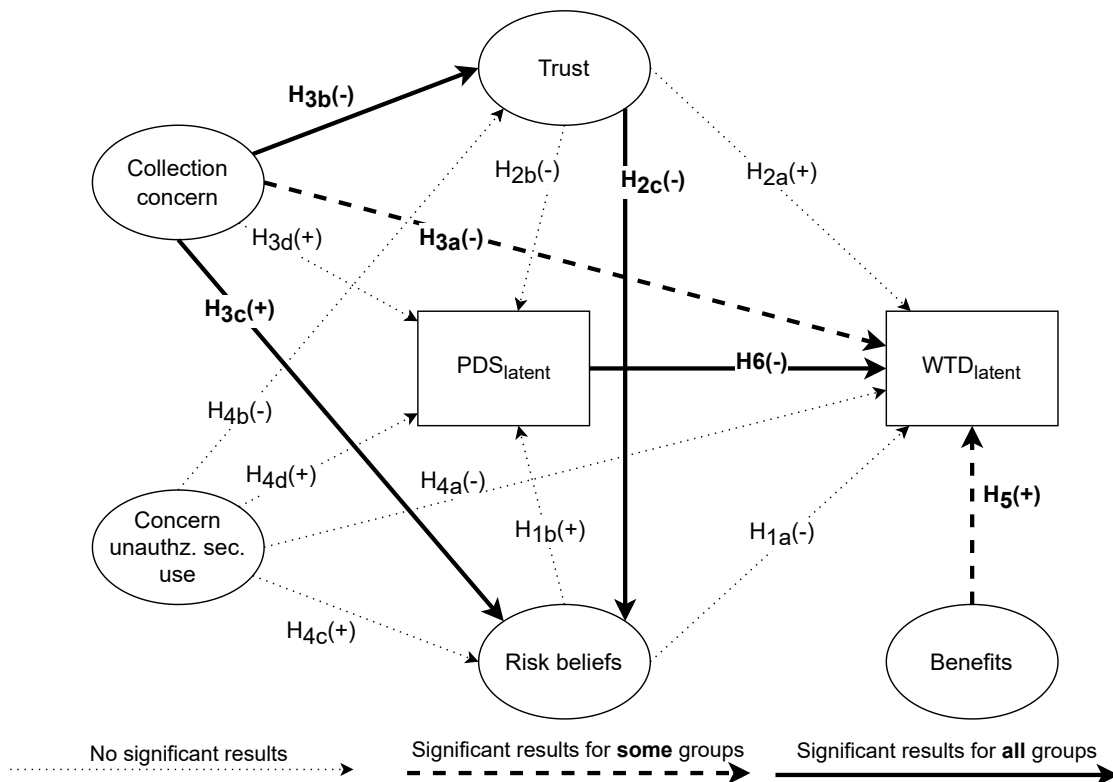
**ANTECEDENT INTERACTIONS** Regarding the relationships between antecedents, we found support for the following anticipated effects. First, *trust* in employers had a significant moderate negative effect on *risk beliefs*, while *collection concern* had a strong ( $|\beta| > .5$ ) positive effect on *risk beliefs*. Moreover, *collection concern* also had a strong negative effect on *trust*. In other words, employees who were **concerned about their employer's collection of personal data** had significantly **less trust** and also anticipated **greater privacy risks**. Concerning *unauthorized secondary use*, no anticipated effect was confirmed.

**DEMOGRAPHIC EFFECTS** With respect to demographic differences, we found **very few** and only **small significant effects**. At this point, we refrain from reporting effects whose confidence intervals ( $\text{CI}_{95}$ ) contain values that are not clearly different from zero. Yet, the detailed results are available in Appendix C.3 and Appendix C.5, respectively.

As such, we found significant small positive effects for German participants on  $\text{WTD}_{\text{ALL}}$  ( $\beta = .13$ ,  $\text{CI}_{95}$ : [.10, .88]), and  $\text{WTD}_{\text{MASTER}}$  ( $\beta = .16$ ,  $\text{CI}_{95}$ : [.22, .93]). Accordingly, Germans had significantly higher willingness to disclose these data to their employer compared to other participants in our sample. Furthermore, looking at effects on the antecedents



(a) Summary for antecedents (cf. Table 6.9) and non-latent groups of personal data (cf. Table 6.7).



(b) Summary for antecedents (cf. Table 6.9) and latent groups of personal data (cf. Table 6.8).

Figure 6.8: SEM models summarizing privacy antecedents' inter-effects and effects on Perceived Data Sensitivity (PDS) and Willingness to Disclose (WTD).

Table 6.7: Results SEM analysis non-latent groups of personal data.

				<i>ALL</i>			<i>GDPR</i>		
Model fit				$\chi^2$ : 293.22	CFI : .99		$\chi^2$ : 293.37	CFI : .99	
				df : 251	GFI : .99		df : 251	GFI : .99	
				p : .03	RMSEA : .02		p : .03	RMSEA : .02	
Hypothesized effect				Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
H1 <sub>a</sub>	RSKB	- →	WTD	.06	[-.07, .19]	.08	.08	[-.05, .21]	.11
H1 <sub>b</sub>	RSKB	+ →	PDS	-.09	[-.24, .05]	-.15	-.17	[-.31, -.02]	-.27*
H2 <sub>a</sub>	TRST	+ →	WTD	.15	[.02, .28]	.16*	.22	[.09, .35]	.23**
H2 <sub>b</sub>	TRST	- →	PDS	-.03	[-.17, .12]	-.04	-.10	[-.26, .06]	-.13
H3 <sub>a</sub>	COLL	- →	WTD	-.21	[-.42, .01]	-.16	-.11	[-.35, .12]	-.09
H3 <sub>d</sub>	COLL	+ →	PDS	.38	[.14, .62]	.35**	.39	[.13, .64]	.36**
H4 <sub>d</sub>	UNAU	+ →	PDS	.23	[.10, .35]	.21***	.25	[.14, .37]	.23***
H4 <sub>a</sub>	UNAU	- →	WTD	-.11	[-.24, .03]	-.09	-.07	[-.20, .06]	-.06
H5	BFTS	+ →	WTD	.22	[.10, .33]	.17***	.19	[.07, .31]	.14**
H6	PDS	- →	WTD	-.50	[-.60, -.41]	-.43***	-.62	[-.72, -.52]	-.51***
				<i>IDENT</i>			<i>MASTER</i>		
Model fit				$\chi^2$ : 293.22	CFI : .99		$\chi^2$ : 293.37	CFI : .99	
				df : 251	GFI : .99		df : 251	GFI : .99	
				p : .03	RMSEA : .02		p : .03	RMSEA : .02	
Hypothesized effect				Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
H1 <sub>a</sub>	RSKB	- →	WTD	.01	[-.12, .14]	.01	.01	[-.12, .14]	.02
H1 <sub>b</sub>	RSKB	+ →	PDS	-.15	[-.30, .00]	-.24	.00	[-.14, .14]	-.01
H2 <sub>a</sub>	TRST	+ →	WTD	.11	[-.02, .24]	.12	.06	[-.06, .18]	.07
H2 <sub>b</sub>	TRST	- →	PDS	-.04	[-.18, .11]	-.05	.01	[-.13, .14]	.01
H3 <sub>a</sub>	COLL	- →	WTD	-.16	[-.39, .07]	-.13	-.21	[-.41, .00]	-.18
H3 <sub>d</sub>	COLL	+ →	PDS	.42	[.17, .67]	.40**	.24	[.01, .48]	.24*
H4 <sub>d</sub>	UNAU	+ →	PDS	.16	[.04, .29]	.15*	.08	[-.04, .20]	.08
H4 <sub>a</sub>	UNAU	- →	WTD	-.15	[-.29, -.01]	-.12*	-.07	[-.21, .07]	-.06
H5	BFTS	+ →	WTD	.24	[.11, .36]	.19***	.17	[.05, .28]	.14**
H6	PDS	- →	WTD	-.50	[-.60, -.41]	-.43***	-.47	[-.58, -.36]	-.41***

Note. N = 393

\*:  $p < .05$  \*\*:  $p < .01$  \*\*\*:  $p < .001$

$\beta$ : standardized path coefficient (measure of effect size [339])



Table 6.8: Results SEM analysis latent groups of personal data.

				<i>NOTSENS</i>			<i>PII</i>		
Model fit				$\chi^2$ : 293.22	CFI : .99		$\chi^2$ : 293.37	CFI : .99	
				df : 251	GFI : .99		df : 251	GFI : .99	
				p : .03	RMSEA : .02		p : .03	RMSEA : .02	
Hypothesized effect				Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
H1 <sub>a</sub>	RSKB	- →	WTD	.06	[-.09, .21]	.09	.07	[-.10, .24]	.12
H1 <sub>b</sub>	RSKB	+ →	PDS	.06	[-.08, .20]	.11	.07	[-.08, .23]	.12
H2 <sub>a</sub>	TRST	+ →	WTD	.04	[-.10, .18]	.05	.06	[-.07, .18]	.07
H2 <sub>b</sub>	TRST	- →	PDS	.00	[-.14, .14]	-.01	.10	[-.04, .23]	.13
H3 <sub>a</sub>	COLL	- →	WTD	-.08	[-.33, .18]	-.07	-.06	[-.32, .20]	-.06
H3 <sub>d</sub>	COLL	+ →	PDS	-.12	[-.34, .10]	-.12	-.04	[-.28, .21]	-.04
H4 <sub>d</sub>	UNAU	+ →	PDS	.02	[-.11, .15]	.02	-.06	[-.18, .06]	-.06
H4 <sub>a</sub>	UNAU	- →	WTD	-.04	[-.16, .09]	-.03	.05	[-.08, .17]	.04
H5	BFTS	+ →	WTD	-.04	[-.16, .08]	-.04	.00	[-.12, .12]	.00
H6	PDS	- →	WTD	-.56	[-.66, -.47]	-.49 <sup>***</sup>	-.44	[-.56, -.33]	-.41 <sup>***</sup>
				<i>SENS</i>			<i>WORK</i>		
Model fit				$\chi^2$ : 293.22	CFI : .99		$\chi^2$ : 293.37	CFI : .99	
				df : 251	GFI : .99		df : 251	GFI : .99	
				p : .03	RMSEA : .02		p : .03	RMSEA : .02	
Hypothesized effect				Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
H1 <sub>a</sub>	RSKB	- →	WTD	.08	[-.08, .24]	.12	-.03	[-.19, .13]	-.05
H1 <sub>a</sub>	RSKB	+ →	PDS	.00	[-.13, .13]	.00	.09	[-.06, .24]	.16
H2 <sub>a</sub>	TRST	+ →	WTD	-.09	[-.22, .04]	-.11	.03	[-.12, .18]	.04
H2 <sub>b</sub>	TRST	- →	PDS	-.03	[-.14, .08]	-.04	.08	[-.07, .23]	.11
H3 <sub>a</sub>	COLL	- →	WTD	-.32	[-.57, -.08]	-.28 <sup>*</sup>	.10	[-.14, .34]	.09
H3 <sub>d</sub>	COLL	+ →	PDS	-.09	[-.30, .12]	-.09	-.08	[-.32, .17]	-.08
H4 <sub>d</sub>	UNAU	+ →	PDS	-.06	[-.18, .05]	-.06	-.04	[-.16, .08]	-.04
H4 <sub>a</sub>	UNAU	- →	WTD	.06	[-.08, .20]	.05	.03	[-.11, .16]	.02
H5	BFTS	+ →	WTD	-.11	[-.24, .02]	-.09	.13	[.01, .25]	.12 <sup>*</sup>
H6	PDS	- →	WTD	-.59	[-.66, -.52]	-.50 <sup>***</sup>	-.44	[-.53, -.35]	-.40 <sup>***</sup>

Note. N = 393

\*:  $p < .05$  \*\*:  $p < .01$  \*\*\*:  $p < .001$

$\beta$ : standardized path coefficient (measure of effect size [339])



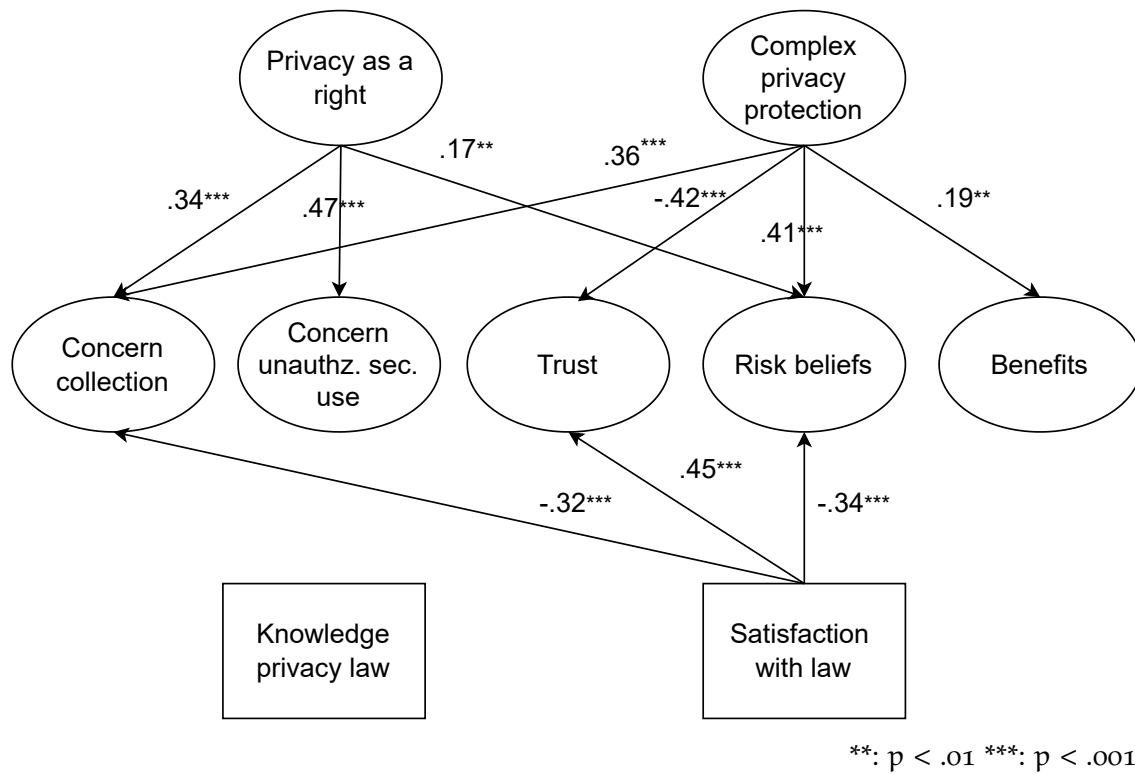


Figure 6.9: Effects of employees' disposition to privacy as a right. The detailed results are provided in Table 6.10. Only paths with significant effects are shown, together with the respective standardized path coefficients ( $\beta$ ). Ellipses symbolize reflective latent variables and rectangles symbolize formative variables.

With regard to **H10**, we found no significant effects of *knowledge about privacy law* on any antecedents studied.

**DEMOGRAPHIC EFFECTS** For demographic differences, we again found **very few and only small** significant effects. As before, we report only effects whose confidence intervals ( $CI_{95}$ ) contain values that are clearly different from zero. The detailed results are available in Appendix C.5.

Overall, we found neither effects from demographic variables on *complexity of privacy protection* nor on *satisfaction with privacy law*. Yet, we found significant small positive effects of both German participants and personal data processing participants on *knowledge* ( $\beta = .17$ ,  $CI_{95}$ : [.10, .88],  $\beta = .17$ ,  $CI_{95}$ : [.11, .60]). Consequently, participants who were German or regularly processed personal data as part of their job were likely to be more knowledgeable about privacy law than the non-German participants and the non-personal data processing participants. Moreover, we found a significant small positive effect on *privacy as a right* for participants with multiple employers ( $\beta = .14$ ,  $CI_{95}$ : [.12, 1.02]). Accordingly, participants who worked for multiple employers had slightly stronger convictions towards having a right to privacy in employment than participants who worked for only one employer.



of antecedents on *perceived data sensitivity* and *willingness to disclose* were largely inconsistent across different groups of personal data. Almost no significant effect was found, particularly for the latent groups of personal data, i.e., the groups identified using factor analysis. In contrast, *benefit*, *trust*, and *privacy concern* showed multiple significant effects on different non-latent groups of personal data. Such differences are likely attributable to the composition of data groups and the specific types of personal data (items) they encompass. Consequently, employees' privacy concerns seem to be less related to their perceived data sensitivity and willingness to disclose, and more related to the actual composition of personal data items than previously thought.

Furthermore, our findings show that concerns about employers collecting too much data severely affect trust in employers and lead to high perceptions of risk. That being said, our survey also shows that, on average, our participants indicated a very high level of trust in their employer. At the same time, risk belief was at a low level and over half the participants considered the disclosure of data to be more of a benefit (cf. Table 6.5). What is striking, however, is that our participants made extremely strong claims about data not being processed for secondary purposes unauthorized. The fact that we found no significant effects for *unauthorized secondary use* at the same time could mean that this conviction is made independently of other factors.

Turning towards RQ3b, "*Are common antecedents affected by employees' personal disposition toward a right to privacy?*", we found evidence that several factors uncovered in the mental model study did indeed have significant effects on employees' privacy perceptions and antecedents. We could confirm effects under H7 *privacy as a right*, H8 *complexity privacy protection*, and H9 *satisfaction privacy law*. However, we found no effect for H10 *knowledge*.

In this sense, it became apparent that employees' privacy concerns and risk beliefs increased as the protection of privacy in employment contexts was perceived as a fundamental right or as complex and difficult. Perceived complexity also showed significant negative effects on employees' trust in employers' handling of their personal data. Given that two-thirds of our participants tended to agree that privacy is a fundamental right in the employment context, and half of our participants considered the protection to be rather complex, these factors are certainly meaningful. According to findings in previous research on the online context, especially high levels of perceived complexity are critical because they can lead to resignation and cynicism about privacy protection [287, 340]. Studies in the online context defined "*»privacy cynicism« as an attitude of uncertainty, powerlessness and mistrust towards the handling of personal data by online services, rendering privacy protection behavior subjectively futile*" [340]. It serves to explain the privacy paradox, in that despite high concerns, trying to protect privacy is seen as a pointless undertaking, resulting in the disclosure of personal data. Following this line of reasoning, our study also shows that *complexity of privacy protection* did have a weak positive effect on anticipated *benefits*. Consistent with the mental model of Control-Seeking Pragmatist (CSP) identified in our first study (cf. Section 5.4.5), employees thus appear to seek control for protection while weighing the need for disclosure in the employment context. In addition, the identified moderate effect of *privacy as a right* on concerns for *unauthorized secondary use* are also consistent with our finding in the mental model study in Chapter 5 that the right to privacy in employment is strongly associated with the notion of "self-determination". This shows the need for establishing solutions in employment that reduce the complexity of privacy protection, thus strengthening the culture of trust and reducing privacy concerns. In this regard, it should be noted that our participants'

perceived satisfaction with the privacy law had positive effects on *trust* and negative effects on *privacy concern*. From the employer's point of view, it can therefore also make sense to show employees how the current legal situation contributes to the protection of privacy. Since the employment context in particular allows little intervention, creating awareness and demonstrating accountability could help reduce the feeling of complexity or counteract its effects.

Finally, we found no effect of participants' factual level of knowledge of privacy law on antecedents. In principle, participants' knowledge of privacy law was rather low. Although our results indicate that data processing employees and Germans performed slightly better, fewer than one third of them knew all answers correctly. In particular, this level of knowledge seems to be low among those involved in the processing of personal data, as they should be familiar with the rules in the course of their activities. In principle, however, this result is consistent with the findings of our mental model study in Chapter 5, showing that knowledge of privacy-related rules and aspects of personal data processing was often superficial.

## 6.6 DIFFERENCES IN EMPLOYEES' PERCEPTIONS OF PERSONAL DATA

After having examined differences between groups of personal data and antecedents, we now focus on differences between employees in their perceptions of sensitivity and willingness to disclose. For this purpose, we report below the results of our analysis targeting **RQ4** "Can employees be categorized based on different perceptions of personal data?" We first present the results of the **LCA** in Section 6.6.1 and then discuss our findings in Section 6.6.2

### 6.6.1 Clusters of employees

To examine **RQ4a** "Can employees be classified into groups according to willingness to disclose and perceived data sensitivity?", we applied **LCA** as described in Section 6.2.6.5. The fit indices of the five repeated **LCA**s are reported in Table 6.11 and indicate that a **three-class solution** was the best model. Because entropy was greater than .8, we fixed the class membership of participants and assigned them to clusters. 85% of participants were assigned to one of these groups with a probability of  $\geq 90\%$ .

To test whether the clusters actually differed in terms of *perceived data sensitivity* and *willingness to disclose*, we compared a restricted **SEM** with an unrestricted **SEM**. The com-

Table 6.11: Comparison of the fit of different solutions for Latent Class Analysis (**LCA**).

Number of classes	Log-likelihood	BIC	cAIC	Entropy
2	-6493.71	13638.57	13747.57	0.86
3	-6285.16	<b>13550.03</b>	<b>13714.03</b>	0.87
4	-6141.01	13590.29	13809.29	0.91
5	-6030.94	13698.71	13972.71	0.91

Note. BIC: Bayesian Information Criterion, cAIC: Consistent Akaike Information Criterion



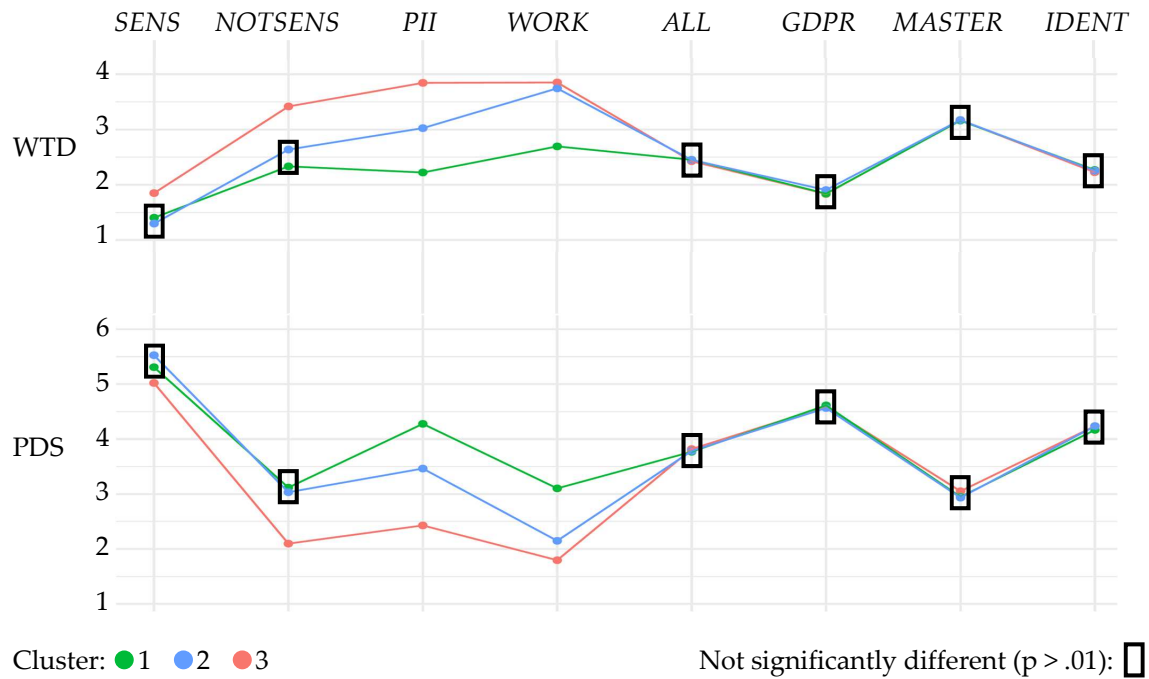


Figure 6.10: Employee clusters differences in Willingness to Disclose (WTD) and Perceived Data Sensitivity (PDS) (composite scores) for various groups of personal data. Clusters were identified using LCA on latent groups of personal data ( $N_1 = 74$ ,  $N_2 = 174$ ,  $N_3 = 145$ ). Significant differences were found only for latent groups of personal data.

parison revealed that the model fit decreased significantly ( $\Delta(\chi^2) = 946.03$ ,  $p < .001$ ), indicating that the three clusters were indeed **significantly different**. An overview of the clusters for different groups of personal data is provided in Figure 6.10. Visual inspection of scores for *willingness to disclose* reveals a **low-medium-high cluster structure**:

▷ **Low-WTD-cluster**

Cluster 1 is the smallest ( $N = 74$ ) and represents participants with **overall low willingness to disclose** and **high perceived data sensitivity** across all latent groups of personal data. Tukey post-hoc analysis revealed that  $WTD_{PII}$  and  $WTD_{NOTSENS}$  did not differ significantly ( $p = .72$ ). Similarly, we did not find significant differences for  $PDS_{NOTSENS}$  nor for  $PDS_{WORK}$  ( $p = .99$ ). In conclusion, it seems that employees in this cluster only distinguished between **three levels** of *perceived data sensitivity* and *willingness to disclose*.

▷ **Mid-WTD-cluster**

Cluster 2 is the largest ( $N = 174$ ) and represents participants whose *willingness to disclose* follows the anticipated order among the latent data groups based on **contextual relevance and sphere** (cf. Section 6.4.3). Tukey post-hoc analysis revealed significant differences between **all latent groups**, i.e., between  $WTD_{SENS}$ ,  $WTD_{NOTSENS}$ ,  $WTD_{PII}$ , and  $WTD_{WORK}$ , as well as between  $PDS_{SENS}$ ,  $PDS_{NOTSENS}$ ,  $PDS_{PII}$ , and  $PDS_{WORK}$  ( $p < .001$ ).

▷ **High-WTD-cluster**

Cluster 3 ( $N = 145$ ) represents participants with **overall high willingness to disclose**. Tukey post-hoc analysis revealed that scores for *willingness to disclose* and



*perceived data sensitivity* did not differ significantly for *NOTSENS* and *PII* ( $p = .11$ ). However, while  $WTD_{NOTSENS}$  was significantly lower than  $WTD_{WORK}$  ( $p < .001$ ), *perceived data sensitivity* did not differ significantly ( $p = .16$ ). This effect was reversed for *PII*, for which  $WTD_{PII}$  and  $WTD_{WORK}$  did not differ significantly ( $p = .99$ ), whereas  $PDS_{PII}$  was higher than  $PDS_{WORK}$  ( $p < .001$ ). Employees in this cluster thus seem to only distinguish between **two levels** of *willingness to disclose* and *perceived sensitivity*, namely data that are sensitive and must be retained, and data that are insensitive and can be disclosed.

Furthermore, when comparing differences between clusters, we find that all clusters differed significantly in *perceived sensitivity* and *willingness to disclose* for the groups *PII* and *WORK*. However, cluster 1 and cluster 2 did not significantly differ for the data groups *SENS* and *NOTSENS* (cf. Figure 6.10). There were also no significant differences between clusters for the non-latent data groups.

Likewise, our investigation of demographic differences under sub-research question **RQ4b** “Do these groups differ in terms of demographic factors or privacy attitudes?” revealed that all analysis for demographics returned insignificant results. Although the *MIMIC SEM* model showed adequate model fit ( $\chi^2(189) = 297.84$ ,  $p < .001$ ,  $CFI = .99$ ,  $GFI = .99$ ,  $RMSEA = .04$ ), **none** of the regressions were **significant** and estimates were well below  $|0.05|$ . The logistic regressions on participant demographics did **not** return **significant** results either. In summary, this means that we found **no evidence** that participants’ demographic characteristics and attitudes toward privacy differed by cluster with respect to the antecedents studied.

### 6.6.2 Discussion

In this section, we examined differences between employees’ perceptions of data, aiming at the identification of more homogenous groups of employees in terms of *willingness to disclose* and *perceived data sensitivity*. Regarding **RQ4a** “Can employees be classified into groups according to willingness to disclose and perceived data sensitivity?”, our results show that employees can indeed be clustered accordingly. However, regarding **RQ4b** “Do these groups differ in terms of demographic factors or privacy attitudes?”, neither privacy beliefs nor demographic background could predict cluster membership. As a result, the differences appear to be explained solely by employees’ perceptions of the four latent data groups.

Furthermore, we find that the clusters differ in two dimensions. The first dimension is the division according to employees’ general willingness to disclose personal data and their perceived data sensitivity into the three levels low, medium, and high. The second dimension is the number of different levels between which a distinction is made. Accordingly, employees in Cluster 1 differentiated between three levels, employees in Cluster 2 between four levels, and employees in Cluster 3 between only two levels. Still, all clusters agreed that highly sensitive personal data represented by the *SENS* data group are generally different from personal data represented by other data groups. For Cluster 3, we also found no differences between *NOTSENS*, *PII*, and *WORK*. In contrast, the difference between Cluster 1 and Cluster 2 is that contextual relevance does not seem to affect *willingness to disclose* to the same extent. Especially, individuals in Cluster 1 seem to prefer disclosing personal data only when absolutely necessary. Due to non-significant effects of the control variables, we cannot determine influencing factors to explain this

observation. However, in terms of the mental model of Privacy Doctrinaires (PDs), or in terms of the persona of *privacy fundamentalists* from online privacy research [283, 287], these might simply represent employees who have a high fundamental need for privacy.

Moreover, the distinction between different levels can vary between *willingness to disclose* and *perceived data sensitivity*, i.e., these perceptions do not seem to be mutually linked. For example, in Cluster 1, no significant differences were found between  $WTD_{NOTSENS}$  and  $WTD_{PII}$ , but significant differences were found between  $PDS_{NOTSENS}$  and  $PDS_{PII}$ . Instead, we found no evidence that  $PDS_{NOTSENS}$  and  $PDS_{WORK}$  are on the same level, but we found evidence for differences between  $WTD_{NOTSENS}$  and  $WTD_{WORK}$ . This again highlights that employees' willingness to disclose personal data seems more likely to be related to contextual relevance, while perceived data sensitivity is more likely to be related to spheres and boundaries. This would also explain why  $WTD_{PII}$  is higher than or close to both  $WTD_{WORK}$  and  $WTD_{NOTSENS}$  in all clusters, whereas  $PDS_{PII}$  is also higher than both  $PDS_{WORK}$  and  $PDS_{NOTSENS}$ . If context was the strongest driving factor,  $PDS_{PII}$  should have been lower than  $PDS_{NOTSENS}$ .

## 6.7 IMPLICATIONS

Privacy engineering requires comprehensive conceptual understanding of personal data and influencing factors, especially to identify risks and threats in the context of *risk management* and to make reasonable decisions in the context of the *architecture definition* process to implement effective privacy controls [9, 12, 15, 16, 143]. This study examined numerous aspects to provide just that needed conceptual understanding.

Under **RQ2** “How do personal data differ in terms of their perceived sensitivity and willingness to disclose by employees?” we investigated whether groups of personal data can be identified based on employees' perceived sensitivity and willingness to disclose personal data, and how these variables differ among these groups. We also analyzed whether perceived data sensitivity differs between the employment and other contexts. We find that the employment context differs significantly from other contexts, with a dramatic increase in perceived data sensitivity of many data relative to other contexts, and vice versa. We also successfully identified a meaningful set of four latent groups of personal data that captures the subtleties of employee' perceived sensitivity and willingness to disclose personal data specific to the employment context.

As part of **RQ3** “Which antecedents influence employees' perception of personal data?”, we examined the impact of several antecedents commonly studied in the privacy literature on *perceived data sensitivity* and *willingness to disclose*. At least for the industries studied, our findings show that overall risk perceptions are low and overall trust is high. Both factors, however, appeared to have little or no effect on willingness to disclose nor on perceived data sensitivity. Instead, depending on the type of data, antecedents differed between trust and concerns, whereas perceived sensitivity seems to be primarily influenced by concerns. Especially for latent groups of personal data, neither antecedents nor demographics had notable effects. In contrast, we found that employees' dispositions toward privacy protection can have a significant impact on trust and privacy concerns.

Under **RQ4** “Can employees be categorized based on different perceptions of personal data?”, we clustered employees into groups according to their willingness to disclose and examined the clusters for differences in demographics and privacy attitudes. We identified three clusters that capture various attitudes toward perceived sensitivity and willingness

to disclose. Unlike similar approaches in online privacy research [251], however, clusters are not associated with any of the surveyed demographics or privacy beliefs. In parallel, the clusters do not differ for non-latent groups of personal data.

In the following, we discuss the results in terms of their theoretical and practical implications for employee privacy.

#### 6.7.1 *Consideration of contextual factors*

We provide empirical evidence that the employment context requires special consideration. In particular, our analysis shows that drastic changes in contexts, i.e., from online and marketing contexts to employment context, outweigh even cultural differences in perceived data sensitivity between online and marketing contexts. This stresses the importance of developing explicit knowledge repositories for employee privacy and not to adopt knowledge from other contexts to privacy engineering or privacy research for employee privacy. Such an approach seems to be acceptable only for minor context changes, e.g., from online to marketing contexts.

Moreover, our results generally support findings from previous studies that examined contextual differences for willingness to disclose [248, 252, 253]. However, our results strongly suggest that the context affected perceived sensitivity and willingness to disclose differently, or its effect was obscured by other (maybe unknown) factors. For one thing, this is supported by the observed low willingness to disclose personal data perceived as particularly insensitive. Our findings suggest that willingness to disclose appears to be more strongly influenced by the data's contextual relevance, whereas perceived data sensitivity appears to be more strongly influenced by the data's affiliation to a specific sphere. One explanation is that perceptions of personal data are influenced not only by general privacy attitudes [247], but also by specific attitudes and norms with varying effects in different contexts. This means that the spheres or boundaries in which individuals locate their personal data are not constant, but vary according to the broader context. The joint consideration of contextual relevance and sphere in the employment context thus seems to be a suitable method for classifying personal data in a manner that reflects the perceptions of employees.

#### 6.7.2 *Classification of personal data*

Our results show that a dichotomous distinction between "sensitive data" and "non-sensitive data", as is common in privacy research [246, 255] and international standards or laws, seems to be generally viable in the employment context. Consequently, our study suggests that legal and international standards' definitions of what constitutes sensitive personal data may serve as broad guidelines for employers to distinguish between dichotomous levels of sensitivity. However, our cluster analysis showed that perceived sensitivity and willingness to disclose may differ substantially for some data but not at all for others. Strictly dichotomous views cannot capture such subtleties. Therefore, considering the multidimensionality of personal data is clearly preferable, especially for the studying of individuals' privacy preferences [66, 251, 278]. The latent groups of data identified in this study may serve as a sound basis for future examinations. Moreover, the definitions provided by law and standards may not necessarily reflect the data that employees consider to be the most sensitive. Recent studies in the online context re-

vealed similar issues with legal definitions [272]. Similar to approaches where employee expertise was used to create meaningful IT security policies for corporate assets [341], we argue that for employee privacy protection, employee sentiments and needs should be incorporated into the classification of personal data. Based on our findings, a distinction based on “private” data may better reflect the perceptions of both consumers [276], but also employees (cf. Study I in Chapter 5).

Furthermore, our cluster analysis shows that a noticeable group of employees is unwilling to disclose truthful personal data, even if the data are highly relevant to the employment context. Employers should be aware that data which are critical to the employment relationship may be perceived as sensitive. However, this view does not seem to be shared equally by all employees. For example, two thirds of our sample perceived *PII* as significantly more sensitive and were less likely to share compared to *WORK*, whereas one third made no difference between these two groups of personal data.

### 6.7.3 Implementation of privacy controls

Our findings support assumptions derived from Study I in Chapter 5 that employees in Germany generally trust their employers with the processing of their personal data. At the same time, we found strong convictions that employees expect to have a fundamental right to privacy. Employees with strong beliefs are also fairly concerned about collection and unauthorized secondary use. Likewise, employees’ perceived complexity of privacy protection negatively affects trust in employers and positively affects privacy concerns. Thus, there is an interest not only from a legal and ethical perspective in reducing perceived complexity and supporting employees in their ability to act, but also from the employer’s perspective in strengthening the culture of trust and reducing concerns. Since satisfaction with the effectiveness of current law seems to have a positive impact on trust and a negative effect on privacy concerns, employers should demonstrate the extent to which current policies and regulations have already been implemented and contribute to the protection of privacy. It could also help to train employees about their rights as well as about the obligations of employers, as the factual knowledge in our study was rather low. Especially employees who process personal data themselves should be supported in their role as executives of the employer to comply with the legal framework despite gaps in their knowledge.

Our results further provide insights for the development of tools that facilitate the exercise of employee data subject rights, in particular, with regard to transparency. Assuming that data with high perceived sensitivity or low willingness to disclose are associated with higher information needs, different levels of detail can be provided for different types of personal data. This might help address the challenge that employees desire comprehensive information on the one hand, but find exercising their rights complex on the other. Thus, the need for information would likely be lowest for data under *WORK* and highest for data under *SENS*. No clear ranking is possible for *PII* and *NOT-SENS*, since contextual relevance and sphere belonging have to be taken into account. In addition, the identified clusters of employees suggest that a “one-size-fits-all” solution may not be a satisfactory solution. Instead, tools should allow for personalization. However, because we did not find any differences in demographic characteristics or attitudes toward privacy between the clusters, future work is needed to examine what types of employees would prefer different forms of transparency and/ or intervention.

#### 6.7.4 Studying employee privacy perceptions

Regarding the studying of employees' privacy perceptions, our results have several implications. First, our findings suggest that the magnitude between *perceived data sensitivity* and *willingness to disclose* is largely stable across different groups of personal data. Instead of treating individuals' perceived sensitivity mostly as an indirect driver of their willingness to disclose [247], its direct effects are also apparent and should be considered. This relationship seems particularly well suited to identifying pitfalls, where the consideration of contextual relevance and sphere is important to detect. It further helps to understand seemingly unrelated changes in either willingness to disclose or perceived data sensitivity. This also implies that examining perceived sensitivity or willingness to disclose in isolation could lead to incorrect conclusions about the specific construct not considered in a study.

Moreover, the studying of antecedents revealed that we hardly found effects for non-latent groups of personal data identified in factor analysis. Since these groups are considerably more heterogeneous than the latent data groups, our results suggest that frequently observed effects of antecedents [247, 262] disappear for smaller and more homogeneous sets of personal data. This stresses the importance to make the type of personal data explicit in privacy research [246]. For example, previous studies using the *IUIPC* and *CFIP* privacy scales in the employment context have indeed found significant effects of *trust* and *risk beliefs* on *behavioral intentions* [73]. However, they did not explicitly indicate any personal data. Therefore, their results could be attributed to the imprecise questions of the scales and are thus subject to interpretation by the employees. In our own study, we also assessed *trust* in a non-specific way. At the same time, we found significant small effects of *trust* on *WTD<sub>ALL</sub>* and *WTD<sub>GDPR</sub>*. This outcome could be attributed to the fact that the groups *ALL* and *GDPR* reflect specific types of personal data that are salient to employees when being asked general questions about privacy. This means that employees may have intuitively thought about data items contained in these groups when responding. Precise questions about *trust* in handling specific data might have yielded different results. Besides, although we did not find significant strong effects of *trust* on *willingness to disclose*, it constitutes an essential factor in the relationship between employer and employee [4]. Thus, both employers and researchers should not take our results as a reason to abandon investigating trust-building measures.

Furthermore, the noted problems of reliability for some constructs adopted from related work may indicate an inappropriate measurement instrument for the employment context in Germany. Based on our findings, we thus recommend that future studies, particularly those in non-English speaking countries, should exercise caution in applying the same measurements and assumptions to employment that have been used in previous research [255, 338]. Also, because recent work revealed validation problems for such scales, even when used in the original (online) context and with native English speakers [342]. Our results may serve other researchers to avoid some of these pitfalls.

### 6.8 STUDY LIMITATIONS

This study took place during the COVID-19 pandemic, such that potential bias in our results due to a larger number of employees working from home during this time cannot be ruled out. However, effects, if any, are likely to be small, as very few data types would



be affected (e.g., IP address). Moreover, sampling is likely affected by a self-selection bias, and limited to the population of employees registered with the panels and employed at the organizations we contacted for recruitment. Nevertheless, our sample incorporates employees with sufficiently different privacy beliefs and perceptions.

In addition, we acknowledge the justified criticism of the privacy macro-model used and the measurement of intent by willingness to disclose [264]. However, given that disclosure of some categories of personal data is indispensable in the employment context, the focus on finding inconsistencies (i.e., a paradox) may also require a different interpretation. Our findings may therefore reveal employees' desire for privacy rather than actual behavior. We point out that, unlike in research on online privacy behavior, it is likely impossible to measure actual disclosure behavior in a cross-sectional study in the employment context [343]. Since we have already found in Study I in Chapter 5 that employees have limited and flawed knowledge about what personal data are processed by employers, research on this aspect cannot rely on self-reported information.

Furthermore, the survey of privacy antecedents was framed in terms of general beliefs about employers. Participants might have responded differently if questions had been asked for specific types of personal data. The latent data groups identified in this study could form the basis for future research to examine any differences.

## 6.9 SUMMARY

In this chapter, we have presented the results of a cross-sectional survey with 553 employees from Germany to gain insight into perceived sensitivity and willingness to disclose personal data in the employment context. According to our literature review in Chapter 3, this study complements the results of Study I in Chapter 5 by providing the first thorough conceptualization of employees' perceptions of personal data under contemporary and Eurocentric views of privacy.

Regarding **RQ2** *"How do personal data differ in terms of their perceived sensitivity and willingness to disclose by employees?"*, we revealed differences in perceived data sensitivity between employment and online/ marketing contexts, as well as that concepts of personal data from law and international standards do not reflect the subtleties of employees' perceptions. Consequently, activities that rely on sound conceptualizations of personal data, e.g., in risk assessment (cf. Section 2.3), must draw on employment specific contextual knowledge. To this end, we provide four empirically derived groups of personal data that help to understand the relationship between perceived data sensitivity and willingness to disclose, as well as the dependence on contextual relevance and boundaries. In this regard, our results under **RQ3** *"Which antecedents influence employees' perception of personal data?"* yielded mixed results; we found that employees trust their employers, yet have high expectations of self-determination and of privacy as a fundamental right, while factual knowledge about privacy law was moderate to low, even for data processing employees. However, none of these factors seem to affect employees' perceptions of personal data. Furthermore, under **RQ4** *"Can employees be categorized based on different perceptions of personal data?"*, we provide empirical evidence that groups of employees can be formed with different levels and conceptualizations of perceived data sensitivity and willingness to disclose. Consequently, the "uniqueness of privacy perceptions among individuals" (cf. Section 2.1) must be taken into account in both research and engineering activities on employee privacy, e.g., in the elicitation of *stakeholder needs*

*and requirements* or in *architecture definition* (cf. Section 2.3.2). The results also give rise to follow-up studies, as demographic differences were not found.

Overall, this study contributes to the fundamental knowledge of employee privacy by providing in-depth empirical insights into how employees conceptualize and perceive personal data. The knowledge gathered completes and empirically confirms key findings from Chapter 5. This results in a solid knowledge base for approaches in usable privacy and privacy engineering under contemporary and Eurocentric views of employee privacy (cf. Section 4.1). Thus, we address one of the objectives of this dissertation as outlined in Section 1.2. The findings provide a basis for creating employee-centric privacy controls and privacy-friendly systems that effectively protect employees' freedom and rights. To the extent applicable, this also relates to findings on data processing employees, which we address in the forthcoming Chapter 7.



## STUDY III — DATA CART: A PRIVACY PATTERN FOR THE GDPR-COMPLIANT HANDLING OF EMPLOYEE PERSONAL DATA

---

*Data protection and privacy must not  
be a mystery, especially to employees at  
the operational forefront of organisations.*

— Kevin Shepherdson

Chapter 5 and Chapter 6 have focused on eliciting employees' conceptualizations of privacy in their role as data subjects, which provides fundamental knowledge for implementing employee-centric privacy controls and privacy-friendly systems. This chapter shifts the focus away from employees in their role as data subjects and turns attention to data processing employees who process employees' personal data and therefore occupy a key role in safeguarding employee privacy. Based on [103], this chapter reports the results of a UCD study with 19 data processing employees from two large public institutions in Germany, to investigate how TOMs must be designed to support this stakeholder group in the privacy-preserving processing of employee personal data under RQ5.

The rest of this chapter is structured as follows: We present the study's background and research model in Section 7.1. Next, we provide details on our methodology, ethical consideration, and study setup in Section 7.2. Afterwards, we present the requirements elicited for the user-centered development of TOMs in Section 7.3, and then present our proposed solution *Data Cart* in Section 7.4. This is followed by details on the implementation of a prototype in Section 7.5, which we used to evaluate our proposed solution. The results of our evaluation are presented in Section 7.6 and Section 7.7, respectively. We then discuss our evaluation results and the proposed solution in Section 7.8, followed by a discussion of our study's limitations in Section 7.9. We finally conclude this chapter, summarizing our findings in Section 7.10.

### 7.1 BACKGROUND AND RESEARCH MODEL

Employees who process personal data as part of their job have always played an important role in putting privacy goals into practice. In this regard, industry reports indicate that up to 90% of all data breaches are caused by some form of human error [344]. Particular problems are both the accidental processing of data without permission and the forwarding of data to the wrong recipients. For example, this is reportedly true for 39% of incidents in the U.S. in 2019 [345] and for two-thirds of incidents in the Netherlands in 2020 [346].<sup>1</sup> Reasons include negligence of employees [347], high stress levels at work, and overlaid communication channels (e.g., email) [348]. Half of the incidents resulted in disciplinary or other professional consequences for the employees [349]. The GDPR has therefore increased the pressure on organizations and their employees to comply

<sup>1</sup> Please note that although controllers are obligated to report personal data breaches to the supervisory authority under Art. 33 GDPR, in Germany, no statistics are published on this topic.

with the regulation's strict rules. However, our own findings on employees' conceptualizations of privacy in Study I in Chapter 5 and Study II in Chapter 6 highlight that data processing employees are not fully familiar with the essential terminology, concepts, and basic rules of data protection law, which increases the risk of noncompliance.

It follows that from a socio-technical perspective, but especially from a usable privacy perspective, the mere implementation of TOMs without taking into account the needs and capabilities of data processing employees is likely to render TOMs ineffective and even harmful to the organization because data processing employees may lack understanding and commit errors, or because TOMs impose a burden for established business routines and increase the workload (cf. Section 4.2). Since the protection of employee privacy depends largely on the effectiveness of TOMs, and since employees also expect enforcement (cf. Chapter 5), we follow the notion that the design of privacy controls must involve the stakeholders who own the particular privacy subtask [98]. For the studying of RQ5 *"How can data processing employees be effectively, efficiently, and satisfactorily supported in the data protection compliant processing of employee personal data?"*, we therefore derive the following sub-research question:

**RQ5<sub>a</sub>** *"What are the needs and requirements of data processing employees for usable privacy controls for the management and processing of employee personal data?"*

Instead of looking at perceptions of already established PETs for processing customer data [19, 270], we advocate a bottom-up approach, where stakeholder requirements and perceptions are explored and considered from the outset. Building up on the principles of PbD (cf. Section 2.3.1), we therefore apply an UCD approach that has already proven useful with managers [98] and employees in their role as data subjects [97]. It is also considered most effective in addressing human factors in systems engineering of socio-technical systems [350]. In this regard, we supplement RQ5 with the following sub-research question:

**RQ5<sub>b</sub>** *"How are TOMs developed under UCD and according to PbD perceived by data processing employees?"*

## 7.2 METHODOLOGY

To investigate our research questions, we conducted a UCD study with 19 data processing employees from two large German institutions (Org. A, Org. B). The research was conducted as part of the large-scale research project *"TrUSD - Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen"* that aimed at developing a framework for GDPR-compliant employee data protection. The project consortium included experts from the fields of law, ergonomics, requirements engineering, IT security, and HCI. The UCD study took place over the course of the project, from 2019 to 2021. In the remainder of this section, we discuss how we addressed ethical considerations in Section 7.2.1, provide details on the study procedure in Section 7.2.2, followed by details on participant recruitment in Section 7.2.3 and participant demographics in Section 7.2.4, concluding with details on data evaluation and analysis in Section 7.2.5.

### 7.2.1 *Ethical considerations of the study*

We took care to minimize potential harm from our study to both our study participants and the participating organizations. We followed the Code of Ethics of the German Sociological Association and the standards of good scientific practice of the German Research Foundation. Furthermore, all study designs were reviewed and approved by the respective DPOs of our participants' organizations and our own institutions. We therefore feel confident that our studies comply with the strict national and EU privacy regulations.

To reduce potential harm, we collected data anonymously when possible (e.g., questionnaires). When not possible (e.g., video and audio recordings), we pseudonymized or anonymized the data for evaluation by removing all direct personal identifiers and organizational information from the transcribed focus group sessions and interviews. The raw material was stored encrypted, to which only a small group of researchers had access. The cleaned transcripts were stored access protected and were provided to our research fellows in the research project if required for analysis. Any contact information of the participants was stored separately.

We only invited employees from the same division to focus groups, to avoid participants disclosing details about internal business processes to externals other than the researchers. When inviting employees to participate in our studies, we highlighted that participation was voluntary and provided consent forms for review prior to the studies. We stressed that aborting a study would have no negative consequences, and we assured that the studies' contents would not be reported back to employers or management.

### 7.2.2 *Study procedure*

To design TOMs that adhere to the principles of PbD, designers and developers need a deep understanding of (1) the situation and context *in which* the TOMs will be used, as well as of (2) the personal data processing activities *for which* the TOMs will be used [351]. To incorporate these aspects early in the design process, we applied a three-step procedure [200] that allowed us to involve our participants (i.e., the target users) early in the design process. The procedure is outlined in Figure 7.1.

For the most part, we relied on focus groups because we expected our participants to enrich each other [303], but we also used interviews because both methods are well suited for both requirements elicitation and evaluation [352]. We either adapted existing workshop concepts to our needs or created our own study protocol in accordance with established guidelines. All study protocols were designed and reviewed by two subject-matter experts, as well as researchers from the research project team, and researchers with experience conducting user studies. Depending on the type of study, we piloted studies with members of our own institutions or other organizations. To comply with the strict rules of the COVID-19 pandemic, studies after 2019 were conducted online. Participants in all studies were informed about the study's contents and purposes, and they were asked to provide informed consent. In the following, we provide an overview of the different studies conducted.

**STUDY 1 – FAMILIARIZATION** We started familiarizing ourselves with the stakeholder group and its daily work by conducting a workshop and an inventory of essential work processes. The workshop was based on the concept of Polst et al. [96]. In the work-

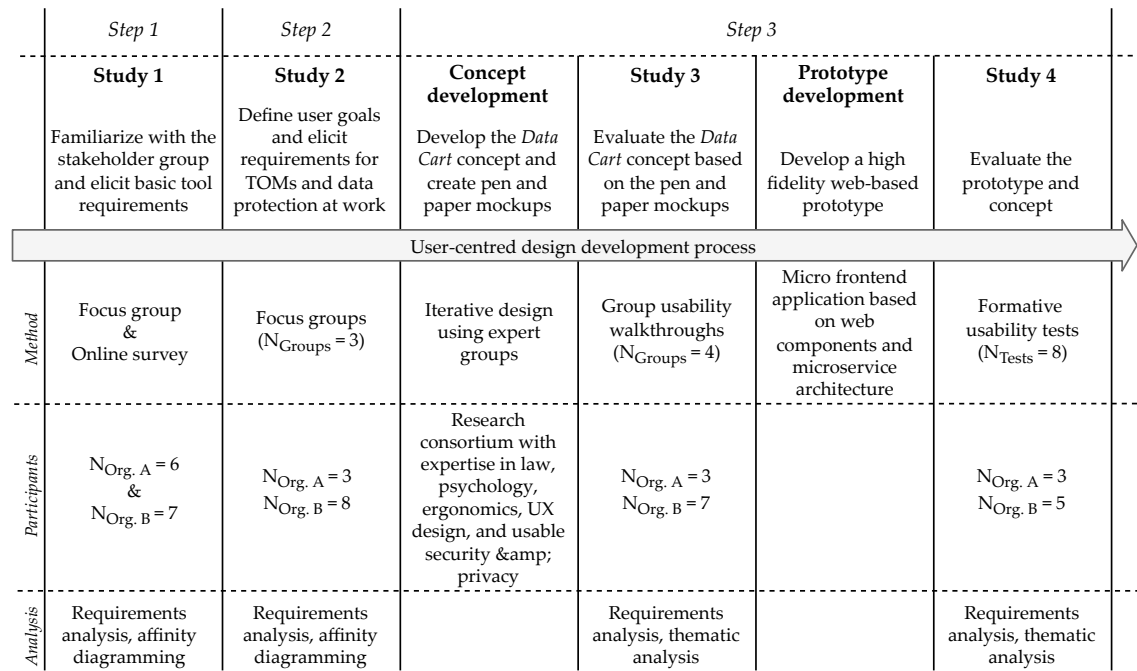


Figure 7.1: User-centered design approach and development process.

shop, we asked participants to describe their job role, work responsibilities, and data handling practices. We then asked about their basic goals with regard to data protection, previous experiences with the introduction of new technologies in the workplace, and which stakeholders were involved in the process. Participants also explained what would characterize a successful implementation of TOMs. All responses were recorded on moderation cards to be collected on a pinboard for group discussion. Participants were also asked to prioritize the most critical processes and requirements. The workshop was conducted with employees from Org. A and lasted two hours (N<sub>Org. A</sub> = 6). The requirements and task profiles of Org. B were gathered using an online survey for logistical reasons (N<sub>Org. B</sub> = 7).

Furthermore, we conducted a detailed survey of the departments' workflows and processes. We received detailed listings of the workflows, access to the internal process documentation tool, copies of the processing directory, and essential forms. We documented the processes by dividing them into use cases and capturing them in Business Process Model and Notation diagrams. We also had the opportunity to visit the workstations and premises of the two organizations.

**STUDY 2 – SPECIFICATION OF USER GOALS** We conducted a second study to sharpen our understanding of our stakeholders' specific goals and their expectations for improvements in the handling of personal data. The study brought together data protection issues with our participants' professional activities and focused on three key aspects that emerged from the previous survey of processes: (1) Obtaining missing data; (2) obtaining permission for data use; and (3) sharing data with third parties. In the study, we asked about helpful and obstructive aspects in the processing of personal data and then presented two data processing scenarios, which our participants were asked to design according to their own ideas regarding relevant information, instructions, and procedures. All answers were again noted on moderation cards, sorted by topics, and

discussed in the group. Participants then rated each topic's importance. We conducted three workshops ( $N_{\text{Org. A}} = 3$ ,  $N_{\text{Org. B}} = 8$ ), each lasting two hours. The workshop's outline is provided in Appendix D.1.

**CONCEPT DEVELOPMENT** Based on the requirements gathered in Study 1 and Study 2, as well as considering identified problems in the mental models study in Chapter 5 regarding understanding and awareness of data protection concepts, we developed a concept that would bring together user requirements and legal requirements for the data protection compliant handling of employee personal data. To make the concept tangible, we developed pen and paper mockups that depicted the basic flow and key requirements. We reviewed the concept and requirements in a series of expert group discussions involving individuals from our research projects with expertise in requirements engineering, UX design, and usable security and privacy.

**STUDY 3 – CONCEPT EVALUATION** To evaluate the concept with our stakeholder group, we conducted a third study by adapting the method of a group usability walkthrough [353]. We chose this approach because it allows obtaining rich feedback on both the flow of a system and its usability based on group discussions. Participants attended the study from their usual workstations and with their own (work) computers and the browsers of their choice. In the study, the participants were first introduced to the concept by explaining related key aspects of data protection law and personal data processing. We then presented our participants a scenario from their everyday working lives, in which they had to process personal data of other employees. We asked our participants to work through the scenario using the concept. To this end, we provided initial pen and paper mockups in an online survey that allowed participants to navigate through the different screens and take notes. Specifically, we asked them to document what actions they would take on each screen to complete the scenario. Afterwards, we went through all the screens and discussed the usefulness of the features provided, missing features, and additional topics that came up in group discussions. Participants then rated the concept using the System Usability Scale (SUS). We conducted four walkthroughs ( $N_{\text{Org. A}} = 3$ ,  $N_{\text{Org. B}} = 7$ ), each lasting two hours. The study's outline is provided in Appendix D.2.

**PROTOTYPE DEVELOPMENT** We revised the concept based on the obtained feedback and discussed the changes with the same group of experts as before. We then developed a high-fidelity prototype using web technologies to evaluate the concept, running formative usability tests [354]. For the design, we also considered the assumed unfamiliarity of our participants with the data protection framework and terminology, as found in Study I in Chapter 5 and confirmed in Study II in Chapter 6.

**STUDY 4 – PROTOTYPE EVALUATION** In the usability studies, participants role-played a fictitious data processing employee with a job profile similar to their own, working at a fictitious public organization. We explained that this organization uses a tool to assist in the processing of personal data. We then asked our participants to use the prototype to work through a scenario in which they had to organize a training session on patent law and process an invention disclosure. The scenario was broken down into several sub-tasks. Among others, these tasks included requesting (missing) data from several different data subjects, obtaining consent, exporting data, forwarding data, and

progress tracking. During the scenario, participants had to ensure that data were handled in accordance with data protection regulations and were also asked questions on the correct handling of data.

To design a realistic and immersive study experience, we modeled the scenario and materials (e.g., invention disclosure) based on the actual process diagrams, workflows, and original documents provided to us in Study 1 and Study 2. In addition, participants attended the study from their usual workstations and with their own (work) computers and the browsers of their choice. Throughout the study, participants were asked to share their screen and think aloud. We made sure that participants limited screen sharing to the prototype so as not to record other content. After completing the scenario, participants answered an SUS questionnaire. We then conducted post-interviews in which we asked participants how they felt about the role-play, how they perceived the handling and processing of (personal) data, what changes they would expect for their daily work if the tool was actually available to them, and what they liked or disliked about the tool. We conducted eight studies ( $N_{\text{Org. A}} = 3$ ,  $N_{\text{Org. B}} = 5$ ), lasting between 75 and 125 minutes. The study material is provided in Appendix D.3.

### 7.2.3 Participant recruitment and enrollment

After contacting several organizations prior to the project and asking for their support, the departments of two organizations (Org. A, Org. B) agreed to participate in our research. These departments dealt with third-party funding, patents, and the management of research projects. In order to obtain approval for our study, we disclosed detailed information about the project and its scope to the organizations' management, legal departments, and DPOs. Upon successful approval, the departments provided us with contact information for employees who volunteered to participate in our research. They further designated a contact person with whom we coordinated our research to limit the extent of disruption to their workflows. We informed interested employees about the project via email and provided information about the project and planned studies on websites and in videos. Employees could then register individually for the study dates. Despite early scheduling and coordination with departments, we were not able to recruit the same employees for all studies.

### 7.2.4 Participant demographics

A total of 19 employees participated in our studies ( $N_{\text{Org. A}} = 11$ ,  $N_{\text{Org. B}} = 8$ ). Their basic demographics are summarized in Table 7.1. A summary of their job profiles and responsibilities is summarized in Figure 7.2. In most cases, they held multiple roles, including research consultant, third-party funding coordinator, team assistant, network manager, and innovation manager. Their tasks included consulting and coaching activities, guiding and supporting grant applications or patent approvals, and monitoring ongoing projects or start-ups. In these activities, they primarily process personal data of the institutions' employees. The data typically include personnel data, contact data, and demographic data, but also classified information (e.g., patents) (cf. Figure 7.2). Other tasks include public relations and marketing as well as networking, which includes the regular planning and hosting of events. These activities require extensive processing of private and professional contact data, as well as image recordings.






 <b>Job profiles</b> <ul style="list-style-type: none"> <li>• Research Officers</li> <li>• Funding Coordinators</li> <li>• Innovation Managers</li> <li>• Legal Officers</li> <li>• Network Managers</li> <li>• Team Assistants</li> </ul>	 <b>(Personal) data processed</b> <ul style="list-style-type: none"> <li>• Account information</li> <li>• Affiliation</li> <li>• Classified data (e.g., business plans, patents)</li> <li>• Contact information (private and business, e.g. name, first name, title, address, phone number, email)</li> <li>• Date of birth</li> <li>• Education</li> <li>• Employment (primary and secondary)</li> <li>• Income</li> <li>• Information about clients and project partners</li> <li>• Personnel data</li> <li>• Resumes</li> <li>• Photos (of individuals)</li> <li>• Research activities</li> <li>• Sex, gender</li> </ul>
 <b>Job tasks</b> <ul style="list-style-type: none"> <li>• Management of research projects and commercial projects</li> <li>• Patent registration and exploitation</li> <li>• Start-up service</li> <li>• Consulting and coaching</li> <li>• Monitoring activities</li> <li>• Academic services</li> <li>• Event management</li> </ul>	

Figure 7.2: Summary stakeholder job profiles, job tasks, and (personal) data processed.

In all of these activities, the stakeholders regularly collaborate and communicate with their colleagues and other departments, or with external organizations such as project sponsors and funding agencies. Particularly often, they contact the [HR](#) department to request personal data instead of obtaining them directly from the data subjects. Moreover, most of their tasks require them to share (personal) data with others or to use the data to generate statistics and reports. Thirteen participants self-reported processing personal data very frequently or regularly, while six participants reported processing such data occasionally. All participants had an academic degree and had been in their job and with the organization for between one and 19 years (median = 3 years, mean = 5.4 years).

### 7.2.5 Evaluation and data analysis

All data from the various focus groups and the usability evaluation were analyzed by two researchers. For the analysis of focus groups, we followed best practices for user requirements analysis [203]. In particular, we used affinity diagramming to identify, document, categorize, and prioritize the requirements for tools that our participants discussed. Since we already used affinity diagramming in our workshops to sort our participants responses written on cards, the two researchers could complete these diagrams with extra input extracted from the focus groups' transcripts and the participants' notes. After the two researchers finished discussing the results, requirements were recorded and archived in a structured way.

We additionally used reflexive thematic analysis [355] to evaluate the discussions and interview responses. For this purpose, we segmented all transcribed audio recordings into thematic sections based on our focus group and interview guidelines. In a first step, the two researchers then familiarized themselves individually with the material by going through all the transcripts and, if necessary, also referring back to the audio recordings. In a second step, both researchers coded the material inductively. For the coding, both semantic codes and latent codes were allowed. Each researcher then constructed initial themes from the derived codes, assigned the codes to each theme, and double-checked

Table 7.1: Participant demographics

ID	Sex	Age (years)	Education	Job description	Job tenure (years)
Po1	f	35 - 44	PhD	Research Funding Officer	6 - 10
Po2	f	35 - 44	PhD	Research Promotion Officer	1 - 5
Po3	m	25 - 34	PhD	Research Officer	1 - 5
Po4	f	45 - 55	Master's degree	Research Officer	1 - 5
Po5	f	45 - 55	Master's degree	Research Officer	1 - 5
Po6	f	45 - 55	Master's degree	Research Officer	6 - 10
Po7	f	35 - 44	Master's degree	Research Officer	1 - 5
Po8	f	35 - 44	Master's degree	Network Manager	16- 20
Po9	m	25 - 34	Master's degree	Innovation Manager	1 - 5
P10	f	55 - 65	State exam	Research Officer	16 - 20
P11	f	35 - 44	State exam	Legal Officer	1 - 5
P12	f	25 - 34	Master's degree	Third-party Funding Coordinator	1 - 5
P13	f	35 - 44	Master's degree	Research Officer	6 - 10
P14	f	35 - 44	PhD	Research Officer	1 - 5
P15	f	35 - 44	State exam	Third-party Funding Coordinator	1 - 5
P16	f	45 - 55	Master's degree	Research Officer	1 - 5
P17	f	45 - 55	Master's degree	Research Officer	6 - 10
P18	f	35 - 44	PhD	Research Officer	6 - 10
P19	f	45 - 55	Bachelor's degree	Team Assistant	6 - 10

whether the themes' existence was supported by participants' statements. Subsequently, the two researchers presented their initial themes to each other and discussed them with the help of thematic maps. They organized and reorganized the themes until consensus was reached. This resulted in a set of revised themes that were then given a final name and description.

### 7.3 PRIVACY REQUIREMENTS FOR THE HANDLING OF EMPLOYEE PERSONAL DATA

In this section, we outline the (privacy) requirements elicited for the design of employee-centric privacy controls to address **RQ5a** *“What are the needs and requirements of data processing employees for usable privacy controls for the management and processing of employee personal data?”* For the sake of brevity, and unless otherwise noted, by “privacy controls” we generally refer to privacy enhancing personal data management tools in the context of our stakeholder's job tasks and data processing activities. To this end, we first briefly discuss legal considerations relevant to the job tasks of our stakeholder group in Section 7.3.1. We then present the results of Study 1 and Study 2 of our UCD approach (cf. Figure 7.1), divided into (1) stakeholder needs for personal data processing in Section 7.3.2, (2) stakeholder needs for data protection in Section 7.3.3, and finally, (3) requirements for designing employee-centric privacy controls that facilitate privacy-compliant processing of employee personal data for our stakeholder group in Section 7.3.4.

### 7.3.1 Legal considerations

Since our stakeholder group regularly processes personal data of employees, privacy controls must comply with legal obligations to protect employee privacy (cf. Section 2.2). However, the provisions are worded abstractly and remain vague. This complicates the identification of specific requirements beyond the basic principles of the GDPR to which all processing of personal data is subject (cf. Section 2.2.4 & Section 2.2.5):

- *Lawfulness, fairness, and transparency* means that privacy controls must (help) ensure that **conditions and legal bases are met prior to processing** of employee personal data by data processing employees. Based on a review of the documents and explanations obtained in Study 1 (cf. Section 7.2.2), our stakeholder group's job tasks are generally based on reasons for (1) performance of a contract, (2) compliance with a legal obligation, and (3) legitimate interest purposes. Activities on the basis of consent are limited to some borderline cases, such as the processing of photographs. Moreover, privacy controls must also promote **clear, open, and honest** handling of employee personal data. They must therefore contribute to informing data subjects about the nature and scope of the personal data processing.
- *Purpose limitation* means that privacy controls must ensure that data processing employees process employee personal data only for **specified purposes** to perform a **specific job task**.
- *Data minimization* means that privacy controls must facilitate **limiting data collection** to employee personal data that are absolutely necessary for a purpose associated with the job tasks of data processing employees.
- *Accuracy* means that privacy controls must ensure that data processing employees have access to personal data that are **accurate and up-to-date** at all times, and are able to ensure that the data they process meet these characteristics.
- *Storage limitation* means that privacy controls must ensure that personal data are not stored beyond the time necessary for a purpose or to comply with legal regulations. In the context of our stakeholders, this means that data should be **deleted and/ or become inaccessible** after a job task has been completed.
- *Integrity and confidentiality* require that privacy controls provide appropriate measures to ensure the proper security of personal data, including protection against unauthorized or unlawful processing. Accordingly, our stakeholder group must only have **authorized access** to personal data required and must also be supported to **store and process** this data themselves in a **suitably protected manner**.
- *Accountability* means that privacy controls must complement towards ensuring and being able to **demonstrate compliance** with the principles mentioned above. In the context of this study, it means that employers must ensure and be able to demonstrate that our stakeholder's processing of employee personal data complies with these principles. This includes **providing privacy policies** based on the inventory of processing records, **documenting and tracking processing activities**, and creating **data protection awareness among data processing employees**.

### 7.3.2 Stakeholder needs for personal data processing

This section outlines general aspects and issues faced by our stakeholder group in the processing of (personal) data. Unless otherwise specified, all aspects and issues presented are direct statements of our participants. We organized these aspects thematically, but the order of appearance does not indicate their significance.

**ORGANIZATION OF WORK** For our stakeholders, **fast and effective communication channels** are of immense importance for their daily work. Especially when requesting data for time-critical tasks. Participants emphasized the advantages of personal contact via phone for initial inquiries in order to discuss the details of a request and prevent a number of time-consuming follow-up queries or lengthy conversations. Participants also preferred personal contact to **facilitate their legitimization** of their person this way: *“When the question ‘Who are you anyway?’ comes up, it is easier to make the inquiry by phone”* (P14). However, for response to requested data, participants then prefer emails, which are valued for their ability to be archived as well as for their traceability of communication. Moreover, the **central management of data, documents, and communication** is seen as advantageous. In particular, a form of central data management is believed to be useful in order to reduce communication load: *“Of course, it would be easiest if I didn’t have to make a phone call, if I didn’t have to write an email, but I could use a system where the data are deposited”* (Po6). In this regard, access to protocols and shared email accounts are commonly used to replace colleagues in case of illness and provide transparency between colleagues in the processing of their tasks. Besides, the **uniformity of processes**, i.e., an organization-wide standardization of processes, is rated as extremely supportive for the handling of personal data at various levels. This includes the use of company-wide standardized forms to elicit data, a uniform presentation of pre-processed data (e.g., calculations), but also **organizational guidelines for handling personal data**. The latter are intended to ensure both a uniform understanding of how data are handled and a uniform process for collecting data.

**PERSONAL DATA HANDLING** The processing of data often requires the transfer of data from some source to another system or form. Any form of **interoperability** that facilitates or automates this transfer is considered helpful. Moreover, an essential prerequisite for efficient work is the **completeness and correctness** of the data at the first request. Particularly when data are collected directly from the data subjects, responses are often incomplete in practice. This frequently results in inquiry loops that are perceived as annoying. Since our stakeholder group also relies heavily on the [HR](#) department to retrieve the necessary personal data from patents or research project applicants and potential employees, it is particularly important for them to know the right contact person right away in order to avoid unnecessary inquiry loops. At last, the **storing and archiving** of data constitutes an integral part of our stakeholders’ job. Data are either processed for networking activities, or the data are archived for verification and documentation of a process. Besides, the archived data also serve as a source for future processing and in order to avoid new inquiries.

**CONSTRAINTS** Our stakeholder’s **time-critical tasks** require that signatures and consents of data subjects or decision-makers be obtained in a timely manner to not miss

deadlines. Our stakeholders also complain about **tedious procedures**, as they often need to compile data from multiple sources. This creates a strong dependency on other departments and entities. Furthermore, **changing and different requirements** are an integral part of our stakeholders' job. Demands for the structure of a processing operation and the data required for it may change regularly if, e.g., funders impose new requirements.

### 7.3.3 Stakeholder needs for data protection

This section presents general issues related to data protection that our stakeholder group reported. Unless otherwise specified, all aspects and issues presented are direct statements of our participants. We organized these aspects thematically, but the order of appearance does not indicate their significance.

**OBSTRUCTIONS** In many situations, our stakeholders perceive **data protection as a burden** because of unclear rules. Often, they do not know whether their actions comply with privacy policies, or whether certain measures are necessary, and how to put them into practice. Here, our stakeholders also complain about a **lack of clear rules** for the transfer of data and **unclear wording** of existing internal regulations. They also feel that their work is impaired by *“general concerns of the data protection officer”* (Po8). Furthermore, their lack of knowledge creates a sense of **uncertainty**, as they always strive for assurance in all their data processing actions. Attempts to guard against privacy violations result in the use of phrases in requests for personal data that are drafted to the best of one's knowledge, and in efforts that are not known to be necessary or even useful.

**ORGANIZATIONAL ISSUES** Established work processes favor **unintended dissemination**, because forwarding (personal) data via existing internal communication channels (e.g., email) do not allow estimating the recipient group. Although our participants themselves welcome shared email accounts, they are concerned when collaborating with other departments, since it is unclear to them which colleagues are involved in the relevant process. It is therefore unclear who have access to the data being processed. Moreover, our stakeholders are concerned about **missing transparency** of their data processing activities toward data subjects. Our participants doubt that employees are aware of the fact that their data are processed and of the extent of processing. Specifically, our participants claimed that information on the processing is not *“explicitly provided - often data subjects are informed via the project manager that their data are in the funds applications”* (Po4) whereas *“explicit consent to data use and disclosure to third parties [...] is not provided at all.”* At the same time, however, our participants also expressed that they themselves do not know how, e.g., the HR department ensures that they are allowed to pass on the requested data to them. Consequently, there is also a **lack of transparency** regarding which **legal bases** would actually apply to their own processing. Here, they consider the entity providing the data to be responsible for compliance.

### 7.3.4 Requirements for employee-centric (re)design of privacy controls

This section describes the requirements that informed our design process presented in the upcoming Section 7.4. The requirements originate in particular from the workshops conducted in the second study (cf. Section 7.2.2), and represent how our stakeholder

group envisions a redesign of its data processing activities to make them more streamlined and privacy-friendly. This is complemented by requirements derived from the fundamental knowledge generated in the mental models in Chapter 5 and the privacy perceptions in Chapter 6. A summary of requirements is presented in Table 7.2. Unless otherwise indicated, requirements represent direct statements of our participants.

**FACILITATION OF THE REQUEST OF PERSONAL DATA** First, in order to **resolve tedious procedures**, privacy controls should facilitate the request of personal data, and be tailored to the needs and use cases of our stakeholders. In particular, they should provide templates and a pre-selection of the data types concerned. Overall, manual effort for accessing and communicating with other parties is to be minimized. To **resolve ambiguity**, data inquiries should ensure that data types can be specified clearly and comprehensively, including deadlines. This is demanded to prevent any follow-up inquiries due to insufficient or wrong information. Furthermore, to **prevent inquiry loops and legitimization issues**, data subjects or personnel in the [HR](#) department should be able to check and verify the legitimacy of the person making the inquiry.

**INCREASED CLARITY** If the required data are unavailable for processing, either because processing is not permitted or because the data have not been obtained, any interface should provide purposeful **instructions on how the data can be obtained and processed**. This includes the (1) reason for non-availability, (2) location of the data, (3) and responsible parties. Furthermore, when creating an inquiry, **ex ante instructions** for the handling of data, e.g., information about the potential uses of the data, should be made available. This includes information (1) on the storage and disclosure of the data, and (2) on any existing or required but pending consent of the data subject. Additional notes should be retrievable for the processing operation, such as special procedures or entities who must be involved. Once personal data are provided, **ex post instructions** for the further use of the data are expected. This includes (1) indication of the permission status (e.g., consent), (2) possible individual restrictions (e.g., further use in publication processes), (3) information on possible data recipients, and (4) the possibility of transferring or storing the data. In this regard, the mental models presented in Chapter 5 emphasize the need to provide precise and explicit instructions and explanations to prevent our stakeholders from drawing implicit conclusions that lead to potential privacy violations and noncompliance. This refers in particular to special treatment of specific data that have an increased sensitivity. Further building upon findings from Chapter 5 and Chapter 6, privacy controls should make data processing employees **aware of data protection obligations** by making data protection visible and explicit in personal data processing. This addresses in particular the lack of knowledge about both employee privacy rights and legal principles, which promotes accidental privacy violations.

**FACILITATION OF DATA MANAGEMENT** Our stakeholders expect automatic enforcement of **privacy preserving access** to personal data to safeguard themselves against any unauthorized processing. This means that stakeholders expect to be granted access to data only if they are authorized. Conversely, they assume that all data that can be accessed are deemed to be legitimate. Thereby, “access” is understood as the “visibility” of data, and is accompanied by the desire to access data in a specific context only. In addition, any data should be accompanied by additional **information and metadata** on



Table 7.2: List of stakeholder requirements.

ID	Description
Req01	Enable detailed and customized data inquiries, including personal messages and deadlines.
Req02	Provide archiving and tracing of correspondence for personal data inquiries.
Req03	Provide centralized access for managing data, documents, and communications.
Req04	Enforce organization-wide consistency of processes related to personal data processing.
Req05	Allow interoperability with other systems in the transfer of personal data.
Req06	Provide complete and accurate personal data upon request.
Req07	Enable storage and archiving of personal data.
Req08	Allow setting deadlines for responding to personal data inquiries.
Req09	Allow compilation of personal data from multiple sources, e.g., multiple data subjects.
Req10	Allow customization of data inquiries in case of new or updated requirements.
Req11	Provide details on recipients when forwarding personal data.
Req12	Provide mechanisms to increase transparency of personal data processing to data subjects.
Req13	Provide templates and pre-selections for data inquiries to avoid lengthy procedures.
Req14	Provide a notice of the lawfulness of personal data inquiries and processing to other entities.
Req15	Provide privacy notices on privacy policies for personal data processing.
Req16	Provide clear instructions on how to obtain personal data.
Req17	Provide clear instructions on how personal data may be processed.
Req18	Provide mechanisms to explicitly obtain permission (e.g., consent from data subjects).
Req19	Provide access to personal data only when authorized to prevent accidental unauthorized processing.
Req20	Provide metadata about personal data, including source, ownership, availability, and timeliness.
Req21	Provide communication mechanisms between data subjects, data owners, and data processing employees.
Req22	Provide mechanisms for informing data subjects about the processing of personal data.
Req23	Allow sharing of ongoing personal data processing with colleagues.
Note. Non-functional requirements according to ISO/IEC 25010 [356] are reported in Appendix D.4.	

data management responsibilities, including (1) the person or department responsible for collection and storage, (2) availability and timeliness of data (including changes since last use), and (3) an overview of previous uses.

**TRANSPARENCY IMPROVEMENT** Privacy controls should provide **feedback channels** that allow personalized notifications to be exchanged with data subjects, and to allow data subjects to ask for particularly sensitive treatment of the data transmitted. Moreover, data subjects should be informed about the (pending) processing of their data via **privacy notifications**. Our participants highlighted the need to demonstrate compliance by (1) informing data subjects about the lawfulness of the processing, (2) explaining to them the underlying business process, and (3) informing them about the recipients of the data and the persons involved in the processing. When data are available for processing, (4) data subjects should also be notified that the data have been processed.

**NON-FUNCTIONAL REQUIREMENTS** In our studies, we also identified non-functional requirements relevant to implementing privacy controls for our stakeholders. We divided the requirements according to the categories of ISO/IEC 25010 [356]. Regarding *compatibility*, privacy controls should reuse existing authorization and authentication mechanisms, and support exchanging information with other systems and software. For *performance efficiency*, privacy controls should support parallel use, provide fast loading times, and low implementation costs. *Reliability* aspects involved expectations of high availability, low susceptibility to errors, and no technical weaknesses of the system. For *maintainability*, our participants expected automatic updating. Regarding *usability*, our participants demanded user-friendly User Interfaces (UIs), low time expenditure and training, clarity and little text, quick access to content, and context-sensitive support. A summary compiling all non-functional requirements is available in Appendix D.4

## 7.4 SOLUTION DESIGN

Based on the collected requirements, we developed *Data Cart*, an employee-centric privacy pattern for privacy-compliant processing of employee personal data. In the following, we first introduce the data cart metaphor underlying the solution in Section 7.4.1. We then introduce *Data Cart* in Section 7.4.2, followed by details on the process flow in Section 7.4.3 and details on the corresponding interaction concept in Section 7.4.4.

### 7.4.1 Data cart metaphor

A key requirement of our stakeholders is the timely and effective access to personal data that are usually not under their control. Thus, a primary task of our stakeholders is to assemble a set of different and varying personal data and data subjects from external sources that are needed for a particular business process. This may require initiating multiple data queries, keeping track of them, and processing the responses. Similar complexity in the compilation and tracking of different items and attributes is a well-known problem in online shopping. This is why we adapted the shopping cart<sup>2</sup> interaction pattern to our context, and created the metaphor of a “data cart”. For this

<sup>2</sup> <http://welie.com/patterns/showPattern.php?patternID=shopping-cart>

purpose, the steps necessary to model the processing of personal data in administrative tasks have been roughly mapped to an online shopping cart. The data cart metaphor serves two purposes. First, we used the metaphor in the context of our internal design and development cycle, as well as in internal communication within the project consortium. This allowed for a common understanding of the interaction concept among all project members. Second, we also used the metaphor to break down the complexity of data protection for our participants and integrate privacy requirements into meaningful workflows that align with their needs. The metaphor also builds on our stakeholders' existing knowledge of interaction concepts for complex processes where one first defines an output based on metadata, considers different statuses (e.g., availability), and only gains access after completing different tasks (e.g., payment, delivery).

#### 7.4.2 Privacy pattern proposal

Based on the data cart metaphor and taking into account legal concerns and stakeholder requirements, we developed an employee-centric solution that provides sufficient flexibility to meet various use cases of our stakeholders related to the processing of employee personal data. The solution basically provides for synchronizing the recurring tasks of retrieving and managing personal data with privacy obligations. The result is a harmonized combination of process flow and interaction concept, which we have documented as a privacy pattern. In the remainder of this section, we provide a basic description of the pattern following established templates [184].

**Name:** Data Cart

**Summary:** A single point of access for data processing employees to obtain and manage personal data in a data protection compliant manner.

**Context:** This pattern applies in particular to data processing employees working in public institutions and processing personal data of employees or other members of the institution.

Target stakeholders	Data processing employees
Category of controller	Public institutions
Processing purposes	Academic services, consulting and coaching, event management, monitoring activities, patent registration and exploitation, project management
Categories of personal data	Contact, education, finances, personal identifiers, pictures, professional activity
Data subjects	Employees, other members of the institution, (external parties)
Categories of recipients	Employees, service providers, authorities, public institutions
Data sources	Data subjects, employees' supervisors, HR department

**Problem:** Data processing employees are frequently required to process personal data for time-critical tasks, which necessitates extensive communication with an organizations' employees, departments, and partners. In an organization, particularly heterogeneous business processes prevent effective data inquiries, either because the data received are incomplete and incorrect, or because the correct contact person in other departments is unknown. In many of these cases, data processing employees perceive data protection as a burden because they are uncertain whether they act in compliance with data protection, or whether certain measures are necessary, and how they should put them into practice. In practice, data processing employees thus act with uncertainty and make efforts to protect themselves from misconduct that they do not know are necessary or even correct. As a result, employers, as data controllers thus liable for the actions of their employees, may subsequently fail to comply with their accountability obligations.

**Solution:** Provide an easily accessible data management interface to employee personal data that (1) streamlines data collection processes in organizations and aligns them with data protection requirements, (2) standardizes access to personal data, (3) simplifies access to privacy policies, and (4) supports in demonstrating transparency and compliance by documenting processing activities.

#### Privacy design strategies [159]:

Primary:

- *enforce* privacy policies compatible with legal requirements;
- *demonstrate* compliance with privacy policies and legal requirements.

Supports:

- *minimize* the amount of personal data that are processed;
- *inform* data subjects about personal data processing;
- *control* over personal data processing by data subjects.

#### 7.4.3 Process flow model

In this section, we describe the process flow associated to the solution outlined above. It shall serve architects and developers as a means to understand and integrate the *Data Cart* pattern into their own systems and processes. The process flow divides into tasks to define a personal data processing activity, process personal data, and help demonstrate compliance. The basic flow is outlined in Figure 7.3 and divides into eight tasks. A detailed process flow diagram is shown in Figure 7.4. The process flow starts by assuming that a data processing employee has a demand to process personal data and opens the *Data Cart* interface. The process flow is described below:

1. The first task requires data processing employees to model a data processing activity to be performed. For this purpose, they must choose a processing activity from the organization's records of processing activities for which they are authorized.

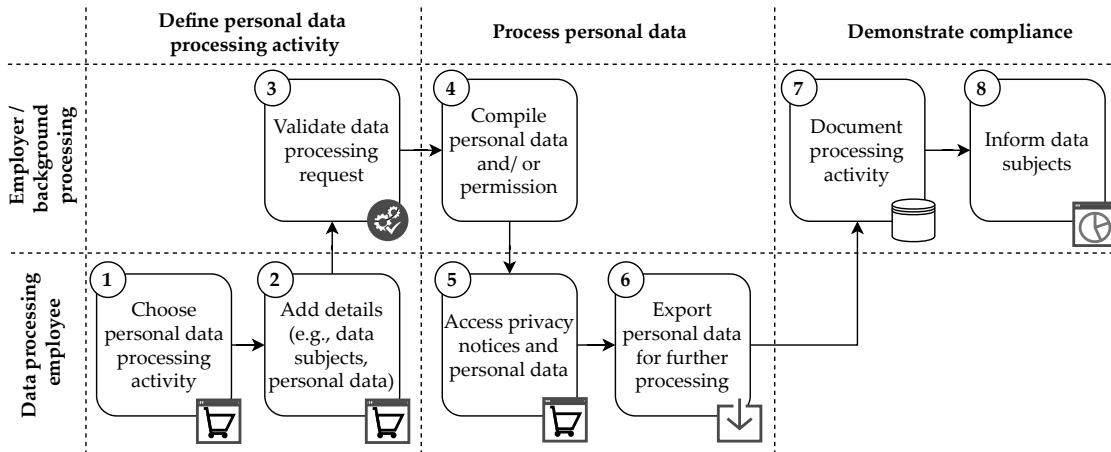


Figure 7.3: Flow of the concept developed using the metaphor of a data cart.

In the event that the personal data have already been collected via form, this can also be imported instead. In such a case, the appropriate processing record entry can be selected automatically.

2. In the second task, data processing employees define tuples of required categories of personal data and data subjects. They may also add additional details, such as specific recipients, the version of personal data they require, or a personal message to the data source (e.g., data subject, [HR](#) department). Once finished, the modeled processing activity is to be submitted as a new data processing request.
3. The submitted processing request must then be validated by verifying for lawfulness of processing against the processing policies extracted from the record of processing activities, and by checking the availability and timeliness of the personal data requested.
4. The next task comprises obtaining missing personal data and permissions. Depending on the processing activity, this may require initiating requests to the respective data subjects or departments to provide the missing data and approvals. It is critical from our stakeholders' point of view that the request be structured, and that input validation is performed. Requests must also include detailed information about the requester and their legitimacy, as well as procedural and legal aspects of the underlying processing. Our own pattern does not specify how such a request should be designed, but privacy patterns similar to *informed consent* may be used here [178].
5. After all tasks have been completed, data processing employees get access to a privacy enhancing personal data management interface. It provides access to meta-data of the data processing request, including status information and details about the tuples requested. In addition, it provides access to contextual privacy policies and reminders extracted from the organizations' directory of processing records. Furthermore, the interface provides the ability to request additional combinations of personal data and data subjects, and to request access to the personal data (e.g., exports).

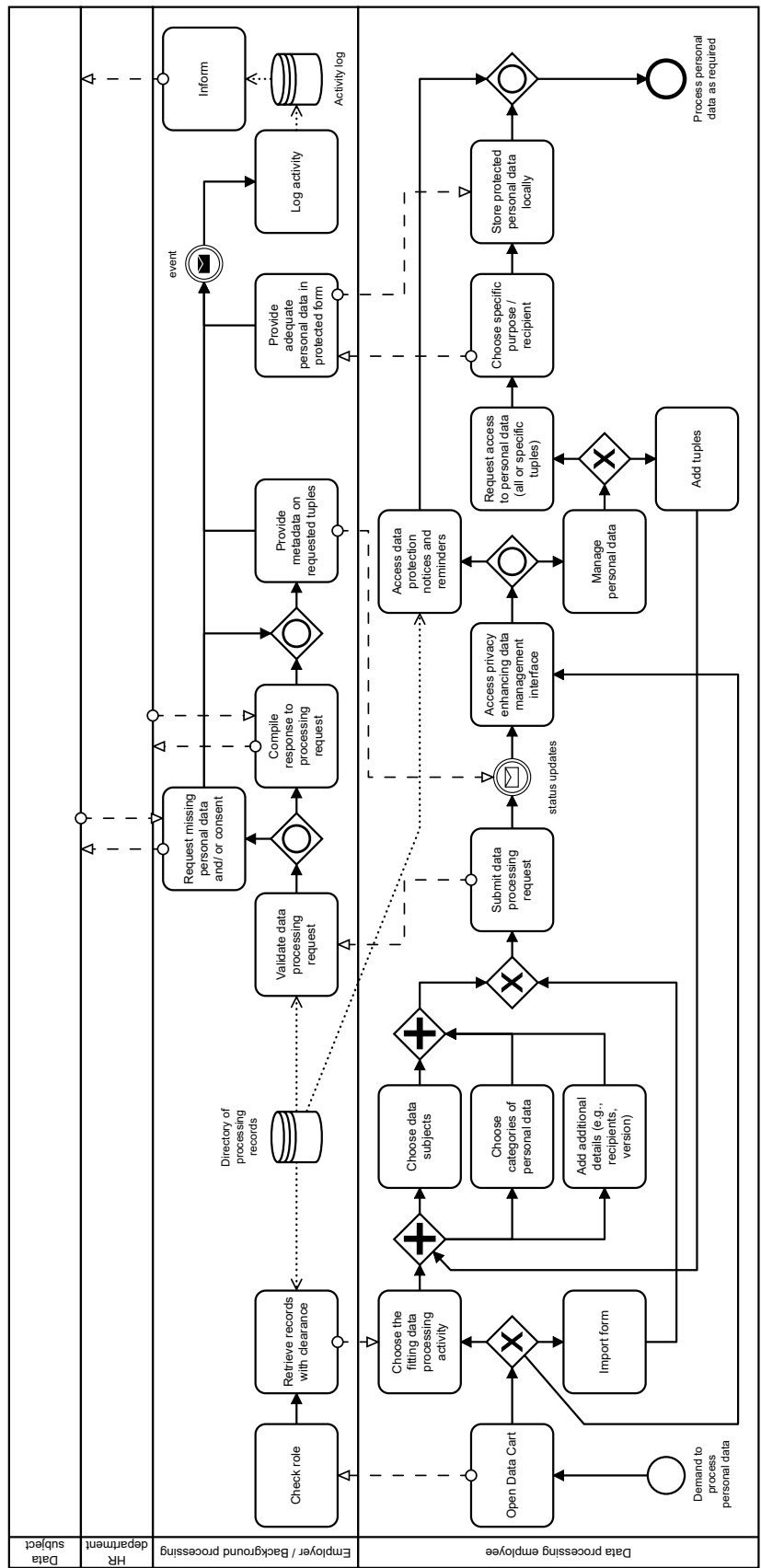


Figure 7.4: Process flow diagram of the concept developed using the metaphor of a data cart.



6. To access raw personal data, data processing employees must choose a specific purpose for which they require the data. Based on this, they should be provided with an export of the personal data, which contains only the data authorized for the purpose and recipients. The export should be adequately protected by default, as our stakeholders do not have the necessary knowledge to do this themselves. All exports should further contain a copy of the data protection information provided in the data management interface, as well as an ID to ensure traceability of the exported file to the original request. The exported personal data then shall be further processed by data processing employees as required. Based on stakeholder feedback, we recommend using common data exchange formats (e.g., MS Excel).
7. All actions, including requests for data and data exports, are logged to document all personal data processing activities. After completing a processing activity, requests can be archived and serve as evidence for later audits and traceability. In addition, the activity log may be used to create a usage history for data processing employees.
8. Furthermore, the here described concept advocates transparency and conceptually provides that data subjects are informed about the processing carried out on the basis of the activity log. This is not covered by our own pattern. Instead, depending on the needs, existing tools and components optimized for employees in their role as data subjects may be used for this purpose [97, 104].

#### 7.4.4 Interaction concept

Based on the process flow outlined above, we developed a corresponding user interaction concept that reflects our stakeholders' point of view. The interaction concept including a mapping to the requirements elicited is shown in Figure 7.5. The interaction concept divides into five parts.

1. First, data processing employees should be offered a personal data management tool that provides for centralized access to personal data and enforces consistency of the full data management process.
2. To model a data processing request, data processing employees should be provided with a preloaded list of processing activities for which they are authorized. Upon selection, employees should be provided with a summary of the processing record. In addition, the planned processing must be given a name and a description. These steps require employees to become aware of the legal basis before processing begins. At the same time, the interaction concept provides for contextual support, such as providing templates and contextual information.
3. To define tuples of personal data and data subjects, data processing employees should be provided with predefined lists. For personal data, these lists may be derived from the selected processing record entry and should be offered as a pre-selection. Likewise, data subjects should be accessible from a list of employees in the organization. The interface should further support the iterative adding of multiple different combinations.

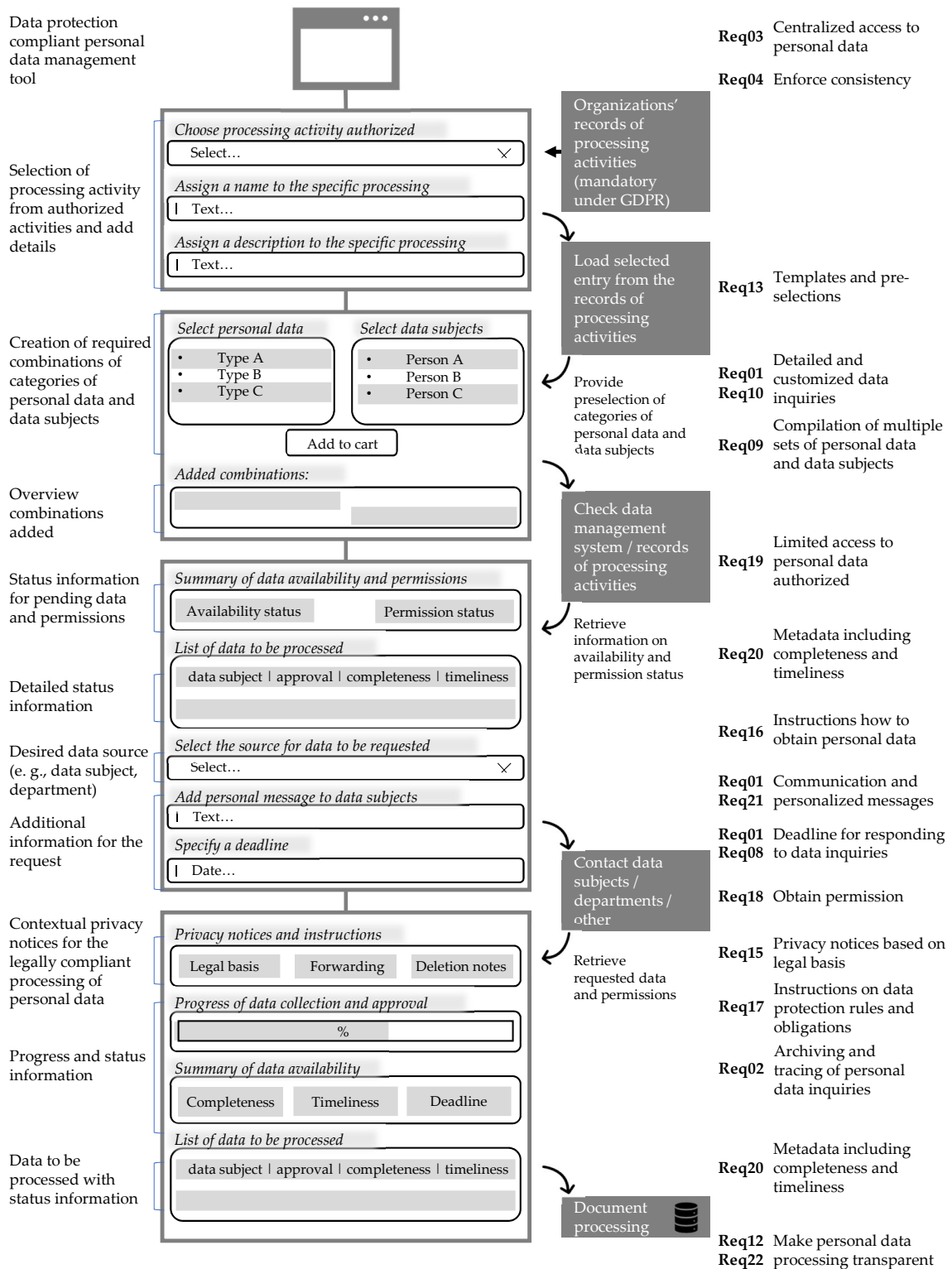


Figure 7.5: Basic interaction concept designed following the data cart metaphor, including a mapping to the stakeholder requirements detailed in Table 7.2. Original screens of the developed prototype that were used for evaluation are included in Appendix D.5.

4. When submitting the request for validation, the results should be provided for review in an overview. It should include status information on whether the processing activity can start immediately after submission of the processing request, or whether additional actions are required, such as collecting personal data or obtaining consent. Detailed status information should be accessible as needed.

At this point, further information may be added to the request. Employees may choose whether to request the data directly from the data subjects, via an administrative department, or in a customized manner. They may also compose individual messages to the data subjects and set a deadline for responding to the request.

5. The privacy enhancing data management interface should provide detailed information on the status of pending requests. This should be complemented by frequently needed or important information on data protection tailored to its users' needs. This includes information on allowed processing operations, whether processing has been approved, to whom data may be disclosed, deletion periods, data sensitivity, and how data must be safeguarded. In general, the interface aims to provide such notices at a glance, with details accessible when necessary. Additional visualizations and a help section for questions accompany detail views (cf. Figure 7.6).

## 7.5 PROTOTYPE DEVELOPMENT

To evaluate the concept presented in Section 7.4, we developed a high-fidelity “Wizard-Of-Oz” prototype [357] referred to as *Data Cart*. To this end, we chose a web application approach based on a micro frontend architecture [358] after comparing the non-functional requirements (cf. Section 7.3.4) with work that investigated various frontend architectures [359]. The prototype was implemented using components of a microservice architecture we developed for company privacy dashboards [104]. Below, we present its essential elements and components relevant for the implementation of *Data Cart*.

The architecture essentially follows the principles of Domain Driven Design [360] and breaks down the topics of employee data protection into functional domains. Within each domain, one or more services implement the domain's tasks. Overall, we differentiate between three core domains: (1) The *transparency* domain focuses on the comprehensive documentation and preparation of information about personal data processing; (2) the *self-determination* domain aggregates functions that allow data subjects to obtain information about and intervene on the processing of their personal data; and (3) the *enforcement* domain is concerned with the technical integration of privacy enhancing technologies into legacy systems that serve a company's core business. Besides, a fourth *generic* domain contains services useful for implementing employee data protection, yet it is not characterized by any content strictly related to data protection.

*Data Cart*'s underlying concept generally benefits from this architecture, as it allows *Data Cart* to be integrated into different IT environments. In addition, the architecture enables us to perform the required policy checks and data availability checks. For the prototype, we primarily used the holistic data model underlying the *transparency* domain, which can be used to clearly describe the information related to employee privacy. It also allows expressing a directory of processing records.

The prototype was implemented using Web Components based on the Stencil JS toolchain. Web Components are reusable UI components whose functionality can be arbitrarily simple or complex. Web Components can further be based on other components and offer great flexibility as they can be programmatically adapted in their content and appearance. This gives Web Components the advantage that they can be individually tested and optimized for their functionality and usability properties. This allows developing UI components tailored specifically for privacy-compliant handling of personal data by data processing employees and reusing them as needed. The components can also be adapted to other use cases or actors with minimal effort.

When implementing the UI, we applied relevant usability heuristics. For the usability tests, the prototype was embedded into a shell application that handled all cross-cutting concerns like authentication, and which was deployed as a microservice using docker. Screenshots of the prototype are shown in Figure 7.6 and in Appendix D.5.

## 7.6 USABILITY PROPERTIES

In the following, we report our findings of the usability testing. In Section 7.6.1 we report participants' understanding of the data cart metaphor, followed by participant feedback and SUS in Section 7.6.2, and identified problems during the study in Section 7.6.3.

### 7.6.1 Metaphor and concept understanding

Overall, our participants did well with the data cart metaphor and were able to apply it to their own workflows. Only one participant stated that they misunderstood the metaphor until they applied the concept, initially assuming that processing requests, rather than data and people, served as "items". Nonetheless, we found that the metaphor was particularly helpful in outlining the basic assumptions and processes of the *Data Cart* concept, including the basics of a directory of processing activities. However, in explaining the concept, participants frequently asked whether such a directory existed and who would maintain it. Only one participant indicated that they knew their organization maintained such a directory. Here, the data cart metaphor supported our participants to relate the tuple of purposes, data subjects, and data categories to a data processing operation without the need to understand the details of the GDPR.

### 7.6.2 Participant feedback and usability rating

All participants stated that the mockups and prototype were "*relatively self-explanatory [to use], given that you were thrown in at the deep end*" (Po7). Other participants stated that *Data Cart* was **intuitive to use** or that one would quickly get used to its flow: "*I first had to look at the interface and get to understand the program, but otherwise I found it quite intuitive*" (Po2). The content was also perceived as **clearly presented**. One participant, however, expressed concern in the event that many *Data Cart* requests are processed simultaneously: "*If there are more requests, I don't know how clear it would still be*" (Po6).

Overall, the SUS scores obtained confirm our participants' qualitative feedback. A median SUS score of 82.5 (mean = 81.25, SD = 7.6) indicates **good usability** (Grade A) [354], however the range was from 67.5 (Grade C) to 95 (Grade A+). This result indicates

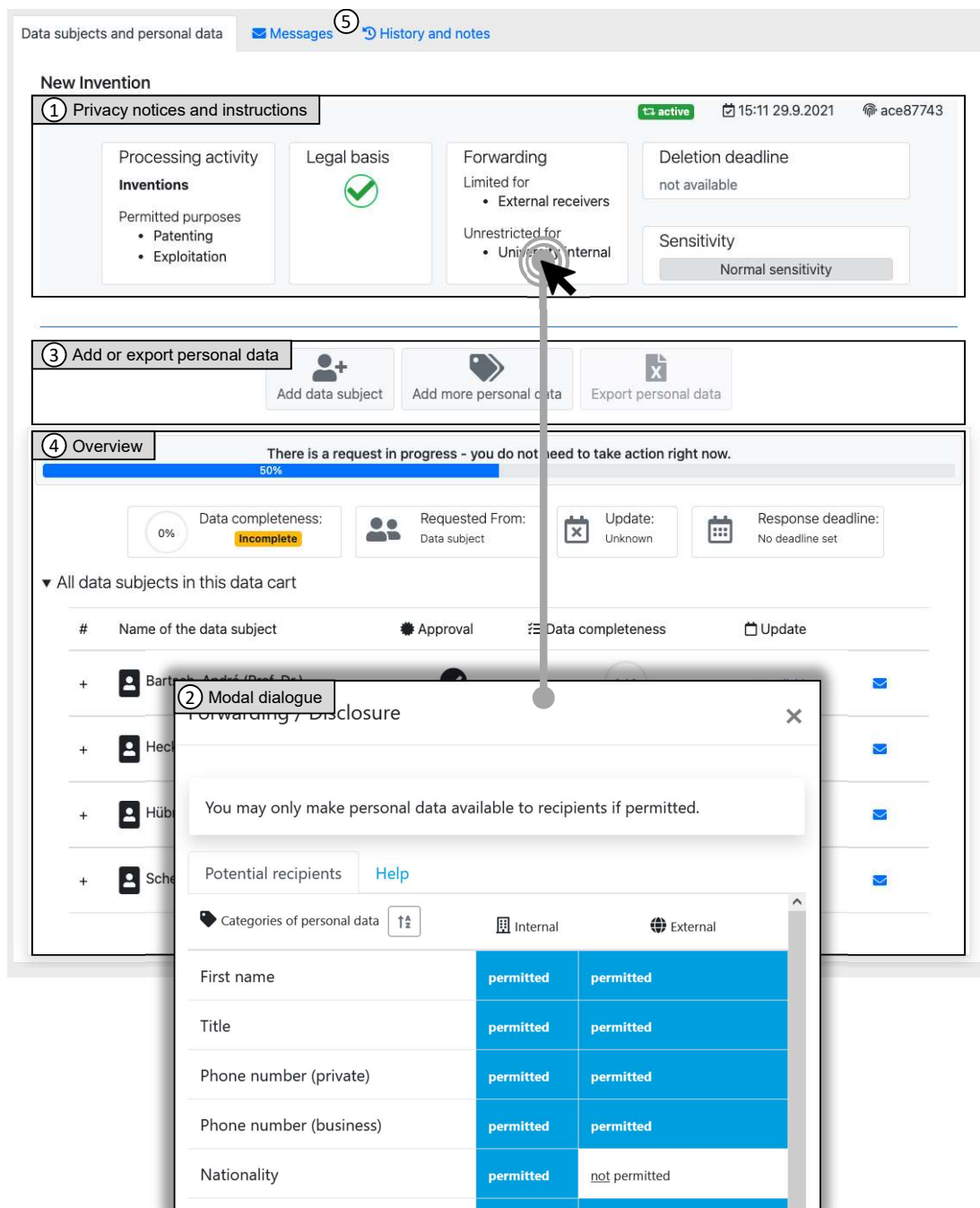


Figure 7.6: Screenshot *Data Cart* personal data management interface with highlighted UI elements of the data management interface implemented in the prototype. The widget bar ① provides essential status information and privacy notices relevant for processing. Interacting with the widgets opens a modal dialogue ② that provides further information and help. Additional data can also be requested, or available data may be exported ③. An overview ④ displays the current status of open and closed requests for all data subjects concerned. Next to data management, the interface provides access to a messenger and activity history ⑤ for the current processing activity.

**potential for improvement.** Problems with operation, which mainly occurred at the beginning of the study, were put into perspective by our participants stating that it was normal to have to get used to the system and that the feeling of secure handling would increase with increasing use of the tool. Some participants expressed concerns about their competence in using the tool and their technical understanding.

### 7.6.3 Identified problems

We identified some problems in the flow of *Data Cart*, in the UI design and wording, as well as some errors in the prototypes' implementation. Some information and functions were also not (correctly) recognized by our participants because they did not have the necessary knowledge or experience. For example, tooltip information was not recognized because they were not unfamiliar with this functionality. In the group usability walkthroughs, we discussed these problems together with the participants. In the formative usability tests, however, these problems mostly occurred at the beginning of the study and disappeared in the course of the study. Furthermore, our participants made suggestions for additional features. We present and discuss these aspects as part of the issues identified in the following subsection.

## 7.7 EMPLOYEE PERCEPTIONS OF DATA CART

To examine **RQ5b**, “How are *TOMs* developed under *UCD* and according to *PbD* perceived by data processing employees?”, we gathered qualitative feedback on the extent to which *Data Cart* would be likely to have an impact on (1) workflows, (2) the handling of personal data, and (3) data protection. Our analysis revealed eleven themes, which we divided into three groups. Section 7.7.1 reports on digitalization and efficiency gains, Section 7.7.2 on data protection aspects, and Section 7.7.3 outlines general concerns.

### 7.7.1 Digitalization and efficiency gains

The first thematic group entails four themes that deal with different topics of digitalization and efficiency gains. The themes are summarized in Table 7.3.

**FUNCTIONAL DIGITALIZATION THROUGH SYSTEMATIZATION** In general, our participants have recognized the potential to optimize processes through digitization. Yet, they are **looking for digitalization**, i.e., a change of processes (cf. [361, 362, 363]). Our participants have liked *Data Cart*'s ability to **systematize and standardize** topics, terms, and processes, since it “*would simplify the work very much and also structure it somehow*” (Po2). In particular, workflows with highly repetitive tasks are expected to become “*a little more streamlined, and then hopefully allow for faster data retrieval as well*” (Po4). Especially for job tasks that involve different personnel and parties, harmonizing the understanding of work processes and work methods is expected to **improve performance**: “*So far I focused more on the efficiency of my work, and Data Cart would increase that in the sense that these requests can be dealt with quickly and in a coherent way*” (Po4).



Table 7.3: Summary of themes related to digitalization and efficiency gains.

Theme	Description
Functional digitalization through systematization	<ul style="list-style-type: none"> <li>▷ Standardizing understanding and terminology</li> <li>▷ Consolidating recurring tasks and issues in practice</li> </ul>
Central data and process management tool	<ul style="list-style-type: none"> <li>▷ Organizing work processes and task planning by mapping business processes</li> <li>▷ Tracking and archiving of activities and personal data</li> </ul>
Replacing less efficient communication channels	<ul style="list-style-type: none"> <li>▷ Mediator / interface between data processing employee, data owners, and data subjects</li> <li>▷ Eliminating the need for e-mails and phone calls</li> <li>▷ Facilitating factual communication and exchange of pertinent information</li> </ul>
Lack of confidence in central data management	<ul style="list-style-type: none"> <li>▷ Concern about maintenance of the system and data</li> <li>▷ Concern about unconnected systems and transfer of data to <i>Data Cart</i></li> </ul>

**REPLACEMENT OF LESS EFFICIENT COMMUNICATION CHANNELS** Our participants emphasized *Data Cart*'s ability to establish **efficient communication channels** for requesting both (personal) data and data processing approvals. *Data Cart* was seen as a mediator between data processing employees, data owners, and data subjects. Here, our participants expected standardization and automation of requests to **replace bloated communications** in established workflows: *"That's just a lot of emails that you send back and forth,[...] I think this [tool] would actually save a lot of communication work if you could then send it [(the data)] via this [tool]."* (Po2). Our participants anticipated that *Data Cart* enforces focusing on the exchange of relevant information, which would have a positive impact on all parties involved. This primarily concerns **increased efficiency and reduced workload**, because a request would contain all necessary information: *"Well, it definitely costs less time than phoning the colleague in the HR department, for example"* (Po7).

**CENTRAL DATA AND PROCESS MANAGEMENT TOOL** Participants described *Data Cart* as a **database interface** and **data management concept** that should fulfill some specific requirements: *"If we have to work with data that are already in a database [...], and all this data maintenance has been done before, then this is a great support – absolutely! That's awesome! And that belongs basically to every database, that should actually exist everywhere"* (Po8). Independent of its primary task, *Data Cart* also helps in **organizing work processes**: *"If I now process many such data, one has an overview here so to speak: I still have this running, I still have this running, the deadline and so on. And if you use it often, it's of course clearer than if you had to remember it yourself, what's going on now or what inquiries I still have, and also what old stuff I might have. Yes, I think that's actually quite good"* (Po5). P10 added that *"you also have your to-dos at a glance, [...] a kind of workflow organization that supports you, so that you also set deadlines and then see which of the deadlines are coming up soon and what I need to take care of now, so that's basically also a tool that supports you in the organizing."*

Table 7.4: Summary of themes related to data protection.

Theme	Description
Desire for systematic data protection	<ul style="list-style-type: none"> <li>▷ Establishing data protection by design</li> <li>▷ Enabling efficient, effortless, and secure handling of personal data</li> </ul>
Consequences of systematic data protection as an obstacle to work	<ul style="list-style-type: none"> <li>▷ Conflicting with established work practices and procedures</li> </ul>
Integration limits as a barrier for data protection	<ul style="list-style-type: none"> <li>▷ Transitions between processes and systems are critical for data protection compliance</li> <li>▷ Processing of data remains unaffected without adaptation of processes</li> </ul>
Raising awareness of data protection	<ul style="list-style-type: none"> <li>▷ Sensitizing data processing employees for data protection</li> <li>▷ Allowing sensitization of data subjects</li> <li>▷ Correcting and aligning interindividual understanding of “sensitive data”</li> </ul>
Central source of information for data protection	<ul style="list-style-type: none"> <li>▷ Eliminating non-uniform handling of data protection rules by providing clear and understandable instructions on data protection</li> <li>▷ Keeping data privacy information available and allowing quick access to “important” information</li> </ul>

**LACK OF CONFIDENCE IN CENTRAL DATA MANAGEMENT** Despite the expected benefits of *Data Cart* for work, our participants had doubts that implementing a central data management platform would succeed: *“From my experience with other situations, I see this as problematic, so the HR department will show some concerns depositing the data there”* (Po8). There were also some **general concerns about data management**: *“So in theory, that’s definitely neat. But the timeliness of the data, ... how up to date are they? Completeness? The data are all there, but the data also need to be maintained on a regular basis”* (Po7).

### 7.7.2 Data protection

The second thematic group deals with five themes on data protection. The themes are summarized in Table 7.4.

**DESIRE FOR SYSTEMATIC DATA PROTECTION BY DESIGN** In general, the *Data Cart* concept encouraged our participants to discuss their need for **systematic data protection** that integrates with work processes, rather than always being added as an additional expense and interfering with work. Participants pointed out that the correct handling of personal data *“is too often overlooked in everyday life, and the use of a such a tool would, on the one hand, simplify this and, on the other hand, somehow make you aware of the relevance of data*

protection and data" (Po6). Furthermore, our participants praised the PbD approach taken by Data Cart, because "[personal data] would be handled in a more sensitive way without making it [(data protection)] too much of an issue" (Po4). In addition, the approach to systemic data protection in the form of Data Cart "creates legal certainty and can somehow take away uncertainty" (Po5) when dealing with personal data: "Well, basically, because everything is already predefined [...] I think you feel a bit safer, because you can make fewer mistakes yourself, because it is automated or because hints are given" (Po3) and "because I don't have to worry at all about whether the person consents or not, because it is all there" (Po3).

**CENTRAL SOURCE OF INFORMATION FOR DATA PROTECTION** Our participants positioned Data Cart as a **central information platform for data protection** topics, which "compiles the information quite well, so you don't have to go through the hassle of finding out how to proceed with it [(personal data)]" (Po3). Particularly important was **quick access to important information**, i.e., that one can "immediately see which data I'm allowed to pass on externally or internally, I think that's pretty good" (Po5), "because you're simply dealing with sensitive data, and you don't always know whether you're allowed to [process data] or not" (Po1).

**RAISING AWARENESS OF DATA PROTECTION** Data Cart is seen as a **driver of awareness** for both data processing employees and data subjects. Our participants particularly welcomed the sensitization for legally compliant data processing: "Otherwise, you are just less aware of it, so I think it makes you more aware that these are all very important data and that they must also be specially protected" (Po4). Here, too, PbD played a role: "Because otherwise it's like this in the everyday handling of data: I don't even think about what people have approved, what they haven't approved" (Po8), but "just by having this tool at your disposal, you're more likely to even think about 'do I need to pay attention to anything right now?'" At the same time, **documentation and communication** through Data Cart allows data processing employees to fulfill their desire to inform data subjects: "I find this tool quite good for that. That I can then write to [employees] whose data I process in the research proposal and make them aware that their data are being processed and whether they agree to it at all" (Po6).

**INTEGRATION LIMITS AS A BARRIER FOR DATA PROTECTION** Our participants noted that tools like Data Cart **cannot solve all privacy issues**. Especially if tools are introduced as a supplement to existing processes or current workflows, "because then the data are accessible again: I have to archive them for later auditing [...] and then, of course, these sensitive data are stored there. That's a place where everyone has access" (Po4). Further problems arise from the **lack of digitalization**, since requests for project proposals are often made via traditional means of communication not under control of Data Cart, yet they may already contain critical data: "But I wonder what happens when you simply receive data. So just in everyday work, one simply gets some kind of data by email" (P15).

**CONSEQUENCES OF SYSTEMATIC DATA PROTECTION AS AN OBSTACLE TO WORK** It becomes clear that the handling of personal data enforced by Data Cart **creates new obstacles**: "Because if we use this here, we make the request, it gets approved, so the data have to be checked first [...] At that moment, we can't continue at that point. And that delays some workflows" (Po1). In particular, lack of or **denial of approval** is perceived as the biggest obstacle: "If someone's data are not approved, then I can't continue processing. Of course, we don't have this situation now because no one knows that the data are being used" (Po6).

Table 7.5: Summary of themes related to general concerns.

Theme	Description
Acceptance requires enforcement	<ul style="list-style-type: none"> <li>▷ Enforcing organization-wide use and central positioning in the organization</li> <li>▷ Requiring initial awareness of data protection issues</li> <li>▷ Concern about acceptance of <i>Data Cart</i> by third parties and externals</li> </ul>
Burdensome, but appropriate	<ul style="list-style-type: none"> <li>▷ Additional tooling creates more overhead and enforces way of working</li> </ul>

### 7.7.3 General concerns

The third thematic group entails two themes related to general concerns regarding *Data Cart*. The themes are summarized in Table 7.5.

**ACCEPTANCE REQUIRES ENFORCEMENT** Key for the successful implementation of tools like *Data Cart* is the **clear commitment by the organization**, as “one would then certainly have to make that [tool] a standard [...] so that one no longer has the choice” (Po7). Po5 added that “there is [also] the question, whether all employees [...] can be obliged to use this [tool] [...] Everything else would make no sense if you could opt out of it and say ‘I’m not gonna do it’.” Our participants also considered the need for **extrinsic motivation to enforce their own use of the tool at all times**: “If I were obliged to know, is it okay to have their data in our database, then this would be an important tool. But that’s not how we work in practice” (Po8).

**BURDENSOME, BUT APPROPRIATE** Although our participants appreciate the efficient processing of requests through *Data Cart* and even associated an increase in efficiency with it, the sometimes **higher effort in certain situations** was criticized. Especially for smaller requests, enforced compliance with data protection is perceived as being time-consuming: “At some point, [...] you don’t want to create a request using *Data Cart* anymore, which is also a matter of time” (Po4). However, these burdens may be accepted when weighed against the **desire to work in compliance** with privacy policies: “Of course, *Data Cart* makes the work a bit more complicated and means extra work [...] but in general, I think it’s the right thing to do, to use *Data Cart* and to work only with permission” (Po1).

## 7.8 DISCUSSION

Our **UCD** approach with data processing employees revealed numerous aspects that are of practical importance for the development and implementation of usable, i.e., effective, efficient, and satisfactory privacy enhancing personal data management tools. Above all, our analysis indicates that the commitment to the **PbD** principles of *privacy embedded into design* and *full functionality* constitutes a significant success factor for the implementation of such **TOMs** from the perspective of our stakeholder group.

Regarding *privacy embedded into design*, our participants indeed perceived privacy protection more as an “add-on” and thus as a burden. The reasons for this may be that existing processes already require a great deal of effort in terms of data management. This was expressed by the desire for more centralization and the standardization of processes. At the same time, however, our participants were aware of their responsibility in dealing with personal and sensitive data. They also wanted to ensure compliance with data protection regulations and the organizations’ policies, if only for reasons of self-assurance. However, as we have already observed in our studies reported in Chapter 5 and Chapter 6, data processing employees also lack the necessary knowledge about data protection rules to be aware of all the circumstances and to comply with privacy policy. Similar to previous research [341] and our mental model study (cf. Chapter 5), we find that data processing employees appear to recognize sensitive data, but their actions are based on individual interpretations rather than formal rules. In this regard, our findings show that data processing employees intuitively derive several requirements for their handling of data from their perceived responsibilities. Many of these requirements are consistent with the principles of both Art. 5 GDPR and PbD: (1) Processing employee data lawfully and fairly; (2) demonstrating accountability by means of transparency; (3) limiting access to data needed and for which one is authorized; and (4) working with accurate data. This suggests that the interests of employers and data processing employees may certainly be brought together.

Our findings further indicate that *Data Cart*’s underlying concept can be beneficial in this regard, since it incorporates these aspects by design: *Lawfulness* and *purpose limitation* are addressed by reducing human error due to ignorance, since information about the legal basis and purpose become an integral part of any request for personal data; *data minimization* and *accuracy* are achieved through (1) centrally controlled access to personal data, (2) providing meta-information about personal data requested, and (3) triggering of updates; *storage limitation* and *integrity and confidentiality* are supported by incorporating *privacy by default* (e.g., encryption of exports) and data handling information; *fairness and transparency*, as well as *accountability*, are supported by the implicit documenting of requests. Apart from fulfilling these principles, *Data Cart* also counteracts the feeling of uncertainty and ambiguity about privacy policies, because it provides a clear and uniform procedure for handling personal data. This kind of implicit enforcement of data protection promotes the *privacy by default* principle, and was perceived as a relief by our participants, because it reduces the manual compliance effort on their end. In this regard, we would point out that our results also show that data processing employees should not be assumed to have an advanced understanding of data protection just because they process personal data on a regular basis (cf. Chapter 5 & Chapter 6). Moreover, our results suggest that management must establish data protection at the heart of the organization and appreciate the efforts of data processing employees to ensure the successful implementation of TOMs like *Data Cart*.

In this respect, our participants repeatedly regarded the introduction phase of TOMs similar to *Data Cart* as a critical phase for their overall success. In particular, there were concerns that other stakeholders might not accept such a tool. In part, this was attributed to our participants’ assumption that *Data Cart*, as a central data management tool, would also require maintaining a central database, with increased overhead for other stakeholders, such as HR. These concerns are most likely the result of past experiences and simplified mental models due to a lack of expertise in information systems and technol-



ogy (cf. Chapter 5). Stakeholders involved in the design and implementation of TOMs should be aware of these issues and address them accordingly in case of a rollout.

Furthermore, success and acceptance from the perspective of data processing employees seems to depend essentially on the PbD principle of *full functionality*. Strictly speaking, our stakeholders even expect “enhanced functionality”, as the most important requirements are the facilitation of the request for personal data and the data management itself. Especially the anticipated increase in efficiency through *Data Cart* is perceived positively for communication and the handling of data. We hypothesize that this can essentially be attributed to the digital transformation process characteristics [361, 362, 363] that tools such as *Data Cart* imply. Since German institutions frequently remain in a stage of mere digitization (i.e., replacing paper with digital documents), approaches for digitalization (i.e., replacing digital documents with advanced information systems) naturally increase work efficiency of data processing employees too. This offers organizations with digitalization deficits a unique opportunity to leverage efficiency gains from digitalization as a means of introducing data protection tools, simply because employees may then respond to these changes with much more positive attitudes. This may also make employees feel positive about data protection, as it gets associated with more efficient tools and business processes. Consequently, our findings suggest that digitalization provides a great opportunity in itself to redesign processes and implement information systems under PbD. This supports the claim that the GDPR provides an opportunity to address privacy and security issues in an organization [95, 364].

Furthermore, for stakeholders involved in privacy engineering, such as employers, researchers, software engineers, and designers, *Data Cart* is particularly useful in technical systems engineering processes (cf. Section 2.3.2). On the one hand, our requirements analysis and evaluation results lay a foundation for the processes *stakeholder needs and requirements* and *systems requirements definition*. The associated privacy pattern consisting of process model and interaction concept, on the other hand, supports *architecture definition* and *design definition* processes. Overall, we expect that employers in particular would benefit from *Data Cart*. To this end, *Data Cart* demonstrates how taking into account human factors facilitates harmonization of data protection activities with the actual business processes. As such, *Data Cart* exemplifies how the legal requirement to integrate safeguards into data processing can be implemented, and how both employers and data-processing employees can benefit. In this regard, *Data Cart* offers insights into how the obligation to maintain a directory of processing records can be leveraged to facilitate the job tasks of data processing employees. In addition, our findings suggest that *Data Cart* helps raise awareness and thus reduces the risk of data breaches. At the same time, *Data Cart* enables documenting activities of manual personal data processing while keeping the burden low for employees.

## 7.9 STUDY LIMITATIONS

This study provides valuable insights into the UCD of TOMs to help data processing employees in the privacy-compliant processing of employee personal data. Nevertheless, our findings are subject to limitations. First and foremost, our findings are limited to responses from a limited group of employees and their specific work tasks. This certainly limits the validity and generalizability of our findings. However, the limited availability of certain user groups is a common problem in usable security and privacy



research [204]. Moreover, our results are focused on public institutions in the German cultural area, which are influential macroeconomic factors in privacy research [247, 316]. That said, because we received similar requirements and feedback from employees at two different public organizations, we expect to have captured the needs of this particular stakeholder group well.

Another limitation is that *Data Cart* could not be integrated into the real-world working environments of the participating organizations. However, because all of our investigations were based on real-world use cases, we are confident that our findings can serve as a solid and realistic foundation for both future research and privacy engineering. Some of our findings are also supported by previous research in other contexts [270], implying that the anticipated effects are indeed plausible. As a result, we consider that our bottom-up approach complements previous research on existing PETs. However, we should note that our and previous work [270] was qualitative in nature, and assumptions about the impact of PETs on work processes (e.g., efficiency) were made based on participant feedback and business process analysis. Future research may attempt to quantify any impact. It will also be up to future research to examine if the degree of digitalization changes the requirements for tools under PbD.

Furthermore, our results may be biased due to the high proportion of female participants. However, to the best of our knowledge, prior research has only found that female employees in the U.S. had lower security self-efficacy than male employees, but that skills and security behaviors were similar or biased by self-reports [365]. Moreover, unlike in the private context, data protection requirements and expected behavior are provided by the employer and the law. Employers are also responsible for providing data protection training. Potential bias in our results thus becomes less likely. Nevertheless, future research needs to examine whether there are gender differences in the requirements for privacy enhancing personal data management tools.

Moreover, the social desirability bias and the Hawthorne effect [352] may have influenced our requirements survey and evaluation. Despite efforts to promote an open and honest discussion, and to formulate questions without bias, participants' judgements may appear to be more positive than they were. In addition, our participants' responses were influenced by the recency and primacy effect, which was expressed by them supporting their arguments with what they had recently experienced. However, the focus groups likely helped to mitigate this effect. Nonetheless, the workshop formats chosen have the disadvantages of participants not sharing personal opinions and certain topics being overrepresented due to group dynamic. [303]. However, we suspect that these disadvantages had little effect because the participants had already been working together for several months or years and the groups were relatively small.

Furthermore, we do not consider *Data Cart* to represent "the" ultimate solution. Still, it represents a decent concept for privacy engineering and research to get to understand (1) how the overall processing of personal data can be improved through tool support, and (2) how these tools must be developed in order to provide effective and satisfying assistance to the target user group. Our findings currently indicate that highly specialized tools that completely map business processes and adhere to PbD may receive the most approval. Certainly, *Data Cart* does not address all PbD principles equally. As our participants have pointed out, the principle of *end-to-end security*, in particular, is only addressed to a limited extent. In addition, we did not investigate security requirements and therefrom resulting usability issues. However, when compared to other systems in-

volving critical data, *Data Cart* does not have any special requirements. As a result, we are confident that mechanisms such as single sign on and risk-based authentication [366] can contribute to *Data Cart*'s usability. Indeed, our participants expected the same login mechanisms as in other systems. Last but not least, *Data Cart* may be adapted in the future to meet participants' demands for more comprehensive solutions and become an integral part of standard software used in organizations.

## 7.10 SUMMARY

In this chapter, we laid out the results of a UCD study with 19 data processing employees to develop a feasible and usable privacy management solution that assists data processing employees in handling employee personal data in a privacy-compliant manner, thereby assisting them in preserving employee privacy. Following our literature survey in Chapter 3, this study complements previous approaches by being the first to design privacy controls that focus on the responsibility of data processing employees to protect employee privacy.

In this regard, our investigation of **RQ5** "*How can data processing employees be effectively, efficiently, and satisfactorily supported in the data protection compliant processing of employee personal data?*" revealed a number of requirements that must be considered for such privacy controls to ensure they do not become a mere burden: (1) Facilitating overall data management as well as requests for personal data; (2) increasing clarity and advice for the correct handling of personal data; and (3) improving transparency towards data subjects. Based on this, we developed and evaluated *Data Cart*, an approach that empowers data processing employees to process employee personal data in a privacy-compliant manner and supports employers in meeting their accountability obligation. To this end, *Data Cart* (1) streamlines data management processes and brings them in line with data protection requirements, (2) standardizes access to personal data, (3) facilitates employee access to privacy policies, and (4) enables documentation of personal data processing.

Our evaluation of *Data Cart* revealed its potential to raise data protection awareness, reduce errors, and increase work efficiency for data processing employees. Our results also indicate that the efficiency gains from merging data management and data protection in the context of digitization could be a decisive factor for employee acceptance of TOMs. As a result, we present a privacy pattern consisting of a process flow and interaction concept that offers practical solutions to stakeholders involved in privacy research or engineering for the human-centered design of privacy controls to safeguard the right to informational self-determination, thus addressing the second objective of this dissertation (cf. Section 1.2). This study's outcomes are of particular value for privacy engineering activities in the *architecture design* and *system definition* processes (cf. Section 2.3.2), but also provide insights for a knowledge repository on broader issues and opportunities for improving the usability of privacy management tools.

## CONCLUSION

*Learn from yesterday, live for today, hope for tomorrow.  
The important thing is not to stop questioning.*

— Albert Einstein

In this chapter, we conclude this dissertation. To this end, we summarize our work in Section 8.1 and then provide an outlook for potential future work in Section 8.2.

## 8.1 SUMMARY

The right to informational self-determination guarantees employees in principle transparency and control over the collection, use, and disclosure of their personal data. However, employees are generally obliged to disclose large amounts of personal data during regular employment because the employer's interests or the law outweigh the employees' privacy interests. To still warrant employees' rights to freedom and privacy, the legislator obligates employers to implement TOMs and data subject rights. For these privacy controls to be effective, they must be designed employee-centric, i.e., they must take into account human factors in employee privacy to address employees' privacy needs and requirements just as much as legal and organizational requirements.

To this end, this dissertation addresses prevailing knowledge and research gaps related to contemporary and Eurocentric perspectives on employee privacy, arguably one of the most influential privacy frameworks of our time. In contrast to previous work, this dissertation provides missing fundamental knowledge on theoretical and abstract privacy concepts that are of great use for the employee-centric design and implementation of the right to privacy, while respecting legal obligations. This is complemented by a practical solution that focuses on the key role of data processing employees for employee privacy protection. The outcome of this dissertation provides a toolkit for the stakeholders involved in various systems engineering processes to enable employee-centric privacy engineering.

In particular, we provide insights into employees' internal conceptualization of information privacy. In eliciting mental models of 27 employees for the right to informational self-determination, we provide insights into employees' (1) perceptions of different categories of data, (2) familiarity with the legal framework regarding expectations for privacy management, and (3) awareness of data processing, data flow, safeguards, and threat models. The three identified types of mental models Privacy Doctrinairist (PD), Data-Flow Concerned Protectionist (DFCP), and Control-Seeking Pragmatist (CSP) make different manifestations of these insights tangible to inform the employee-centric privacy engineering process. Our results also revealed implications for the implementation of notice and transparency, control and intervention abilities, as well as for rising employee awareness and the implementation of TOMs.

To complement these implications drawn from qualitative work with empirical evidence, we conducted a cross-sectional survey with 553 employees from Germany to

gain a better understanding of perceived data sensitivity and willingness to disclose personal data in employment. We provide evidence that the employment context differs significantly from other contexts in this regard. We further identified four groups of personal data that represent different dimensions of context, sensitivity, and willingness to disclose that are unique to the employment context. In studying common antecedents and employees' disposition to a right to privacy, our results highlight the importance to make privacy controls usable to avoid burdening the employer-employee relationship, and that future research is needed to understand the specifics of employee privacy. Furthermore, we revealed the first clusters of employees with different perceptions of personal data. We outlined our findings' implications for classifying personal data and implementing employee data subject rights in privacy engineering. Our research also revealed several implications for the future studying of employee privacy and the consideration of contextual factors.

Moreover, we presented the privacy pattern *Data Cart* for implementing employee-centric personal data management tools that help data processing employees in complying with data protection obligations. Based on a thorough UCD process with a series of eight workshops and additional usability tests, the pattern combines legal, organizational, and employee requirements for the processing of employee personal data. Our solution empowers data processing employees in the privacy-compliant processing of employee personal data by (1) streamlining processes involving data collection, (2) standardizing access to personal data, and (3) facilitating access to privacy policies. Our results suggest that efficiency gains from merging data management and data protection along with the digitalization of processes can be a decisive factor for the acceptance of TOMs among employees. Moreover, *Data Cart* assists employers in their role as data controllers to improve GDPR-compliance, since it is likely to raise awareness and thus reduce human errors, but also facilitates documentation of work processes. Employers, IT engineers, and researchers may take up on our findings to elaborate other aspects in the future design of usable privacy controls.

Our overall contributions benefit a wide range of stakeholders. By providing in-depth insights into employee requirements and needs, our results help employers and developers design improved work tools, privacy technologies, and business processes that are better aligned with employees' expectations. Our findings also provide policymakers and researchers with profound knowledge about employees' privacy attitudes. As such, our results lay the groundwork for more targeted research in the future. Employers, IT engineers, and researchers come to understand how data processing employees can become levers to protect employee privacy. Simultaneously, we demonstrate how employers can enhance and encourage compliance. We are confident that our findings will also be of interest to stakeholders outside of Germany and the EU, as some of the GDPR's key concepts are now reflected in privacy laws worldwide.

## 8.2 LIMITATIONS AND OUTLOOK

Like any study in the field of privacy research, our work has some overall limitations. First, although our results constitute an important step towards complementing the results of prior studies that had U.S.-biased samples (cf. Chapter 3), the generalizability of our results is limited by macro-environmental factors. This particularly applies to the cultural background and the existing strong governmental regulation framework in Ger-

many and the EU [247]. Results thus may vary for employees from different regions and cultures [253], or industries and organizations [316]. Considering that the differences between the various jurisdictions on privacy issues are being mitigated by the GDPR and harmonization is emerging in the EU, but also globally, our findings nevertheless provide a solid basis for various stakeholders worldwide. In particular, our work constitutes an important step toward closing prevailing research gaps, especially compared to research in the non-employment context. In this way, our work offers some starting points for future work, listed below.

**EMPIRICAL INVESTIGATIONS AND UPDATED PRIVACY MACRO MODELS** To investigate human factors in both privacy research and privacy engineering, measurement instruments must provide results of high contextual validity and reliability to adequately address stakeholder privacy needs and requirements [342]. Since the focus of existing, modern instruments is on contexts outside the employment context, it offers much potential for validation and adaptation to the employment context. Our research has revealed several insights that confirm, challenge, but also extend aspects of current privacy macro models for use in employment contexts. Also, there are other individual factors and antecedents as well as control variables that were not examined in this dissertation [112, 250, 262]. This opens up new opportunities for research to examine the effects of, e.g., perceived control, expected benefits, personality traits, and mental models, as well as to extend or build upon the 62 types of personal data, the latent groups of data, and the clusters of employees that we identified. In this regard, since we found that contextual differences seem to outweigh cultural differences (cf. section 6.3), study formats similar to ours could be replicated in other cultural settings in the employment context to gather evidence and compare cultural characteristics. If researchers have the resources available, study designs with individual large organizations and unambiguous insights into personal data disclosure (e.g., through management reports) would provide a valuable contribution in this respect, since much of the research on actual disclosure behavior in employment was conducted in the U.S. in the 1980s [79, 80].

**EMPLOYEE-CENTRIC PRIVACY PATTERN CATALOGS** Privacy patterns are of great value in privacy engineering to build knowledge repositories and convert privacy requirements into concrete designs that fulfil the foundational principles of PbD (cf. Section 2.3.4). This dissertation provides a first privacy design pattern focusing on data processing employees. Other work has already successfully validated the privacy pattern “privacy dashboard” to implement employee data subject rights [97]. Given the power imbalance between employees and employers, and the high contextual uniqueness of the employment context, we advocate that the design of employee specific privacy patterns should be fostered in the future. In the medium term, this would enable the provision of employee privacy pattern catalogs, which could be converted to privacy pattern languages in the long term, complementing approaches in non-employment contexts (cf. Section 2.3.4). In this regard, we consider that incorporating all perspectives from various stakeholder groups in the implementation of PbD is the right way to go, and we would encourage the inclusion of other stakeholder groups in future investigations. Future research should also consider heterogeneous user groups or consider the requirements through mixed approaches that, e.g., bring together the views of both data subjects and data processing employees to provide for comprehensive solutions.





## BIBLIOGRAPHY

---

- [1] Bundesverfassungsgericht. Az. 1 BvR 209, 269, 362, 420, 440, 484/83, 1983.
- [2] Benedikt Lebek, Kenan Degirmenci, and Michael H. Breitner. Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices. In *Proceedings of the 19th Americas' Conference on Information Systems (AMCIS)*, pages 1–8, 2013.
- [3] Tobias Mettler and Jochen Wulf. Physiolytics at the Workplace: Affordances and Constraints of Wearables Use from an Employee's Perspective. *Information Systems Journal*, 29(1):245–273, 2019.
- [4] Nils 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.
- [5] Christian Runte and Michael Kamps. GDPR Enforcement Tracker Report: Executive Summary. Survey 2nd Edition, CMS Law-Now, 2021. URL <https://cms.law/en/media/local/cms-hs/files/publications/publications/gdpr-enforcement-tracker-report-2021-executive-summary>.
- [6] Seda Gürses, Carmela Troncoso, and Claudia Diaz. Engineering Privacy by Design. In *Proceedings of the 4th Conference on Computers, Privacy & Data Protection (CPDP)*, pages 1–25, 2011.
- [7] Nicolas Notario, Alberto Crespo, Yod-Samuel Martin, Jose M. Del Alamo, Daniel Le Metayer, Thibaud Antignac, Antonio Kung, Inga Kroener, and David Wright. PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology. In *Proceedings of the IEEE Security and Privacy Workshops (SPW)*, pages 151–158, 2015.
- [8] MITRE Privacy Engineering Framework and Life Cycle Adaptation Guide. White Paper 19-00598-5, Mitre, 2019. URL <https://www.mitre.org/sites/default/files/publications/pr-19-00598-5-privacy-engineering-framework-v2.pdf>.
- [9] ISO/IEC JTC 1/SC 27. ISO/IEC TR 27550:2019: Information Technology —Security Techniques —Privacy Engineering for System Life Cycle Processes. Technical report, International Organization for Standardization, 2019. URL <https://www.iso.org/standard/72024.html>.
- [10] Sean W. Brooks, Michael E. Garcia, Naomi B. Lefkowitz, Suzanne Lightman, and Ellen M. Nadeau. An Introduction to Privacy Engineering and Risk Management in Federal Information Systems. NIST Interagency/Internal Report NISTIR 8062, National Institute of Standards and Technology, 2017. URL <https://doi.org/10.6028/NIST.IR.8062>.

- [11] Ann Cavoukian, Stuart Shapiro, and R. Jason Cronk. Privacy Engineering: Proactively Embedding Privacy by Design. White Paper, Information and Privacy Commissioner of Ontario Canada, 2014. URL <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-priv-engineering.pdf>.
- [12] Denis Feth, Andreas Maier, and Svenja Polst. A User-Centered Model for Usable Security and Privacy. In *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)*, pages 74–89, 2017.
- [13] Seda Gürses and Jose M. del Alamo. Privacy Engineering: Shaping an Emerging Field of Research and Practice. *IEEE Security and Privacy*, 14(2):40–46, 2016.
- [14] Antonio Kung, Christophe Jouvray, Nicolas Notario, Alberto Crespo, Samuel Martin, José del Álamo, and Carmela Troncoso. Contribution to Study Period on Privacy Engineering Framework. Technical Report v1, PRIPARE, 2015. URL [https://lists.oasis-open.org/archives/pmr/201508/msg00003/WG5\\_N94\\_PRIPARE\\_Contribution\\_SP\\_Priv\\_engineer\\_frmwk.pdf](https://lists.oasis-open.org/archives/pmr/201508/msg00003/WG5_N94_PRIPARE_Contribution_SP_Priv_engineer_frmwk.pdf).
- [15] Sarah Spiekermann and Lorrie Faith Cranor. Engineering Privacy. *IEEE Transactions on Software Engineering*, 35(1):67–82, 2009.
- [16] Awanthika Senarath, Nalin A. G. Arachchilage, and Jill Slay. Designing Privacy for You: A Practical Approach for User-Centric Privacy. In *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)*, pages 739–752, 2017.
- [17] William Stallings. *Information Privacy Engineering and Privacy by Design: Understanding Privacy Threats, Technology, and Regulations Based on Standards and Best Practices*. Pearson Education Inc, 1st edition, 2020.
- [18] Simone Fischer-Hübner, John Sören Pettersson, and Julio Angulo. HCI Requirements for Transparency and Accountability Tools for Cloud Service Chains. In *Proceedings of the 1st Summer School on Accountability and Security in the Cloud*, pages 81–113, 2015.
- [19] Andrew S. Patrick and Steve Kenny. From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interactions. In *Proceedings of the Workshops on Privacy Enhancing Technologies (PET)*, pages 107–124, 2003.
- [20] Majed Alshammari and Andrew Simpson. Towards a Principled Approach for Engineering Privacy by Design. In *Proceedings of the 5th Annual Privacy Forum (APF)*, pages 161–177, 2017.
- [21] ISO/TC 159/SC 4. *ISO 9241-210:2019: Ergonomics of Human-System Interaction Part 210: Human-centred Design for Interactive Systems*. International Organization for Standardization, 2nd edition, 2019. URL <https://www.iso.org/standard/77520.html>.
- [22] ISO/TC 159/SC 4. *ISO 9241-11:2018: Ergonomics of Human-System Interaction Part 11: Usability: Definitions and Concepts*. International Organization for Standardization, 2018. URL <https://www.iso.org/standard/63500.html>.

- [23] Kovila P.L. Coopamootoo and Thomas Groß. Mental Models of Online Privacy: Structural Properties with Cognitive Maps. In *Proceedings of the 28th International BCS Human Computer Interaction Conference (BCS-HCI)*, pages 287–292, 2014.
- [24] Pamela J. Wisniewski and Xinru Page. Privacy Theories and Frameworks. In Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano, editors, *Modern Socio-Technical Perspectives on Privacy*, pages 15–41. Springer, 2022.
- [25] Devasheesh P. Bhawe, Laurel H. Teo, and Reeshad S. Dalal. Privacy at Work: A Review and a Research Agenda for a Contested Terrain. *Journal of Management*, 46(1):127–164, 2020.
- [26] Leslie K. John, Alessandro Acquisti, and George Loewenstein. Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information. *Journal of Consumer Research*, 37(5):858–873, 2011.
- [27] Helen Nissenbaum. Privacy as Contextual Integrity. *Washington Law Review*, 79(1):1119–157, 2004.
- [28] Daniel J. Solove. A Taxonomy of Privacy. *University of Pennsylvania Law Review*, 154(3):477–560, 2006.
- [29] Kim Wuyts and Wouter Joosen. LINDDUN Privacy Threat Modeling: A Tutorial. Technical Report C685, Department of Computer Science, KU Leuven, 2015. URL [https://www.linddun.org/\\_files/ugd/cc602e\\_f98d9a92e4804e6a9631104c02261e1f.pdf](https://www.linddun.org/_files/ugd/cc602e_f98d9a92e4804e6a9631104c02261e1f.pdf).
- [30] Nurul Amin Badrul, Shirley Ann Williams, and Karsten Øster Lundqvist. Online Disclosure of Employment Information: Exploring Malaysian Government Employees’ Views in Different Contexts. *ACM SIGCAS Computers and Society*, 45(3):38–44, 2016.
- [31] Ricardo Buettner. Analyzing the Problem of Employee Internal Social Network Site Avoidance: Are Users Resistant Due to Their Privacy Concerns? In *Proceedings of the 48th Hawaii International Conference on System Sciences (HICSS)*, pages 1819–1828, 2015.
- [32] Richard Burkhard, Benjamin Schooley, Juanita Dawson, and Thomas Horan. Information Systems and Healthcare XXXVII: When Your Employer Provides Your Personal Health Record —Exploring Employee Perceptions of an Employer-Sponsored PHR System. *Communications of the Association for Information Systems*, 27(1), 2010.
- [33] Peter Cardon, Haibing Ma, A. Carolin Fleischmann, and Jolanta Aritz. Recorded Work Meetings and Algorithmic Tools: Anticipated Boundary Turbulence. In *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS)*, pages 196–205, 2021.
- [34] Darrell Carpenter, Michele Maasberg, Chelsea Hicks, and Xiaogang Chen. A Multicultural Study of Biometric Privacy Concerns in a Fire Ground Accountability

- Crisis Response System. *International Journal of Information Management*, 36(5):735–747, 2016.
- [35] Darrell Carpenter, Alexander McLeod, Chelsea Hicks, and Michele Maasberg. Privacy and Biometrics: An Empirical Examination of Employee Concerns. *Information Systems Frontiers*, 20(1):91–110, 2018.
- [36] Byungjoo Choi, Sungjoo Hwang, and SangHyun Lee. What Drives Construction Workers’ Acceptance of Wearable Technologies in the Workplace?: Indoor Localization and Wearable Health Devices for Occupational Safety and Health. *Automation in Construction*, 84:31–41, 2017.
- [37] Fred D. Davis. Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, 13(3):319–340, 1989.
- [38] Kenan Degirmenci, J P Shim, Michael H Breitner, Ferry Nolte, and Jens Passlick. Future of Flexible Work in the Digital Age: Bring Your Own Device Challenges of Privacy Protection. In *Proceedings of the 40th International Conference on Information Systems (ICIS)*, pages 1–17, 2019.
- [39] Sören Diel, Niklas Gutheil, Fabian Richter, and Christoph Buck. My Data, My Choice?! The Difference between Fitness and Stress Data Monitoring on Employees’ Perception of Privacy. In *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*, pages 4077–4086, 2022.
- [40] William Berkley Easley, S. Nisa Asgarali-Hoffman, Amy Hurst, Helena M. Mentis, and Foad Hamidi. Using a Participatory Toolkit to Elicit Youth’s Workplace Privacy Perspectives. In *Proceedings of the 1st European Symposium on Usable Security (EuroUSEC)*, pages 211–222, 2021.
- [41] Adrian Engelbrecht, Jin Gerlach, Alexander Benlian, and Peter Buxmann. Analysing Employees’ Willingness To Disclose Information In Enterprise Social Networks: The Role Of Organisational Culture. In *Proceedings of the 25th European Conference on Information Systems (ECIS)*, pages 2119–2135, 2017.
- [42] James Lee Jr, Merrill Warkentin, Robert E. Crossler, and Robert F. Otondo. Implications of Monitoring Mechanisms on Bring Your Own Device Adoption. *Journal of Computer Information Systems*, 57(4):309–318, 2017.
- [43] Kimberly M. Lukaszewski, Dianna L. Stone, and Eugene F. Stone-Romero. The Effects of the Ability to Choose the Type of Human Resources System on Perceptions of Invasion of Privacy and System Satisfaction. *Journal of Business and Psychology*, 23(3):73, 2008.
- [44] Domitilla Magni, Veronica Scuotto, Alberto Pezzi, and Manlio Del Giudice. Employees’ Acceptance of Wearable Devices: Towards a Predictive Model. *Technological Forecasting and Social Change*, 172:121022, 2021.
- [45] Pedro Seguel. Information-Sharing Workarounds in Enterprise Social Networks: Privacy-related Triggers. In *Proceedings of the 42nd International Conference on Information Systems (ICIS)*, pages 1–10, 2021.

- [46] Ruth Stock and Martin Hannig. Is There a Privacy Paradox in the Workplace? In *Proceedings of the 41st International Conference on Information Systems (ICIS)*, pages 1–17, 2020.
- [47] Sarah Träutlein and Jin Gerlach. Perceived Information-Based Vulnerability of Enterprise Information Systems: Concept, Antecedents, and Outcomes. In *Proceedings of the 36th International Conference on Information Systems (ICIS)*, pages 1–11, 2015.
- [48] Venkatesh, Morris, Davis, and Davis. User Acceptance of Information Technology: Toward a Unified View. *MIS Quarterly*, 27(3):425, 2003.
- [49] Rebecca M. Chory, Lori E. Vela, and Theodore A. Avtgis. Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses. *Employee Responsibilities and Rights Journal*, 28(1):23–43, 2016.
- [50] Stéphanie Gauttier. Modifying Consent Procedures to Collect Better Data: The Case of Stress-Monitoring Wearables in the Workplace. In *Proceedings of the 22nd International Conference on Business Information Systems (BIS)*, pages 350–360, 2019.
- [51] Frances S. Grodzinsky, Andra Gumbus, and Stephen Lilley. Ethical Implications of Internet Monitoring: A Comparative Study. *Information Systems Frontiers*, 12(4): 433–441, 2010.
- [52] Gundars Kaupins and Malcolm Coco. Perceptions of Internet-of-Things Surveillance by Human Resource Managers. *S.A.M. Advanced Management Journal*, 82(2): 53–61, 2017.
- [53] Cliona McParland and Regina Connolly. Dataveillance in the Workplace: Managing the Impact of Innovation. *Business Systems Research*, 11(1):106–124, 2020.
- [54] Clay Posey, Becky Bennett, Tom Roberts, and Paul B. Lowry. When Computer Monitoring Backfires: Invasion of Privacy and Organizational Injustice as Precursors to Computer Abuse. *Journal of Information System Security*, 7(1):24–47, 2011.
- [55] Sebastian Pütz, Vera Rick, Alexander Mertens, and Verena Nitsch. Using IoT Devices for Sensor-Based Monitoring of Employees’ Mental Workload: Investigating Managers’ Expectations and Concerns. *Applied Ergonomics*, 102:103739, 2022.
- [56] Jason L. Snyder. E-Mail Privacy in the Workplace: A Boundary Regulation Perspective. *Journal of Business Communication*, 47(3):266–294, 2010.
- [57] Myria Watkins Allen, Stephanie J. Coopman, Joy L. Hart, and Kasey L. Walker. Workplace Surveillance and Managing Privacy Boundaries. *Management Communication Quarterly*, 21(2):172–200, 2007.
- [58] Talya N. Bauer, Donald M. Truxillo, Jennifer S. Tucker, Vaunne Weathers, Marilena Bertolino, Berrin Erdogan, and Michael A. Campion. Selection in the Information Age: The Impact of Privacy Concerns and Computer Experience on Applicant Reactions. *Journal of Management*, 32(5):601–621, 2006.

- [59] Stephanie L. Black, Dianna L. Stone, and Andrew F. Johnson. Use of Social Networking Websites on Applicants' Privacy. *Employee Responsibilities and Rights Journal*, 27(2):115–159, 2015.
- [60] Grant M. Brady, Donald M. Truxillo, Talya N. Bauer, and Mark P. Jones. The Development and Validation of the Privacy and Data Security Concerns Scale (PDSCS). *International Journal of Selection and Assessment*, 29(1):100–113, 2021.
- [61] John Drake, Dianne Hall, J. Bret Becton, and Clay Posey. Job Applicants' Information Privacy Protection Responses: Using Social Media for Candidate Screening. *AIS Transactions on Human-Computer Interaction*, 8(4):160–184, 2016.
- [62] Marcelline R. Fusilier and Wayne D. Hoyer. Variables Affecting Perceptions of Invasion of Privacy in a Personnel Selection Situation. *Journal of Applied Psychology*, 65(5):623–626, 1980.
- [63] Debora Jeske, Sonia Lippke, and Kenneth S. Shultz. Predicting Self-Disclosure in Recruitment in the Context of Social Media Screening. *Employee Responsibilities and Rights Journal*, 31(2):99–112, 2019.
- [64] Xun Li and Radhika Santhanam. Will It Be Disclosure or Fabrication of Personal Information? An Examination of Persuasion Strategies on Prospective Employees. *International Journal of Information Security and Privacy*, 2(4):91–109, 2008.
- [65] Marsha L. Nielsen and Kristine M. Kuhn. Late Payments and Leery Applicants: Credit Checks as a Selection Test. *Employee Responsibilities and Rights Journal*, 21(2):115–130, 2009.
- [66] Bernard L. Rosenbaum. Attitude toward Invasion of Privacy in the Personnel Selection Process and Job Applicant Demographic and Personality Correlates. *Journal of Applied Psychology*, 58(3):333–338, 1973.
- [67] Eugene F. Stone-Romero, Dianna L. Stone, and David Hyatt. Personnel Selection Procedures and Invasion of Privacy. *Journal of Social Issues*, 59(2):343–368, 2003.
- [68] Dianna L. Stone and Eugene F. Stone. Effects of Missing Application-Blank Information on Personnel Selection Decisions: Do Privacy Protection Strategies Bias the Outcome? *Journal of Applied Psychology*, 72(3):452–456, 1987.
- [69] Eugene F. Stone and Dianna L. Stone. Privacy in Organizations: Theoretical Issues, Research, Findings, and Protection Mechanisms. *Personnel and Human Resources Management*, 8:349–411, 1990.
- [70] J. William Stoughton, Lori Foster Thompson, and Adam W. Meade. Examining Applicant Reactions to the Use of Social Networking Websites in Pre-Employment Screening. *Journal of Business and Psychology*, 30(1):73–88, 2015.
- [71] G. Stoney Alder, Marshall Schminke, and Terry W. Noel. The Impact of Individual Ethics on Reactions to Potentially Invasive HR Practices. *Journal of Business Ethics*, 75(2):201–214, 2007.



- [72] Bradley J. Alge, Gary A. Ballinger, Subrahmaniam Tangirala, and James L. Oakley. Information Privacy in Organizations: Empowering Creative and Extrarole Performance. *Journal of Applied Psychology*, 91(1):221–232, 2006.
- [73] Shawn F. Clouse, Ryan T. Wright, and Ronald E. Pike. Employee Information Privacy Concerns with Employer Held Data: A Comparison of Two Prevalent Privacy Models. *Journal of Information Privacy and Security*, 6(3):47–71, 2010.
- [74] Thomas W. Dillon, Arthur J. Hamilton, Daphyne S. Thomas, and Mark L. Usry. The Importance of Communicating Workplace Privacy Policies. *Employee Responsibilities and Rights Journal*, 20(2):119–139, 2008.
- [75] Erik R. Eddy, Dianna L. Stone, and Eugene E Stone-Romero. The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives. *Personnel Psychology*, 52(2):335–358, 1999.
- [76] Howard Garland, Jane Giacobbe, and J. Lawrence French. Attitudes Toward Employee and Employer Rights in the Workplace. *Employee Responsibilities and Rights Journal*, 2(1):49–59, 1989.
- [77] Kevin W. Mossholder, William F. Giles, and Mark A. Wesolowski. Information Privacy and Performance Appraisal: An Examination of Employee Perceptions and Reactions. *Journal of Business Ethics*, 10(2):151–156, 1991.
- [78] Dianna L. Stone and Debra A. Ketch. Individuals' Attitudes Toward Organizational Drug Testing Policies and Practices. *Journal of Applied Psychology*, 74(3):518–521, 1989.
- [79] Paul D. Tolchinsky, Michael K. McCuddy, Jerome Adams, Daniel C. Ganster, Richard W. Woodman, and Howard L. Fromkin. Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment. *Journal of Applied Psychology*, 66(3):308–313, 1981.
- [80] Richard W. Woodman, Daniel C. Ganster, Jerome Adams, Michael K. McCuddy, Paul D. Tolchinsky, and Howard Fromkin. A Survey of Employee Perceptions of Information Privacy in Organizations. *Academy of Management Journal*, 25(3):647–663, 1982.
- [81] David Krebs and Juris 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.
- [82] Lothar Determann and Robert Sprague. Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States. *Berkeley Technology Law Journal*, 26(2):979–1036, 2011.
- [83] Adam Eichelberger. Global Employee Privacy: A Case Study on the Minefield of Employee Privacy Rights in the EU, USA, and KSA. *Indiana International & Comparative Law Review*, 31(1):177–224, 2021.

- [84] Stephan A. Fahrenkrog-Petersen, Han van der Aa, and Matthias Weidlich. PRETSA: Event Log Sanitization for Privacy-aware Process Discovery. In *Proceedings of the 1st International Conference on Process Mining (ICPM)*, pages 1–8, 2019.
- [85] Munyaradzi Gudo and Keshnee Padayachee. SpotMal: A Hybrid Malware Detection Framework with Privacy Protection for BYOD. In *Proceedings of the Annual Research Conference on South African Institute of Computer Scientists and Information Technologists (SAICSIT)*, pages 1–6, 2015.
- [86] Christian Jandl, Jamilya Nurgazina, Lucas Schöffner, Christian Reichl, Markus Wagner, and Thomas Moser. SensiTrack - A Privacy by Design Concept for Industrial IoT Applications. In *Proceedings of the 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*, pages 1782–1789, 2019.
- [87] Paul A. Karger. Privacy and Security Threat Analysis of the Federal Employee Personal Identity Verification (PIV) Program. In *Proceedings of the 2nd Symposium on Usable Privacy and Security (SOUPS)*, pages 114–121, 2006.
- [88] Jinhyung Kim and Hyung Jong Kim. A Study on Privacy Preserving Data Leakage Prevention System. In Ford Lumban Gaol, editor, *Recent Progress in Data Engineering and Internet Technology*, pages 191–196. Springer, 2012.
- [89] Stan Kurkovsky, Ewa Syta, and Bernardo Casano. Continuous RFID-enabled Authentication and Its Privacy Implications. In *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*, pages 103–110, 2010.
- [90] Dominik Lucke, Engelbert Westkamper, Mike Eissele, Thomas Ertl, and Oliver Siemoneit. Privacy-Preserving Self-Localization Techniques in next Generation Manufacturing: An Interdisciplinary View on the Vision and Implementation of Smart Factories. In *Proceedings of the 10th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, pages 1183–1188, 2008.
- [91] Moritz Christian Müller. Preserving Privacy in Production. In *Proceedings of the 8th IFIP International Summer School on Privacy and Identity Management*, pages 177–187, 2014.
- [92] Felix Mannhardt, Sobah Abbas Petersen, and Manuel Fradinho Oliveira. Privacy Challenges for Process Mining in Human-Centered Industrial Environments. In *Proceedings of the 14th International Conference on Intelligent Environments (IE)*, pages 64–71, 2018.
- [93] Marleen Voss, Mark Hoebertz, Olga Bosak, Felix Mohsenzadeh, Maximilian Schnebbe, Jens Poeppelbuss, and Maik Eisenbeiss. Privacy-Centered Design Principles for Employee-Determined Data Collection and Use in Personalized Assistance Systems. In *Proceedings of the 27th Americas' Conference on Information Systems (AMCIS)*, pages 1–10, 2021.
- [94] Maedeh Yassaee. Design Principles for Digital Occupational Health Systems. In *Proceedings of the 20th International Conference on Business Information Systems (BIS)*, pages 16–27, 2017.

- [95] Emanuel Gonçalves, Paulo Teixeira, and Joaquim P. Silva. Development of GDPR-Compliant Software: Document Management System for HR Department. In *Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI)*, pages 1–6, 2020.
- [96] Svenja Polst, Patricia Kelbert, and Denis Feth. Company Privacy Dashboards: Employee Needs and Requirements. In *Proceedings of the 1st International Conference on Human-Computer Interaction for Cybersecurity, Privacy and Trust (HCI-CPT)*, pages 429–440, 2019.
- [97] Waliyah Sahqani and Luca Turchet. Co-Designing Employees’ Data Privacy: A Technology Consultancy Company Use Case. In *Proceedings of the 28th Conference of Open Innovations Association (FRUCT)*, pages 398–406, 2021.
- [98] Carolyn Brodie, Clare-Marie Karat, John Karat, and Jinjuan Feng. Usable Security and Privacy: A Case Study of Developing Privacy Management Tools. In *Proceedings of the 1st Symposium on Usable Privacy and Security (SOUPS)*, pages 35–43, 2005.
- [99] ISO/IEC JTC 1/SC 27. *ISO/IEC 27701:2019 Extension to ISO/IEC 27001 and ISO/IEC 27002 for Privacy Information Management –Requirements and Guidelines*. International Organization for Standardization, 2019. URL <https://www.iso.org/standard/71670.html>.
- [100] Jan Tolsdorf and Florian 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.
- [101] 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. *Proceedings on Privacy Enhancing Technologies*, 2021(3):5–27, 2021.
- [102] Jan Tolsdorf, Delphine Reinhardt, and Luigi Lo Iacono. Employees’ Privacy Perceptions: Exploring the Dimensionality and Antecedents of Personal Data Sensitivity and Willingness to Disclose. *Proceedings on Privacy Enhancing Technologies*, 2022(2): 68–94, 2022.
- [103] Jan Tolsdorf, Florian Dehling, and Luigi Lo Iacono. Data Cart – Designing a Tool for the GDPR-compliant Handling of Personal Data by Employees. *Behaviour & Information Technology*, 41(10):2070–2105, 2022.
- [104] Florian Dehling, Denis Feth, Svenja Polst, Bianca Steffes, and Jan Tolsdorf. Components and Architecture for the Implementation of Technology-driven Employee Data Protection. In *Proceedings of the 18th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*, 12927, pages 99–111, 2021.
- [105] Jan Tolsdorf, Christian K. Bosse, Aljoscha Dietrich, Denis Feth, and Hartmut Schmitt. Privatheit am Arbeitsplatz - Transparenz und Selbstbestimmung bei Arbeit 4.0. *Datenschutz und Datensicherheit*, 44(3):176–181, 2020.
- [106] Jan Tolsdorf, Florian Dehling, and Denis Feth. Benutzerfreundlicher Datenschutz in Cloud-basierten Office-Paketen. *Datenschutz und Datensicherheit*, 45(1):33–39, 2021.

- [107] Jan Tolsdorf, Florian Dehling, and Luigi Lo Iacono. Take Back Control! The Use of Mental Models to Develop Privacy Dashboards. *ITG News*, 8(3):15–20, 2020.
- [108] Jan Tolsdorf, Michael Fischer, and Luigi Lo Iacono. A Case Study on the Implementation of the Right of Access in Privacy Dashboards. In *Proceedings of the 9th Annual Privacy Forum (APF)*, pages 23–46, 2021.
- [109] Christian K. Bosse, Aljoscha Dietrich, Patricia Kelbert, Hagen Kuchler, Hartmut Schmitt, Jan Tolsdorf, and Andreas Weßner. Beschäftigtendatenschutz: Rechtliche Anforderungen und Technische Lösungskonzepte. In *Proceedings of the 23rd Internationalen Rechtsinformatik Symposions (IRIS)*, pages 1–8, 2020.
- [110] Svenja Polst, Jan Tolsdorf, Florian Dehling, and Denis Feth. Verarbeitung von Beschäftigtendaten. *Datenschutz und Datensicherheit*, 45(1):19–22, 2021.
- [111] Stephan Wiefeling, Jan Tolsdorf, and Luigi Lo Iacono. Privacy Considerations for Risk-based Authentication Systems. In *Proceedings of the 7th IEEE International Workshop on Privacy Engineering (IWPE)*, pages 320–327, 2021.
- [112] France Bélanger and Robert E. Crossler. Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4):1017–1042, 2011.
- [113] H. Jeff Smith, Tamara Dinev, and Heng Xu. Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, 35(4):989–1016, 2011.
- [114] Heng Xu, Tamara Dinev, Jeff Smith, and Paul Hart. Information Privacy Concerns: Linking Individual Perceptions with Institutional Privacy Assurances. *Journal of the Association for Information Systems*, 12(12):798–824, 2011.
- [115] Haejung Yun, Gwanhoo Lee, and Dan J. Kim. A Meta-Analytic Review of Empirical Research on Online Information Privacy Concerns: Antecedents, Outcomes, and Moderators. In *Proceedings of the 14th International Conference on Security and Privacy (ICIS)*, pages 1–13, 2014.
- [116] Haejung Yun, Gwanhoo Lee, and Dan J Kim. A Chronological Review of Empirical Research on Personal Information Privacy Concerns: An Analysis of Contexts and Research Constructs. *Information & Management*, 56(4):570–601, 2019.
- [117] Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano. Introduction and Overview. In Bart P. Knijnenburg, Xinru Page, Pamela Wisniewski, Heather Richter Lipford, Nicholas Proferes, and Jennifer Romano, editors, *Modern Socio-Technical Perspectives on Privacy*, pages 1–11. Springer, 2022.
- [118] Kirstie Ball, Elizabeth M. Daniel, and Chris Stride. Dimensions of Employee Privacy: An Empirical Study. *Information Technology & People*, 25(4):376–394, 2012.
- [119] Stephen T. Margulis. On the Status and Contribution of Westin’s and Altman’s Theories of Privacy. *Journal of Social Issues*, 59(2):411–429, 2003.
- [120] Irwin Altman. *The Environment and Social Behavior: Privacy, Personal Space, Territory, Crowding*. Brooks/Cole Pub. Co, 1975.

- [121] Irwin Altman. Privacy Regulation: Culturally Universal or Culturally Specific? *Journal of Social Issues*, 33(3):66–84, 1977.
- [122] Marylène Gagné and Devasheesh Bhave. Autonomy in the Workplace: An Essential Ingredient to Employee Engagement and Well-Being in Every Culture. In Valery I. Chirkov, Richard M. Ryan, and Kennon M. Sheldon, editors, *Human Autonomy in Cross-Cultural Context: Perspectives on the Psychology of Agency, Freedom, and Well-Being*, Cross-Cultural Advancements in Positive Psychology, pages 163–187. Springer, 2011.
- [123] Alan Furman Westin. *Privacy and Freedom*. Athenum Press, 1967.
- [124] Samuel D. Warren and Louis D. Brandeis. The Right to Privacy. *Harvard Law Review*, 4(5):193–220, 1890.
- [125] Xiaogang Chen, Jing Ma, Jiafei Jin, and Patricia Fosh. Information Privacy, Gender Differences, and Intrinsic Motivation in the Workplace. *International Journal of Information Management*, 33(6):917–926, 2013.
- [126] Sandra Petronio. *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press, 2002.
- [127] Stephanie A. Smith and Steven 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.
- [128] Human Rights Council United Nations. General Assembly Resolution 42/15, The Right to Privacy in the Digital Age, A/HRC/RES/42/15, 2019.
- [129] Willis Ware. Records, Computers and the Rights of Citizens Report of the Secretary’s Advisory Committee on Automated Personal Data Systems. Technical report, U.S. Department of Health, Education and Welfare, 1973. URL <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.
- [130] Kenneth G. Younger (Chairman). Report of the Committee on Privacy. Technical report, Great Britain. Home Office, 1972. URL <https://discovery.nationalarchives.gov.uk/details/r/C14466146>.
- [131] Robert Gellman. Fair Information Practices: A Basic History. Technical Report Version 2.21, 2021. URL <https://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf>.
- [132] David Wright and Paul De Hert, editors. *Enforcing Privacy - Regulatory, Legal and Technological Approaches*, volume 25. Springer, 2016.
- [133] European Union. General Data Protection Regulation. 2016. Regulation (EU) 2016/679.
- [134] State of California. California Privacy Rights Act of 2020. 2020.
- [135] Federative Republic of Brazil. General Personal Data Protection Law 13709/2018. 2018.

- [136] Personal Information Protection Commission Japan. Amended Act on the Protection of Personal Information. 2020.
- [137] European Commission. EU Member States notifications to the European Commission under the GDPR. URL [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en).
- [138] Hans D. Jarass, Martin Kment, and Bodo Pieroth. *Grundgesetz Für Die Bundesrepublik Deutschland*. C.H.Beck, 16th edition, 2020.
- [139] Ulf Buermeyer. *Informationelle Selbstbestimmung und effektiver Rechtsschutz im Strafvollzug: Verwirklichungsbedingungen von Datenschutz und Informationsrechten im Vollzug von Freiheitsentziehungen*. Nomos Verlagsgesellschaft mbH & Co. KG, 2019.
- [140] Claus Dieter Classen. Das Prinzip Der Verhältnismäßigkeit Im Spiegel Europäischer Rechtsentwicklungen. In Michael Sachs and Helmut Siekmann, editors, *Der Grundrechtsgeprägte Verfassungsstaat. Festschrift Für Klaus Stern Zum 80. Geburtstag*. Duncker & Humblot, 2012.
- [141] Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder am 3. April 2019, 2019. URL [https://www.datenschutzkonferenz-online.de/media/en/20190405\\_Entschliessung\\_Unternehmenshaftung.pdf](https://www.datenschutzkonferenz-online.de/media/en/20190405_Entschliessung_Unternehmenshaftung.pdf).
- [142] Paul M. Schwartz and Daniel J. Solove. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, 86(6):1814–1894, 2011.
- [143] ISO/IEC JTC 1/SC 27. *ISO/IEC 29100:2011: Information Technology —Security Techniques —Privacy Framework*. International Organization for Standardization, 2011. URL <https://www.iso.org/standard/45123.html>.
- [144] Erika McCallister, Tim Grance, and Karen Scarfone. Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). Technical Report 800-122, Nist, 2010. URL <https://doi.org/10.6028/NIST.SP.800-122>.
- [145] Paul M. Schwartz and Daniel J. Solove. Reconciling Personal Information in the United States and European Union. *California Law Review*, 102:877–916, 2014.
- [146] ISO/IEC JTC 1/SC 27. *ISO/IEC 29101:2018: Information Technology —Security Techniques —Privacy Architecture Framework*. International Organization for Standardization, 2nd edition, 2018. URL <https://www.iso.org/standard/75293.html>.
- [147] Article 29 Data Protection Working Party. Opinion 2/2017 on Data Processing at Work (WP249), 2017. URL <https://ec.europa.eu/newsroom/article29/items/610169/en>.
- [148] Stephan Weth, Maximilian Herberger, Michael Wächter, and Christoph Sorge, editors. *Daten- und Persönlichkeitsschutz im Arbeitsverhältnis*. C.H. Beck, 2nd edition, 2019.



- [149] Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, Stefan Schiffner, George Danezis, European Union, and European Network and Information Security Agency. Privacy and Data Protection by Design - from Policy to Engineering. Report, European Union Agency for Cybersecurity (ENISA), 2014. URL <https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design>.
- [150] Marit Hansen, Meiko Jensen, and Martin Rost. Protection Goals for Privacy Engineering. In *Proceedings of the IEEE Security and Privacy Workshops (SPW)*, pages 159–166, 2015.
- [151] Ann Cavoukian. Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices. Brochure, Information and Privacy Commissioner of Ontario Canada, 2011. URL <https://iapp.org/resources/article/privacy-by-design-the-7-foundational-principles/>.
- [152] Resolution on Privacy by Design. Technical report, 32nd International Conference of Data Protection and Privacy Commissioners, 2010. URL <https://globalprivacyassembly.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf>.
- [153] European Data Protection Supervisor (EDPS). Opinion 5/2018 Preliminary Opinion on Privacy by Design, 2018. URL [https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design\\_en](https://edps.europa.eu/data-protection/our-work/publications/opinions/privacy-design_en).
- [154] Luke Stark, Jen King, Xinru Page, Airi Lampinen, Jessica Vitak, Pamela Wisniewski, Tara Whalen, and Nathaniel Good. Bridging the Gap Between Privacy by Design and Privacy in Practice. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA)*, page 3415–3422, 2016.
- [155] ISO/IEC JTC 1/SC 7. *ISO/IEC/IEEE 15288:2015: Systems and Software Engineering –System Life Cycle Processes*. IEEE, 1st edition, 2015. URL <https://www.iso.org/standard/63711.html>.
- [156] Michael Colesky, Jaap-Henk Hoepman, Christoph Boesch, Frank Kargl, Henning Kopp, Patrick Mosby, Daniel Le Métayer, Olha Drozd, José M. del Álamo, Yod Samuel Martín, Julio C. Caiza, Mohit Gupta, and Nick Doty. Privacy Patterns. <https://www.privacypatterns.org/>. last visited: March 16, 2022.
- [157] ISO/IEC JTC 1/SC 27. *ISO/IEC 29134:2017: Information Technology —Security Techniques —Guidelines for Privacy Impact Assessment*. International Organization for Standardization, 1st edition, 2017. URL <https://www.iso.org/standard/62289.html>.
- [158] Michael Colesky, Jaap-Henk Hoepman, and Christiaan Hillen. A Critical Analysis of Privacy Design Strategies. In *Proceedings of the IEEE Security and Privacy Workshops (SPW)*, pages 33–40, 2016.
- [159] Jaap-Henk Hoepman. Privacy Design Strategies. In *Proceedings of the 29th IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*, pages 446–459, 2014.

- [160] Simone Fischer-Hübner and Stefan Berthold. Privacy-Enhancing Technologies. In *Computer and Information Security Handbook*, pages 759–778. Elsevier, 2017.
- [161] Yun Shen and Siani Pearson. Privacy Enhancing Technologies: A Review. Technical Report HPL-2011-113, HP Laboratories, 2011. URL <https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf>.
- [162] Milena Janic, Jan Pieter Wijnnga, and Thijs Veugen. Transparency Enhancing Tools (TETs): An Overview. In *Proceedings of the 3rd Workshop on Socio-Technical Aspects in Security and Trust (STAST)*, pages 18–25, 2013.
- [163] Patrick Murmann and Simone Fischer-Hübner. Tools for Achieving Usable Ex Post Transparency: A Survey. *IEEE Access*, 5:22965–22991, 2017.
- [164] David Goldschlag, Michael Reed, and Paul Syverson. Onion Routing. *Communications of the ACM*, 42(2):39–41, 1999.
- [165] Latanya Sweeney. K-Anonymity: A Model for Protecting Privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(5):557–570, 2002.
- [166] Cynthia Dwork. Differential Privacy. In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, pages 1–12, 2006.
- [167] Sabrina Kirrane, Javier D. Fernández, Wouter Dullaert, Uros Milosevic, Axel Polleres, Piero A. Bonatti, Rigo Wenning, Olha Drozd, and Philip Raschke. A Scalable Consent, Transparency and Compliance Architecture. In *Proceedings of the Satellite Events of the 15th Extended Semantic Web Conference (ESWC Satellite Events)*, pages 131–136, 2018.
- [168] Johannes Heurix, Peter Zimmermann, Thomas Neubauer, and Stefan Fenz. A Taxonomy for Privacy Enhancing Technologies. *Computers & Security*, 53:1–17, 2015.
- [169] Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design Patterns: Elements of Reusable Object-Oriented Software*. Addison-Wesley, 1995.
- [170] Frank Buschmann, Regine Meunier, Hans Rohnert, Peter Sommerlad, and Michael Stal. *Pattern-Oriented Software Architecture - A System of Patterns*, volume 1. Wiley, 1996.
- [171] Julio C. Caiza, Yod-Samuel Martín, Jose M. Del Alamo, and Danny S. Guamán. Organizing Design Patterns for Privacy: A Taxonomy of Types of Relationships. In *Proceedings of the 22nd European Conference on Pattern Languages of Programs (EuroPLoP)*, pages 1–11, 2017.
- [172] Joseph Yoder and Jeffrey Barcalow. Architectural Patterns for Enabling Application Security. In *Proceedings of the 4th Conference on Patterns Language of Programming (PLoP)*, pages 1–31, 1997.
- [173] Sasha Romanosky, Alessandro Acquisti, Jason Hong, Lorrie Faith Cranor, and Batya Friedman. Privacy Patterns for Online Interactions. In *Proceedings of the 13th Conference on Pattern Languages of Programs (PLoP)*, pages 1–9, 2006.

- [174] Markus Schumacher. Patterns and Security Standards —With Selected Security Patterns for Anonymity and Privacy. In *Proceedings of the 8th European Conference on Pattern Languages of Programms (EuroPLoP)*, pages 1–11, 2003.
- [175] Alexander Gabel and Ina Schiering. Privacy Patterns for Pseudonymity. In *Proceedings of the 13th IFIP International Summer School on Privacy and Identity Management*, pages 155–172, 2019.
- [176] Munawar Hafiz. A Pattern Language for Developing Privacy Enhancing Technologies. *Software: Practice and Experience*, 43(7):769–787, 2013.
- [177] Nick Doty and Mohit Gupta. Privacy Design Patterns and Anti-Patterns - Patterns Misapplied and Unintended Consequences. In *Proceedings of the 1st Trustbusters for User Interfaces Workshop*, pages 1–5, 2013.
- [178] Simone Fischer-Hübner, Christina Köffel, John Sören Pettersson, Peter Wolkerstorfer, Cornelia Graf, Leif Erik Holtz, Ulrich König, Hans Hedbom, and Benjamin Kellermann. HCI Pattern Collection – Version 2. Deliverable D4.1.3, PrimeLife, 2010. URL [https://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci\\_pattern\\_collection\\_v2-public.pdf](https://primelife.ercim.eu/images/stories/deliverables/d4.1.3-hci_pattern_collection_v2-public.pdf).
- [179] Cornelia Graf, Peter Wolkerstorfer, Arjan Geven, and Manfred Tscheligi. A Pattern Collection for Privacy Enhancing Technology. In *Proceedings of the 2nd International Conferences on Pervasive Patterns and Applications (PATTERNS)*, pages 21–16, 2010.
- [180] Johanneke Siljee. Privacy Transparency Patterns. In *Proceedings of the 20th European Conference on Pattern Languages of Programs (EuroPLoP)*, pages 1–11, 2015.
- [181] Maha Aljohani, James Blustein, and Kirstie Hawkey. Toward Applying Online Privacy Patterns Based on the Design Problem: A Systematic Review. In *Proceedings of the 7th International Conference on Design, User Experience, and Usability (DUXU)*, pages 608–627, 2018.
- [182] Manos Papoutsakis, Konstantinos Fysarakis, George Spanoudakis, Sotiris Ioannidis, and Konstantina Koloutsou. Towards a Collection of Security and Privacy Patterns. *Applied Sciences*, 11(4):1396, 2021.
- [183] Olha Drozd. Privacy Pattern Catalogue: A Tool for Integrating Privacy Principles of ISO/IEC 29100 into the Software Development Process. In *Proceedings of the 10th IFIP International Summer School on Privacy and Identity Management*, pages 129–140, 2016.
- [184] Michael Colesky and Julio C. Caiza. A System of Privacy Patterns for Informing Users: Creating a Pattern System. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs (EuroPLoP)*, pages 1–11, 2018.
- [185] Michael Colesky, Julio C. Caiza, José M. Del Álamo, Jaap-Henk Hoepman, and Yod-Samuel Martín. A System of Privacy Patterns for User Control. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing (SAC)*, pages 1150–1156, 2018.

- [186] Simone Agostinelli, Fabrizio Maria Maggi, Andrea Marrella, and Francesco Sapia. Achieving GDPR Compliance of BPMN Process Models. In *Proceedings of the CAiSE Forum as part of the 31st International Conference on Advanced Information Systems Engineering (CAiSE Forum)*, pages 10–22, 2019.
- [187] Maha Aljohani, Kirstie Hawkey, and James Blustein. Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia’s Personal Health Information Act. In *Proceedings of the 4th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)*, pages 91–102, 2016.
- [188] Masoud Barati and Omer Rana. Design and Verification of Privacy Patterns for Business Process Models. In Srikanta Patnaik, Tao-Sheng Wang, Tao Shen, and Sushanta Kumar Panigrahi, editors, *Blockchain Technology and Innovations in Business Processes*, pages 125–139. Springer, 2021.
- [189] Erik Buchmann and Jürgen Anke. Privacy Patterns in Business Processes. In *Proceedings of the 47th Jahrestagung der Gesellschaft für Informatik (INFORMATIK)*, pages 793–798, 2017.
- [190] Maria Dias Coelho, André Vasconcelos, and Pedro Sousa. Privacy by Design Enterprise Architecture Patterns. In *Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS)*, pages 743–750, 2021.
- [191] Marcin Robak and Erik Buchmann. How to Extract Workflow Privacy Patterns from Legal Documents. In Ewa Ziemba, editor, *Information Technology for Management: Current Research and Future Directions*, pages 214–234. Springer, 2020.
- [192] Gaëlle Blanco-Lainé, Jean-Sébastien Sottet, and Sophie Dupuy-Chessa. Using an Enterprise Architecture Model for GDPR Compliance Principles. In *Proceedings of the 12th IFIP Working Conference on the Practice of Enterprise Modeling (PoEM)*, pages 199–214, 2019.
- [193] Andy Dearden and Janet Finlay. Pattern Languages in HCI: A Critical Review. *Human–Computer Interaction*, 21(1):49–102, 2006.
- [194] Stefan L. Pauwels, Christian Hübscher, Javier A. Bargas-Avila, and Klaus Opwis. Building an Interaction Design Pattern Language: A Case Study. *Computers in Human Behavior*, 26(3):452–463, 2010.
- [195] Deirdre K Mulligan and Jennifer King. Bridging The Gap Between Privacy And Design. *University of Pennsylvania Journal of Constitutional Law*, 14(4):1–46, 2012.
- [196] Richmond Y. Wong and Deirdre K. Mulligan. Bringing Design to the Privacy Table: Broadening “Design” in “Privacy by Design” Through the Lens of HCI. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–17, May 4 - 9, 2019.
- [197] Dayana Spagnuolo, Ana Ferreira, and Gabriele Lenzini. Transparency Enhancing Tools and the GDPR: Do They Match? In *Proceedings of the International Conference on Information Systems Security and Privacy (ICISSP)*, pages 162–185, 2020.

- [198] Johanna Johansen and Simone Fischer-Hübner. Making GDPR Usable: A Model to Support Usability Evaluations of Privacy. In *Proceedings of the 14th IFIP International Summer School on Privacy and Identity Management*, pages 275–291, 2020.
- [199] Oshrat Ayalon and Eran Toch. User-Centered Privacy-by-Design: Evaluating the Appropriateness of Design Prototypes. *International Journal of Human-Computer Studies*, 154:102641, 2021.
- [200] Clay Spinuzzi. The Methodology of Participatory Design. *Technical Communication*, 52:163–174, 2005.
- [201] Donald A. Norman. *The Psychology of Everyday Things*. Basic Books, 1988.
- [202] Chadia Abras, Diane Maloney-Krichmar, and Jenny Preece. User-Centered Design. In William S. Bainbridge, editor, *Encyclopedia of Human-Computer Interaction*, pages 763–768. Berkshire Publishing Group, 1st edition, 2004.
- [203] Martin Maguire and Nigel Bevan. User Requirements Analysis: A Review of Supporting Methods. In *Proceedings of the 17th IFIP World Computer Congress*, pages 133–148, 2002.
- [204] Florian Mathis, Kami Vaniea, and Mohamed Khamis. Prototyping Usable Privacy and Security Systems: Insights from Experts. *International Journal of Human-Computer Interaction*, 38(5):468–490, 2021.
- [205] Chauncey Wilson. *User Interface Inspection Methods: A User-Centered Design Method*. Morgan Kaufmann Publishers Inc., 2013.
- [206] Farzaneh Karegar, Tobias Pulls, and Simone Fischer-Hübner. Visualizing Exports of Personal Data by Exercising the Right of Data Portability in the Data Track - Are People Ready for This? In *Proceedings of the 11th IFIP International Summer School on Privacy and Identity Management*, pages 164–181, 2016.
- [207] Marija Schufrin, Steven Lamarr Reynolds, Arjan Kuijper, and Jörn Kohlhammer. A Visualization Interface to Improve the Transparency of Collected Personal Data on the Internet. *IEEE Transactions on Visualization and Computer Graphics*, 27(2):1840–1849, 2021.
- [208] Sophie Veys, Daniel Serrano, Madison Stamos, Margot Herman, Nathan Reitering, Michelle L. Mazurek, and Blase Ur. Pursuing Usable and Useful Data Downloads Under GDPR/CCPA Access Rights via Co-Design. In *Proceedings of the 17th Symposium on Usable Privacy and Security (SOUPS)*, pages 217–242, 2021.
- [209] Olha Drozd and Sabrina Kirrane. Privacy CURE: Consent Comprehension Made Easy. In *Proceedings of the 35th IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*, 2020.
- [210] Dominique Machuletz and Rainer Böhme. Multiple Purposes, Multiple Problems: A User Study of Consent Dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies*, 2020(2):481–498, 2020.

- [211] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. (Un)Informed Consent: Studying GDPR Consent Notices in the Field. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 973–990, 2019.
- [212] Midas Nouwens, Ilaria Liccardi, Michael Veale, David Karger, and Lalana Kagal. Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1–13, 2020.
- [213] Fatemeh Alizadeh, Timo Jakobi, Alexander Boden, Gunnar Stevens, and Jens Boldt. GDPR Reality Check - Claiming and Investigating Personally Identifiable Data from Companies. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 120–129, 2020.
- [214] Wanda Presthus and Hanne Sørsum. Consumer Perspectives on Information Privacy Following the Implementation of the GDPR. *International Journal of Information Systems and Project Management*, 7(3):19–34, 2019.
- [215] Christoph Bier, Kay Kühne, and Jürgen Beyerer. PrivacyInsight: The Next Generation Privacy Dashboard. In *Proceedings of the 4th Annual Privacy Forum (APF)*, pages 135–152, 2016.
- [216] Patrick Murmann, Delphine Reinhardt, and Simone Fischer-Hübner. To Be, or Not to Be Notified: Eliciting Privacy Notification Preferences for Online mHealth Services. In *Proceedings of the 34th IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*, pages 99–114, 2019.
- [217] Natalie Jones, Helen Ross, Timothy Lynam, Pascal Perez, and Anne Leitch. Mental Models: An Interdisciplinary Synthesis of Theory and Methods. *Ecology and Society*, 16(1), 2011.
- [218] K. J. W. Craik. *The Nature of Explanation*. Cambridge: Cambridge University Press, 1943.
- [219] Allan Collins and Dedre Gentner. How people construct mental models. In Dorothy Holland and Naomi Quinn, editors, *Cultural Models in Language and Thought*, pages 243–266. Cambridge University Press, 1987.
- [220] D. A. Norman. Some observations on mental models. In D. Gentner and A. L. Stevens, editors, *Mental Models*, pages 7–14. Lawrence Erlbaum Associates Inc., 1983.
- [221] Philip N. Johnson-Laird. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness*. Harvard University Press, 1986.
- [222] Stephen J. Payne. Mental Models in Human-Computer Interaction. In Andrew Sears and Julie A. Jacko, editors, *The Human-Computer Interaction Handbook : Fundamentals, Evolving Technologies and Emerging Applications*, page 14. CRC Press LLC, 2nd edition, 2007.



- [223] Melanie Volkamer and Karen Renaud. Mental Models –General Introduction and Review of Their Application to Human-Centred Security. In Marc Fischlin and Stefan Katzenbeisser, editors, *Number Theory and Cryptography: Papers in Honor of Johannes Buchmann on the Occasion of His 60th Birthday*, pages 255–280. Springer, 2013.
- [224] Alessandro Acquisti and Jens Grossklags. Privacy and Rationality in Individual Decision Making. *IEEE Security and Privacy*, 3(1):26–33, 2005.
- [225] Eva-Maria Schomakers, Chantal Lidynia, and Martina 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 (IoT BDS)*, pages 85–94, 2018.
- [226] Cristian Bravo-Lillo, Lorrie Faith Cranor, Julie Downs, and Saranga Komanduri. Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *IEEE Security and Privacy Magazine*, 9(2):18–26, 2011.
- [227] Fahimeh Raja, Kirstie Hawkey, and Konstantin Beznosov. Revealing Hidden Context: Improving Mental Models of Personal Firewall Users. In *Proceedings of the 5th Symposium on Usable Privacy and Security (SOUPS)*, pages 1–12, 2009.
- [228] Rick Wash. Folk Models of Home Computer Security. In *Proceedings of the 6th Symposium on Usable Privacy and Security (SOUPS)*, pages 1–16, 2010.
- [229] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel 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 (SP)*, pages 246–263, 2019.
- [230] Erik Wästlund, Julio Angulo, and Simone Fischer-Hübner. Evoking Comprehensive Mental Models of Anonymous Credentials. In *Proceedings of the IFIP International Workshop on Open Problems in Network Security (iNetSec)*, pages 1–14, 2011.
- [231] Karen Renaud, Melanie Volkamer, and Arne Renkema-Padmos. Why Doesn’t Jane Protect Her Privacy? In *Proceedings of the 14th International Privacy Enhancing Technologies Symposium (PETS)*, pages 244–262, 2014.
- [232] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. “My Data Just Goes Everywhere:” User Mental Models of the Internet and Implications for Privacy and Security. In *Proceedings of the 11th Symposium On Usable Privacy and Security (SOUPS)*, pages 39–52, 2015.
- [233] Eric Zeng, Shrirang Mare, and Franziska Roesner. End User Security and Privacy Concerns with Smart Homes. In *Proceedings of the 13th Symposium on Usable Privacy and Security (SOUPS)*, pages 65–80, 2017.
- [234] Kelsey R. Fulton, Rebecca Gelles, Alexandra McKay, Richard Roberts, Yasmin Abdi, and Michelle L. Mazurek. The Effect of Entertainment Media on Mental Models of Computer Security. In *Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS)*, pages 79–95, 2019.

- [235] Nina Gerber, Verena Zimmermann, and Melanie Volkamer. Why Johnny Fails to Protect his Privacy. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 109–118, 2019.
- [236] Monica Maceli. Librarians’ Mental Models and Use of Privacy-Protection Technologies. *Journal of Intellectual Freedom & Privacy*, 4(1):18–32, 2019.
- [237] Maggie Oates, Yama Ahmadullah, Abigail Marsh, Chelse Swoopes, Shikun Zhang, Rebecca Balebako, and Lorrie Faith Cranor. Turtles, Locks, and Bathrooms: Understanding Mental Models of Privacy Through Illustration. *Proceedings on Privacy Enhancing Technologies*, 2018(4):5–32, 2018.
- [238] Sandra Spickard Prettyman, Susanne Furman, Mary Theofanos, and Brian 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.
- [239] Priya Kumar, Shalmali Milind Naik, Utkarsha Ramesh Devkar, Marshini Chetty, Tamara L. Clegg, and Jessica 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):64:1–64:21, 2017.
- [240] L. Jean Camp. Mental Models of Privacy and Security. *IEEE Technology and Society Magazine*, 28(3):37–46, 2009.
- [241] Jialiu Lin, Norman Sadeh, Shahriyar Amini, Janne Lindqvist, Jason I. Hong, and Joy Zhang. Expectation and Purpose: Understanding Users’ Mental Models of Mobile App Privacy through Crowdsourcing. In *Proceedings of the ACM Conference on Ubiquitous Computing (UbiComp)*, pages 501–510, 2012.
- [242] Alessandro Acquisti, Curtis R. Taylor, and Liad Wagman. The Economics of Privacy. *Journal of Economic Literature*, 52(2):442–492, 2016.
- [243] Mary J. Culnan and Pamela K. Armstrong. Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, 10(1):104–115, 1999.
- [244] Tamara Dinev and Paul Hart. An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, 17(1):61–80, 2006.
- [245] Tamara Dinev, Heng Xu, Jeff H Smith, and Paul Hart. Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. *European Journal of Information Systems*, 22(3):295–316, 2013.
- [246] David L. Mothersbaugh, William K. Foxx, Sharon E. Beatty, and Sijun Wang. Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information. *Journal of Service Research*, 15(1):76–98, 2012.
- [247] Yuan Li. Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, 28:453–496, 2011.

- [248] Kirsten E. M. Martin and Helen Nissenbaum. Measuring Privacy: An Empirical Test Using Context To Expose Confounding Variables. *Columbia Science and Technology Law Review*, 18:176–218, 2015.
- [249] Icek Ajzen and Martin Fishbein. *Understanding Attitudes and Predicting Social Behavior*. Prentice-Hall, 1980.
- [250] Tobias Dienlin and Sabine Trepte. Is the Privacy Paradox a Relic of the Past? An in-Depth Analysis of Privacy Attitudes and Privacy Behaviors. *European Journal of Social Psychology*, 45(3):285–297, 2015.
- [251] Bart P. Knijnenburg, Alfred Kobsa, and Hongxia Jin. Dimensionality of Information Disclosure Behavior. *International Journal of Human-Computer Studies*, 71(12):1144–1162, 2013.
- [252] Sandra Gabriele and Sonia Chiasson. Understanding Fitness Tracker Users’ Security and Privacy Knowledge, Attitudes and Behaviours. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, page 1–12, 2020.
- [253] Hsiao-Ying Huang and Masooda Bashir. Privacy by Region: Evaluation Online Users’ Privacy Perceptions by Geographical Region. In *Proceedings of the Future Technologies Conference (FTC)*, pages 968–977, 2016.
- [254] Insu Park. The Study on the Relationship Between Privacy Concerns and Information Systems Effectiveness. In *Proceedings of the 30th International Conference on Information Systems (ICIS)*, pages 1–20, 2009.
- [255] Naresh K. Malhotra, Sung S Kim, and James Agarwal. Internet Users’ Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, 15(4):336–355, 2004.
- [256] H. Jeff Smith, Sandra J. Milberg, and Sandra J. Burke. Information Privacy: Measuring Individuals’ Concerns about Organizational Practices. *MIS Quarterly*, 20(2):167–196, 1996.
- [257] Tom Buchanan, Carina Paine, Adam N. Joinson, and Ulf-Dietrich Reips. Development of Measures of Online Privacy Concern and Protection for Use on the Internet. *Journal of the American Society for Information Science and Technology*, 58(2):157–165, 2007.
- [258] Wei Yin Hong and James Y. L. Thong. Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, 37(1):275–298, 2013.
- [259] Mena Teebken and Thomas Hess. Privacy in a Digitized Workplace: Towards an Understanding of Employee Privacy Concerns. In *Proceedings of the 54th Hawaii International Conference on System Sciences (HICSS)*, pages 6661–6670, 2021.
- [260] Heng Xu, Tamara Dinev, H Jeff Smith, and Paul Hart. Examining the Formation of Individual’s Privacy Concerns: Toward an Integrative View. In *Proceedings of the 29th International Conference on Information Systems (ICIS)*, pages 1–16, 2008.

- [261] Spyros Kokolakis. Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon. *Computers & Security*, 64:122–134, 2017.
- [262] Nina Gerber, Paul Gerber, and Melanie Volkamer. Explaining the Privacy Paradox: A Systematic Review of Literature Investigating Privacy Attitude and Behavior. *Computers & Security*, 77(8):226–261, 2018.
- [263] José Luis Gómez-Barroso. Experiments on Personal Information Disclosure: Past and Future Avenues. *Telematics and Informatics*, 35(5):1473–1490, 2018.
- [264] Tamara Dinev, Allen R. McConnell, and H. Jeff Smith. Research Commentary—Informing Privacy Research Through Information Systems, Psychology, and Behavioral Economics: Thinking Outside the “APCO” Box. *Information Systems Research*, 26(4):639–655, 2015.
- [265] Mena Angela Teebken. What Makes Workplace Privacy Special? An Investigation of Determinants of Privacy Concerns in the Digital Workplace. In *Proceedings of the 27th Americas’ Conference on Information Systems (AMCIS)*, pages 1–10, 2021.
- [266] Maren Gierlich-Joas, Mena Teebken, and Thomas Hess. A Synthesized Perspective on Privacy and Transparency in the Digital Workplace. In *Proceedings of the 55th Hawaii International Conference on System Sciences (HICSS)*, pages 5191–5200, 2022.
- [267] Jane Webster and Richard T. Watson. Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, 26(2):xiii–xxiii, 2002.
- [268] Verena Distler, Matthias Fassl, Hana Habib, Katharina Krombholz, Gabriele Lenzini, Carine Lallemand, Lorrie Faith Cranor, and Vincent Koenig. A Systematic Literature Review of Empirical Methods and Risk Representation in Usable Privacy and Security Research. *ACM Transactions on Computer-Human Interaction*, 28(6):1–50, 2021.
- [269] Jošt Bartol, Vasja Vehovar, and Andraž Petrovčič. Should We Be Concerned about How Information Privacy Concerns Are Measured in Online Contexts? A Systematic Review of Survey Scale Development Studies. *Informatics*, 8(2):31, 2021.
- [270] May Fen Gan, Hui Na Chua, and Siew Fan Wong. Privacy Enhancing Technologies Implementation: An Investigation of Its Impact on Work Processes and Employee Perception. *Telematics and Informatics*, 38:13–29, 2019.
- [271] Eva-Maria Schomakers, Chantal Lidynia, Dirk Müllmann, and Martina Ziefle. Internet Users’ Perceptions of Information Sensitivity –Insights from Germany. *International Journal of Information Management*, 46(1):142–150, 2019.
- [272] Eva-Maria Schomakers, Chantal Lidynia, Dirk Müllmann, Roman Matzutt, Klaus Wehrle, Indra Spiecker genannt Döhmann, and Martina Ziefle. Putting Privacy into Perspective – Comparing Technical, Legal, and Users’ View of Information Sensitivity. In *Proceedings of the 50th Jahrestagung der Gesellschaft für Informatik (INFORMATIK)*, pages 857–870, 2020.
- [273] Khaled Almotairi and Bilal Bataineh. Perception of Information Sensitivity for Internet Users in Saudi Arabia. *Acta Informatica Pragensia*, 9(2):184–199, 2020.

- [274] Ereni Markos, Geroge R. Milne, and James 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.
- [275] Miguel Malheiros, Sören Preibusch, and M. Angela Sasse. “Fairly Truthful”: The Impact of Perceived Effort, Fairness, Relevance, and Sensitivity on Personal Data Disclosure. In *Proceedings of the 6th International Conference on Trust and Trustworthy Computing (TRUST)*, pages 250–266, 2013.
- [276] Ereni Markos, Lauren I. Labrecque, and George R. Milne. A New Information Lens: The Self-Concept and Exchange Context as a Means to Understand Information Sensitivity of Anonymous and Personal Identifying Information. *Journal of Interactive Marketing*, 42:46–62, 2018.
- [277] Miriam J. Metzger. Privacy, Trust, and Disclosure: Exploring Barriers to Electronic Commerce. *Journal of Computer-Mediated Communication*, 9(4):JCMC942, 2004.
- [278] George R. Milne, George Pettinico, Fatima M. Hajjat, and Ereni Markos. Information Sensitivity Typology: Mapping the Degree and Type of Risk Consumers Perceive in Personal Data Sharing. *Journal of Consumer Affairs*, 51(1):133–161, 2017.
- [279] Joseph Phelps, Glen Nowak, and Elizabeth Ferrell. Privacy Concerns and Consumer Willingness to Provide Personal Information. *Journal of Public Policy & Marketing*, 19(1):27–41, 2000.
- [280] Kim Bartel Sheehan and Mariea Grubbs Hoy. Dimensions of Privacy Concern among Online Consumers. *Journal of Public Policy & Marketing*, 19(1):62–73, 2000.
- [281] Fred A. Mael, Mary Connerley, and Ray A. Morath. None of Your Business: Parameters of Biodata Invasiveness. *Personnel Psychology*, 49(3):613–650, 1996.
- [282] Athina Ioannou, Iis Tussyadiah, and Graham Miller. That’s Private! Understanding Travelers’ Privacy Concerns and Online Data Disclosure. *Journal of Travel Research*, page 0047287520951642, 2020.
- [283] Ponnuram Kumaraguru and Lorrie Faith Cranor. Privacy Indexes: A Survey of Westin’s Studies. Research Report Cmu-isri-5-138, Institute for Software Research, International School of Computer Science Carnegie Mellon University Pittsburgh, 2005. URL <https://www.cs.cmu.edu/~ponguru/CMU-ISRI-05-138.pdf>.
- [284] Bart P. Knijnenburg. Information Disclosure Profiles for Segmentation and Recommendation. In *Proceedings of the 1st USENIX Workshop on Privacy Personas and Segmentation (PPS)*, pages 1–4, 2014.
- [285] Janna-Lynn Dupree, Richard Devries, Daniel M. Berry, and Edward Lank. Privacy Personas: Clustering Users via Attitudes and Behaviors Toward Security Practices. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 5228–5239, 2016.
- [286] Marija Kuzmanovic and Gordana Savic. Avoiding the Privacy Paradox Using Preference-Based Segmentation: A Conjoint Analysis Approach. *Electronics*, 9(9):1382, 2020.

- [287] Eva-Maria Schomakers, Chantal Lidynia, Luisa Vervier, and Martina 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.
- [288] Lemi Baruh and Zeynep Cemalcı. It Is More than Personal: Development and Validation of a Multidimensional Privacy Orientation Scale. *Personality and Individual Differences*, 70:165–170, 2014.
- [289] Sören Preibusch. Managing Diversity in Privacy Preferences: How to Construct a Privacy Typology. In *Proceedings of the 1st USENIX Workshop on Privacy Personas and Segmentation (PPS)*, pages 1–6, 2014.
- [290] Jennifer Urban and Chris Jay Hoofnagle. The Privacy Pragmatic as Privacy Vulnerable. In *Proceedings of the 1st USENIX Workshop on Privacy Personas and Segmentation (PPS)*, pages 1–5, 2014.
- [291] Laura Burbach, Chantal Lidynia, Philipp Brauner, and Martina Ziefle. Data Protectors, Benefit Maximizers, or Facts Enthusiasts: Identifying User Profiles for Life-Logging Technologies. *Computers in Human Behavior*, 99(C):9–21, 2019.
- [292] Isioma Elueze and Anabel Quan-Haase. Privacy Attitudes and Concerns in the Digital Lives of Older Adults: Westin’s Privacy Attitude Typology Revisited. *American Behavioral Scientist*, 62(10):1372–1391, 2018.
- [293] Pamela Wisniewski, Bart P. Knijnenburg, and Heather Richter Lipford. Profiling Facebook Users’ Privacy Behaviors. In *Proceedings of the 1st USENIX Workshop on Privacy Personas and Segmentation (PPS)*, pages 1–6, 2014.
- [294] Nancy K. Lankton, D. Harrison McKnight, and John F. Tripp. Facebook Privacy Management Strategies. *Computers in Human Behavior*, 76(C):149–163, 2017.
- [295] Judith S. Olson, Jonathan Grudin, and Eric Horvitz. A Study of Preferences for Sharing and Privacy. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA)*, pages 1985–1988, 2005.
- [296] Takashi Koshimizu, Tomoji Toriyama, and Noboru Babaguchi. Factors on the Sense of Privacy in Video Surveillance. In *Proceedings of the 3rd ACM Workshop on Continuous Archival and Retrieval of Personal Experiences (CARPE)*, pages 35–44, 2006.
- [297] Sean Sirur, Jason R.C. Nurse, and Helena Webb. Are We There Yet? Understanding the Challenges Faced in Complying with the General Data Protection Regulation (GDPR). In *Proceedings of the 2nd International Workshop on Multimedia Privacy and Security (MPS)*, pages 88–95, 2018.
- [298] Steering Committee on the Usability, Security, and Privacy of Computer Systems. *Toward Better Usability, Security, and Privacy of Information Technology: Report of a Workshop*. National Academies Press, 2010.
- [299] Predrag Klasnja, Sunny Consolvo, Jaeyeon Jung, Benjamin M. Greenstein, Louis LeGrand, Pauline Powledge, and David Wetherall. "When I Am on Wi-Fi, I Am



- Fearless": Privacy Concerns & Practices in Eeryday Wi-Fi Use. In *Proceedings of the CHI Conference on Human Factors in Computing Systems*, pages 1993–2002, 2009.
- [300] Mike Bergmann. Testing Privacy Awareness. In *The Future of Identity in the Information Society*, pages 237–253, 2009.
- [301] Stefanie Pöttsch. Privacy Awareness: A Means to Solve the Privacy Paradox? In *Proceedings of the 4th IFIP International Summer School on Privacy and Identity Management*, pages 226–236, 2009.
- [302] Judith Reitman Olson and Henry H. Rueter. Extracting Expertise from Experts: Methods for Knowledge Acquisition. *Expert Systems*, 4(3):152–168, 1987.
- [303] Richard A. Krueger and Mary Anne Casey. *Focus Groups: A Practical Guide for Applied Research*. Sage, 5th edition, 2015.
- [304] Farzaneh Asgharpour, Debin Liu, and L. Jean Camp. Mental Models of Security Risks. In *Proceedings of the 1st International Workshop on Usable Security (USEC)*, pages 367–377, 2007.
- [305] M. Granger Morgan, Baruch Fischhoff, Ann Bostrom, and Cynthia J. Atman. *Risk Communication: A Mental Models Approach*. Cambridge University Press, 2002.
- [306] Jitka Šišková and Enikő Lőrinczová. Implementation of GDPR into Payroll Accounting in the Czech Republic. In *Proceedings of the 10th Hradec Economic Days (HED)*, pages 1–8, 2020.
- [307] Michelle Kwasny, Kelly Caine, Wendy A. Rogers, and Arthur D. Fisk. Privacy and Technology: Folk Definitions and Perspectives. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA)*, pages 3291–3296, 2008.
- [308] John L. Campbell, Charles Quincy, Jordan Osserman, and Ove K. Pedersen. Coding In-depth Semistructured Interviews: Problems of Unitization and Intercoder Reliability and Agreement. *Sociological Methods & Research*, 42(3):294–320, 2013.
- [309] Philipp Mayring. Qualitative Content Analysis. *Forum Qualitative Sozialforschung*, 1(2):1–10, 2000.
- [310] Kilem Li Gwet. Computing Inter-Rater Reliability and Its Variance in the Presence of High Agreement. *British Journal of Mathematical and Statistical Psychology*, 61(1): 29–48, 2008.
- [311] Alvan R. Feinstein and Domenic V. Cicchetti. High Agreement but Low Kappa: I. the Problems of Two Paradoxes. *Journal of Clinical Epidemiology*, 43(6):543–549, 1990.
- [312] Joel R Reidenberg, Travis Breaux, Lorrie Faith Cranor, Brian French, Amanda Grannis, James T Graves, Fei Liu, Aleecia McDonald, Thomas B Norton, Rohan Ramanath, N Cameron Russell, Norman Sadeh, and Florian Schaub. Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding. *Berkeley Technology Law Journal*, 30(1):39–88, 2015.

- [313] Anthony Morton and M. Angela 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.
- [314] Jennifer King. Taken Out of Context: An Empirical Analysis of Westin’s Privacy Scale. In *Proceedings of the 1st USENIX Workshop on Privacy Personas and Segmentation (PPS)*, pages 1–8, 2014.
- [315] Alessandro Acquisti, Laura Brandimarte, and George Loewenstein. Privacy and Human Behavior in the Age of Information. *Science*, 347(6221):509–514, 2015.
- [316] Eugene F. Stone, Hal G. Gueutal, Donald G. Gardner, and Stephen 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.
- [317] Philipp K. Masur, Doris Teutsch, and Sabine Trepte. Entwicklung Und Validierung Der Online-Privatheitskompetenzskala (OPLIS) (Development and Validation of the Online Privacy Literacy Scale (OPLIS)). *Diagnostica*, 63(4):256–268, 2017.
- [318] Mirta Galesic and Michael Bosnjak. Effects of Questionnaire Length on Participation and Indicators of Response Quality in a Web Survey. *Public Opinion Quarterly*, 73(2):349–360, 2009.
- [319] Federal Statistical Office. Homepage, 2021. URL [https://www.destatis.de/EN/Home/\\_node.html](https://www.destatis.de/EN/Home/_node.html).
- [320] Guillaume A. Rousselet, Cyril R. Pernet, and Rand R. Wilcox. The Percentile Bootstrap: A Primer With Step-by-Step Instructions in R. *Advances in Methods and Practices in Psychological Science*, 4(1):2515245920911881, 2021.
- [321] Conrad Zygmunt and Mario R. Smith. Robust Factor Analysis in the Presence of Normality Violations, Missing Data, and Outliers: Empirical Questions and Possible Solutions. *The Quantitative Methods for Psychology*, 10(1):40–55, 2014.
- [322] Marley W. Watkins. Exploratory Factor Analysis: A Guide to Best Practice. *Journal of Black Psychology*, 44(3):219–246, 2018.
- [323] Joseph F. Hair, William C. Black, Barry J. Babin, and Rolph E. Anderson. *Multivariate Data Analysis*. Cengage Learning, 8th edition, 2019.
- [324] Francisco Pablo Holgado-Tello, Salvador Chacón-Moscoso, Isabel Barbero-García, and Enrique Vila-Abad. Polychoric versus Pearson Correlations in Exploratory and Confirmatory Factor Analysis of Ordinal Variables. *Quality & Quantity*, 44(1): 153, 2008.
- [325] Njål Foldnes and Steffen Grønneberg. The Sensitivity of Structural Equation Modeling with Ordinal Data to Underlying Non-Normality and Observed Distributional Forms. *Psychological Methods*, pages 1–40, 2021.

- [326] Kristopher J. Preacher, Guangjian Zhang, Cheongtag Kim, and Gerhard Mels. Choosing the Optimal Number of Factors in Exploratory Factor Analysis: A Model Selection Perspective. *Multivariate Behavioral Research*, 48(1):28–56, 2013.
- [327] Rex B. Kline. Assumptions in Structural Equation Modeling. In Rick H. Hoyle, editor, *Handbook of Structural Equation Modeling*, pages 111–125. The Guildford Press, 2012.
- [328] Jörg Henseler, Christian M. Ringle, and Marko Sarstedt. A New Criterion for Assessing Discriminant Validity in Variance-Based Structural Equation Modeling. *Journal of the Academy of Marketing Science*, 43(1):115–135, 2015.
- [329] Steven G. Luke. Evaluating Significance in Linear Mixed-Effects Models in R. *Behavior Research Methods*, 49(4):1494–1502, 2017.
- [330] Shawn N. Geniole, Valentina Proietti, Brian M. Bird, Triana L. Ortiz, Pierre L. Bonin, Bernard Goldfarb, Neil V. Watson, and Justin M. Carré. Testosterone Reduces the Threat Premium in Competitive Resource Division. *Proceedings of the Royal Society B: Biological Sciences*, 286(1903):20190720, 2019.
- [331] Charilaos Yiotis, Jennifer C McElwain, and Bruce A Osborne. Enhancing the Productivity of Ryegrass at Elevated CO<sub>2</sub> Is Dependent on Tillering and Leaf Area Development Rather than Leaf-Level Photosynthesis. *Journal of Experimental Botany*, 72(5):1962–1977, 2021.
- [332] Jichuan Wang and Xiaoqian Wang. 7.1 The Rules of Thumb for Sample Size Needed for SEM. In *Structural Equation Modeling: Applications Using Mplus*. Wiley, 2nd edition, 2012.
- [333] Karen L. Nylund, Tihomir Asparouhov, and Bengt O. Muthén. Deciding on the Number of Classes in Latent Class Analysis and Growth Mixture Modeling: A Monte Carlo Simulation Study. *Structural Equation Modeling: A Multidisciplinary Journal*, 14(4):535–569, 2007.
- [334] Bethany C. Bray, Stephanie T. Lanza, and Xianming Tan. Eliminating Bias in Classify-Analyze Approaches for Latent Class Analysis. *Structural Equation Modeling: A Multidisciplinary Journal*, 22(1):1–11, 2015.
- [335] Daniel J. Stekhoven and Peter Bühlmann. MissForest —Non-Parametric Missing Value Imputation for Mixed-Type Data. *Bioinformatics*, 28(1):112–118, 2012.
- [336] Daniel J. Mundfrom, Dale G. Shaw, and Tian Lu Ke. Minimum Sample Size Recommendations for Conducting Factor Analyses. *International Journal of Testing*, 5(2):159–168, 2005.
- [337] Cees van der Eijk and Jonathan Rose. Risky Business: Factor Analysis of Survey Data –Assessing the Probability of Incorrect Dimensionalisation. *Plos One*, 10(3): e0118900, 2015.
- [338] David Harborth and Sebastian Pape. German Translation of the Concerns for Information Privacy (CFIP) Construct. Technical Report SSRN 3112207, 2018.

- [339] Joseph A. Durlak. How to Select, Calculate, and Interpret Effect Sizes. *Journal of Pediatric Psychology*, 34(9):917–928, 2009.
- [340] Christian Pieter Hoffmann, Christoph Lutz, and Giulia Ranzini. Privacy Cynicism: A New Approach to the Privacy Paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 10(4), 2016.
- [341] Michelle L. Kaarst-Brown and E. Dale Thompson. Cracks in the Security Foundation: Employee Judgments about Information Sensitivity. In *Proceedings of the ACM SIGMIS Conference on Computers and People Research (SIGMIS-CPR)*, pages 145–151, 2015.
- [342] Thomas Groß. Validity and Reliability of the Scale Internet Users’ Information Privacy Concerns (IUIPC). *Proceedings on Privacy Enhancing Technologies*, 2021(2): 235–258, 2021.
- [343] Lebek Benedikt. Information Security Awareness and Behavior: A Theory-Based Literature Review. *Management Research Review*, 37(12):1049–1092, 2014.
- [344] Seb Goodman. Human Error to Blame for 9 in 10 UK Cyber Data Breaches in 2019, 2020. URL <https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/>. last visited: March 16, 2022.
- [345] Privacy Rights Clearinghouse (PRC). PRC Data Breach Chronology. Database 1.13.20, Privacy Rights Clearinghouse, 2020. URL <https://privacyrights.org/sites/default/files/2020-01/PRC%20Data%20Breach%20Chronology%20-%201.13.20.csv>.
- [346] Rapportage Datalekken 2020. Technical report, Autoriteit Persoonsgegevens, 2020. URL [https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage\\_datalekken\\_2020.pdf](https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/rapportage_datalekken_2020.pdf).
- [347] Ellen Rosen. Human Error Biggest Cause of Data Breach: Survey. *Bloomberg Law*, 2015. URL <https://news.bloomberglaw.com/business-and-practice/human-error-biggest-cause-of-data-breach-survey>. last visited: March 16, 2022.
- [348] Jordan Brackenbury and Rebecca Bailey. 2020 Outbound Email Security Report | Egress, 2020. URL <https://www.egress.com/newsroom/2020-outbound-email-security-report>. last visited: March 16, 2022.
- [349] Andrey Evdokimov, Alena Reva, and Koen Maris. Taking Care of Corporate Security and Employee Privacy. Survey, AO Kaspersky Lab, 2020. URL [https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/04/20043942/Kaspersky-2020\\_Report\\_Human\\_angle\\_FINAL.pdf](https://media.kasperskydaily.com/wp-content/uploads/sites/92/2020/04/20043942/Kaspersky-2020_Report_Human_angle_FINAL.pdf). last visited: June 30, 2022.
- [350] Gordon Baxter and Ian Sommerville. Socio-Technical Systems: From Design Methods to Systems Engineering. *Interacting with Computers*, 23(1):4–17, 2011.

- [351] Luca Piras, Mohammed Ghazi Al-Obeidallah, Michalis Pavlidis, Haralambos Mouratidis, Aggeliki Tsohou, Emmanouil Magkos, Andrea Praitano, Annarita Iodice, and Beatriz Gallego-Nicasio Crespo. DEFEND DSM: A Data Scope Management Service for Model-Based Privacy by Design GDPR Compliance. In *Proceedings of the 17th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)*, pages 186–201, 2020.
- [352] Jonathan Lazar, Jinjuan Heidi Feng, and Harry Hochheiser. *Research Methods in Human Computer Interaction*. Elsevier, 2nd edition, 2017.
- [353] Chauncey Wilson. Pluralistic Usability Walkthrough. In *User Interface Inspection Methods*, pages 81–97. Elsevier, 2014.
- [354] Jeff Sauro and James R. Lewis. *Quantifying the User Experience: Practical Statistics for User Research*. Elsevier/Morgan Kaufmann, 2012.
- [355] Virginia Braun, Victoria Clarke, Nikki Hayfield, and Gareth Terry. Thematic Analysis. In Pranee Liamputtong, editor, *Handbook of Research Methods in Health Social Sciences*, pages 843–860. Springer, 2019.
- [356] ISO/IEC JTC 1/SC 7. *ISO/IEC 25010:2011: Systems and Software Engineering —Systems and Software Quality Requirements and Evaluation (SQuaRE) —System and Software Quality Models*. International Organization for Standardization, 1st edition, 2011. URL <https://www.iso.org/standard/35733.html>.
- [357] David Maulsby, Saul Greenberg, and Richard Mander. Prototyping an Intelligent Agent through Wizard of Oz. In *Proceedings of the INTERACT and CHI Conference on Human Factors in Computing Systems*, pages 277–284, 1993.
- [358] Michael Geers. *Micro Frontends in Action*. Manning Publications, 2020.
- [359] Holger Harms, Collin Rogowski, and Luigi Lo Iacono. Guidelines for Adopting Frontend Architectures and Patterns in Microservices-Based Systems. In *Proceedings of the 11th Joint Meeting on Foundations of Software Engineering (ESEC/FSE)*, pages 902–907, 2017.
- [360] Eric Evans. *Domain-Driven Design: Tackling Complexity in the Heart of Software*. Addison-Wesley, 2004.
- [361] Ines Mergel, Noella Edelmann, and Nathalie Haug. Defining Digital Transformation: Results from Expert Interviews. *Government Information Quarterly*, 36(4): 101385, 2019.
- [362] Gregory Vial. Understanding Digital Transformation: A Review and a Research Agenda. *The Journal of Strategic Information Systems*, 28(2):118–144, 2019.
- [363] Markku Kuusisto. Organizational Effects of Digitalization: A Literature Review. *International Journal of Organization Theory and Behavior*, 20(03):341–362, 2017.
- [364] He Li, Lu Yu, and Wu He. The Impact of GDPR on Global Technology Development. *Journal of Global Information Technology Management*, 22(1):1–6, 2019.

- [365] Mohd Anwar, Wu He, Ivan Ash, Xiaohong Yuan, Ling Li, and Li Xu. Gender Difference and Employees' Cybersecurity Behaviors. *Computers in Human Behavior*, 69:437–443, 2017.
- [366] Stephan Wiefeling, Markus Dürmuth, and Luigi Lo Iacono. More Than Just Good Passwords? A Study on Usability and Security Perceptions of Risk-based Authentication. In *Proceedings of the 36th Annual Computer Security Applications Conference (ACSAC)*, pages 203–218, 2020.
- [367] Yichuan Wang, Shiwei Sun, John R Drake, and Dianne Hall. Job Applicants' Information Privacy- Protective Response: Exploring the Roles of Technology Readiness and Trust. In *Proceedings of the 21st Americas' Conference on Information Systems (AMCIS)*, pages 1–13, 2015.
- [368] OECD. STAN Industry ISIC Rev. 4. 2017. URL <https://www.oecd-ilibrary.org/content/data/data-00649-en>.
- [369] R Core Team. *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing, 2020.
- [370] Guillaume A. Rousselet, Cyril R. Pernet, and Rand R. Wilcox. A practical introduction to the bootstrap: a versatile method to make inferences by using data-driven simulations. *PsyArXiv*, 2019. URL <https://psyarxiv.com/h8ft7/>.
- [371] William Revelle. *psych: Procedures for Psychological, Psychometric, and Personality Research*. Northwestern University, 2021. R package version 2.1.3.
- [372] Markus D. Steiner and Silvia Grieder. EFAtools: An R package with fast and flexible implementations of exploratory factor analysis tools. *Journal of Open Source Software*, 5(53):2521, 2020.
- [373] John Fox. *polycor: Polychoric and Polyserial Correlations*, 2020. R package version 0.8-0/r22.
- [374] Yves Rosseel. Lavaan: An R Package for Structural Equation Modeling. *Journal of Statistical Software*, 48(1):1–36, 2012.
- [375] Terrence D. Jorgensen, Sunthud Pornprasertmanit, Alexander M. Schoemann, Yves Rosseel, Patrick Miller, Corbin Quick, Mauricio Garnier-Villareal, James Selig, Aaron Boulton, Kristopher Preacher, Donna Coffman, Mijke Rhemtulla, Alexander Robitzsch, Craig Enders, Ruben Arslan, Bell Clinton, Pavel Panko, Edgar Merkle, Steven Chesnut, Jarrett Byrnes, Jason D. Rights, Ylenio Longo, Maxwell Mansolf, Mattan S. Ben-Shachar, Mikko Rönkkö, and Andrew R. Johnson. *semTools: Useful Tools for Structural Equation Modeling*, 2021.
- [376] Selcuk Korkmaz, Dincer Goksuluk, and Gokmen Zararsiz. MVN: An R Package for Assessing Multivariate Normality. *The R Journal*, 6(2):151–162, 2014.
- [377] Douglas Bates, Martin Mächler, Ben Bolker, and Steve Walker. Fitting Linear Mixed-Effects Models Using Lme4. *Journal of Statistical Software*, 67(1):1–48, 2015.

- [378] Alexandra Kuznetsova, Per B. Brockhoff, and Rune H. B. Christensen. lmerTest Package: Tests in Linear Mixed Effects Models. *Journal of Statistical Software*, 82(13): 1–26, 2017.
- [379] Manuel Koller. Robustlmm: An R Package for Robust Estimation of Linear Mixed-Effects Models. *Journal of Statistical Software*, 75(1):1–24, 2016.
- [380] Drew A. Linzer and Jeffrey B. Lewis. poLCA: An R Package for Polytomous Variable Latent Class Analysis. *Journal of Statistical Software*, 42(1):1–29, 2011.
- [381] Federal Labour Office. Klassifikation der Berufe 2010 – überarbeitete Fassung 2020 Band 1: Systematischer und alphabetischer Teil mit Erläuterungen. Official document, Bundesagentur für Arbeit, 2021. URL <https://statistik.arbeitsagentur.de/DE/Navigation/Grundlagen/Klassifikationen/Klassifikation-der-Berufe/KldB2010-Fassung2020/Publikationen/Publikationen-Nav.html>.





APPENDIX LITERATURE SURVEY

---

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Recorded Work Meetings and Algorithmic Tools: Anticipated Boundary Turbulence</i> – Impact of algorithmic evaluation (i.e., AI) on employee data on employee privacy and trust. (Cardon et al., 2021)	Social contract theory	Qualitative, semi-structured interviews	Employees (China, U.S., Germany) N=50	n.a.	Information system use: AI
<i>A multicultural study of biometric privacy concerns in a fire ground accountability crisis response system</i> – Investigate cultural and ethnic differences on employees' perceived privacy concerns toward using biometric technology. (Carpenter et al., 2016)	TAM, UTAUT, privacy concerns	Quantitative, online survey	Firefighters (U.S.) N=303	PLS-SEM	Information system use: Biometric
<i>Privacy and biometrics: An empirical examination of employee concerns</i> – Investigate impact of privacy concerns and self-construal on employees' attitude toward using biometric technology. (Carpenter et al., 2018)	TAM, UTAUT, privacy concerns	Quantitative, online survey	Firefighters (U.S.) N=309	PLS-SEM	Information system use: Biometric
<i>Investigating the Influence of Security, Privacy, and Legal Concerns on Employees' Intention to Use BYOD Mobile Devices</i> – (Lebek et al., 2013)	TAM	Quantitative, online survey	Employees (Germany) N=151	PLS-SEM	Information system use: BYOD
<i>Implications of Monitoring Mechanisms on Bringing Your Own Device Adoption</i> – Examining the impact of employee privacy concerns caused by BYOD monitoring mechanisms on intention to use BYOD, and whether privacy concerns suppress the benefits of increased job performance expectations when assessing BYOD program participation. (Lee Jr et al., 2017)	Privacy concerns, TPB, IUIPC, UTAUT	Quantitative online factorial survey	Students and Alumni (U.S.) N=275	Hierarchical linear modeling, Chi-sq	Information system use: BYOD

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Future of Flexible Work in the Digital Age: Bring Your Own Device Challenges of Privacy Protection Challenges of Privacy Protection</i> – Impact of employees' privacy concerns and perceived risks on intention to use BYOD when being monitored by mobile device management software. ( <a href="#">Degirmenci et al., 2019</a> )	Privacy concerns, TAM calculus,	Case study, company survey	Employees (U.S., many, South Korea) N=542	PLS-SEM	Information system use: BYOD
<i>Using a Participatory Toolkit to Elicit Youth's Workplace Privacy Perspectives</i> – Adaptation and evaluation of a participatory toolkit to investigate privacy perceptions of youth employees, to qualitatively investigate their perceived appropriateness and expectation of information disclosure to other stakeholders (e.g., managers, clients, advertisers). ( <a href="#">Easley et al., 2021</a> )	Expected access to (personal) data	Qualitative interview study, case study	Youth employees (U.S.) N=5	Open axial coding	Information system use: ICT
<i>Analyzing the Problem of Employee Internal Social Network Site Avoidance: Are Users Resistant due to their Privacy Concerns?</i> – Impact of employees' privacy concerns on intention to use Enterprise Social Networks. ( <a href="#">Buettner, 2015</a> )	TAM, UTAUT	Quantitative, online survey	Employees (Germany) N=253	PLS-SEM	Information system use: ESN
<i>Perceived Information-Based Vulnerability of Enterprise Information Systems: Concept, Antecedents, and Outcomes</i> – Antecedents for the disclosure of honest personal data in enterprise social networks. ( <a href="#">Träutlein and Gerlach, 2015</a> )	Control, information sensitivity, trust	Research framework development	n.a.	n.a.	Information system use: ESN

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Analysing Employees’ Willingness To Disclose Information In Enterprise Social Networks: The Role Of Organizational Culture</i> – Impact of employees’ trusting and risk beliefs on their willingness to disclose information in Enterprise Social Networks in different organizational cultures. (Engelbrecht et al., 2017)	APCO, IUPC, risk beliefs, trust, willingness to disclose	Quantitative, online survey, mailing lists	Employees (Germany) N=282	PLS-SEM	Information system use: ESN
<i>Information-sharing Workarounds in Enterprise Social Networks: Privacy-related Triggers</i> – Model to research workaround strategies used by employees to protect their privacy when using Enterprise Social Networks. (Seguel, 2021)	Theory of multilevel information privacy, information privacy norms, privacy calculus	Research model development	n.a.	Non-systematic	Information system use: ESN
<i>The Study on the Relationship Between Privacy Concerns and Information Systems Effectiveness</i> – Investigating employees’ (as users of information systems) psychological mechanisms involving the relationship between privacy concerns and perceived usefulness and satisfaction through information systems reactance on systems and procedural justice. (Park, 2009)	Privacy concerns under psychological reactance theory	Quantitative, online survey	Employees (Korea) N=251	SEM	Information system use: General
<i>Information Systems and Healthcare XXXVII: When Your Employer Provides Your Personal Health Record—Exploring Employee Perceptions of an Employer-Sponsored PHR System</i> – Perceived privacy and security of personal health data in employer-sponsored personal health records. (Burkhard et al., 2010)	Privacy concerns	Quantitative, online survey	Employees (U.S.); N=132	ANOVA, Chi-sq	Information system use: Health sys.

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>My data, my choice?! The difference between fitness and stress data monitoring on employees' perception of privacy</i> – Comparing employees' perceived privacy risks regarding the monitoring of either stress or fitness when using wearables in occupational health management. ( <a href="#">Diel et al., 2022</a> )	APCO, privacy awareness, privacy experience, privacy calculus	Experiment multiple treatments	Employees (Germany) N=155	Mann-Whitney U Test, Chi-sq	Information system use: Health sys.
<i>The Effects of the Ability to Choose the Type of Human Resources System on Perceptions of Invasion of Privacy and System Satisfaction</i> – Impact of employees' control over choosing the type of system and type of personal information on their privacy perceptions and satisfaction with HR. ( <a href="#">Lukaszewski et al., 2008</a> )	Privacy invasion	Experiment A/B treatment	Employees (U.S.) N=71	Regression analysis	Information system use: HR system
<i>Online disclosure of employment information: exploring Malaysian government employees' views in different contexts</i> – Examining differences in privacy perceptions regarding control and ownership of employment information published via private online social network vs. published on employers' website. ( <a href="#">Badrul et al., 2016</a> )	Information boundary and communication privacy management theory	Semi-structured interviews	Government employees (Malaysia) N=5	Thematic analysis	Information system use: OSN

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<p><i>What drives construction workers' acceptance of wearable technologies in the workplace?: Indoor localization and wearable health devices for occupational safety and health</i></p> <p>– Examining determinants of construction workers' intentions to use wearables for occupational safety and health, including consideration of perceived privacy risks. (Choi et al., 2017)</p>	Privacy concerns, risks, TAM	Experiment, case study	Construction Workers (U.S.) N=120	Hierarchical regression, ANOVA	Information system use: Wearables
<p><i>Physiology at the workplace: Affordances and constraints of wearables use from an employee's perspective</i></p> <p>– Identification of different employee mental models of using wearables in the workplace. (Mettler and Wulf, 2019)</p>	Affordance theory, constraints of privacy and freedom	Qualitative, online survey	Employees (Germany) N=20	Q-Method.	Information system use: Wearables
<p><i>Employees' acceptance of wearable devices: Towards a predictive model</i> – Design and validate a predictive model for employees' acceptance of wearables, considering privacy issues. (Magni et al., 2021)</p>	Privacy calculus, perceived TAM, risks	Quantitative, online survey	Employees (Italy) N=523	Multiple regression analysis	Information system use: Wearables
<p><i>Is There a Privacy Paradox in the Workplace?</i> – Employee self-disclosure when interacting with robots at the workplace. (Stock and Hannig, 2020)</p>	APCO, information reluctance, privacy concerns	Quantitative, vignette survey	Employees (international) N=210	ANCOVA	Information system use: Robots
<p><i>Employee perceptions of invasion of privacy: A field simulation experiment.</i> – Explore employees' perceived invasion of privacy, depending on the type of information and employees' consent. (Tolchinsky et al., 1981)</p>	Privacy invasion	Quantitative, survey	Employees (U.S.) N=2047	ANOVA	Information privacy perceptions



Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>A Survey of Employee Perceptions of Information Privacy in Organizations</i> – Explore employees' perceptions regarding the types of personal information allegedly processed by employers, and examine accuracy of such. (Woodman et al., 1982)	Expected knowledge, privacy concern	Quantitative, survey	Employees (U.S.) N=2047	Descriptive statistics	Information privacy perceptions
<i>Attitudes Toward Employee and Employer Rights in the Workplace</i> – Determine the types of information and the types of purposes that employees would perceive as normative or intrusive if employers had the right to obtain the information and use it for certain purposes. (Garland et al., 1989)	Contextual norms of personal information use	Quantitative, survey	Students (U.S.) N=692	Factor analysis	Information privacy perceptions
<i>Individuals' Attitudes Toward Organizational Drug Testing Policies and Practices</i> – Examining effects of two hypothetical drug testing policies: (a) advance notice of drug testing (not provided vs provided) and (b) the consequences of detected drug use (termination vs rehabilitation) on attitudes toward drug testing. (Stone and Ketch, 1989)	Privacy invasion	Quantitative, vignette	Employees (U.S.) N=73	Regression	Information privacy perceptions

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Information Privacy and Performance Appraisal: An Examination of Employee Perceptions and Reactions</i> – Examining employees' perceptions and reactions regarding various aspects of performance appraisal as an invasion of privacy and determining the relationships between these privacy-related attitudes and employees' satisfaction with the organization's appraisal system. (Mossholder et al., 1991)	Privacy invasion in terms of collection, release, and storage	Quantitative, survey on-premise	Managers, supervisory personnel (U.S.) N=320	Correlation analysis	Information privacy perceptions
<i>The Effects of Information Management Policies on Reactions to Human Resource Information Systems: An Integration of Privacy and Procedural Justice Perspectives</i> – Examining the main and interactive effects of policies concerning employees' ability to authorize disclosure and disclosure target (internal vs. external) on employees' invasion of privacy and fairness perceptions. (Eddy et al., 1999)	Privacy invasion, procedural fairness, employee policy acceptance	Experiment, multiple treatments	Part-time employees / students (U.S.) N=124	ANOVA, MANOVA, CFA	Information privacy perceptions
<i>Information Privacy in Organizations: Empowering Creative and Extrarole Performance</i> – Design and validate a predictive model for employees' organizational citizenship behavior and performance based on perceived privacy. (Alge et al., 2006)	APCO, gathering control, handling perceived legitimacy	Quantitative, online survey	Employees (U.S.) N=310 / 303	SEM	Information privacy perceptions

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>The Impact of Individual Ethics on Reactions to Potentially Invasive HR Practices</i> – Examining effects of employees' ethics on their attitudes and perceived appropriateness towards potentially invasive organizational practices based on perceived privacy invasion. (Alder et al., 2007)	Privacy invasion	Quantitative, online survey	Employees (U.S.) N=186	Multiple regression analysis	Information privacy perception
<i>The Importance of Communicating Workplace Privacy Policies</i> – Examining employees' demographic differences for their attitudes towards organizational practices of handling and communicating workplace privacy policies. (Dillon et al., 2008)	Attitudes towards workplace privacy policies	Quantitative online survey	Employees (U.S.) N=1085	ANOVA, factor analysis, t-test, descriptive analysis	Information privacy perceptions
<i>Employee Information Privacy Concerns with Employer Held Data: A Comparison of Two Prevalent Privacy Models</i> – Empirically evaluate two privacy models relying on APCO for the work context. (Clouse et al., 2010)	CFIP, IUIPC	Quantitative, online survey	Employees (U.S.) N=457	SEM	Information privacy perceptions
<i>Dimensions of employee privacy: an empirical study</i> – Identification of different notions of workplace privacy (information, work environment, and solitude) (Ball et al., 2012)	Privacy concerns, control	Quantitative, online survey, Qualitative, semi-structured interviews	Employees (South Africa, UK) N=91 / N=30	CMV analysis, thematic analysis	Information privacy perceptions

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Information privacy, gender differences, and intrinsic motivation in the workplace</i> – Examining the relationship between information privacy, gender differences, and intrinsic motivation of employees. (Chen et al., 2013)	Gathering control, handling control	Quantitative, online survey	Employees (China) N=320	PLS-SEM	Information privacy perceptions
<i>What Makes Workplace Privacy Special? An Investigation of Determinants of privacy Concerns in the Digital Workplace</i> – Identification of determinants of workplace privacy concerns. (Teebken, 2021)	Privacy information disclosure	Qualitative, semi-structured interviews	Experts N=13	Grounded theory approach	Information privacy perceptions
<i>Privacy in a Digitized Workplace: Towards an Understanding of Employee Privacy Concerns</i> – Identification of dimensions of workplace specific privacy concerns. (Teebken and Hess, 2021)	APCO, CFIP, IPC, IUPC, privacy concerns	Qualitative, semi-structured interviews	Employees (Germany) N=33	Thematic analysis	Information privacy perceptions
<i>A Synthesized Perspective on Privacy and Transparency in the Digital Workplace</i> – Impact of direct and inverse transparency on employees' information privacy, revealing a privacy-transparency paradox in employment. (Gierlich-Joas et al., 2022)	APCO, multidimensional development theory, direct and inverse transparency, privacy concerns, sphere theory	Literature survey	n.a.	Systematic review	Information privacy perceptions
<i>Attitude toward invasion of privacy in the personnel selection process and job applicant demographic and personality correlates.</i> – (Rosenbaum, 1973)	Information sensitivity	Quantitative, survey	Applicants (U.S.) N=1392	Factor analysis	Job application

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Variables affecting perceptions of invasion of privacy in a personnel selection situation</i> – Examining the effects of perceived control over the personal information disclosed, the outcome of the disclosure, the type of disclosure, and the type of information disclosed on job applicants’ perceptions of invasion of privacy in a personnel selection procedure. (Fusilier and Hoyer, 1980)	Privacy control	Experiment factorial design	Students (U.S.) N=423	Multiple regression analysis	Job application
<i>Effects of missing application-blank information on personnel selection decisions: Do privacy protection strategies bias the outcome?</i> – Exploring the main and interaction effects of information management strategy (omitting, lying), applicant race, and job type on an applicant’s assessment of qualifications and likelihood of job success. (Stone and Stone, 1987)	Disclosure behavior, willingness to disclose	Experiment multiple treatments	Managers, employees (U.S.) N=188	Regression analysis	Job application
<i>Personnel Selection Procedures and Invasion of Privacy</i> – Impact of personnel selection procedures on employees’ perceived privacy invasiveness, disclosure behavior, performance, and more. (Stone-Romero et al., 2003)	Privacy invasiveness, attitudes	Quantitative survey	Employees (U.S.) N=84, Students (U.S.) N=149	Correlation analysis	Job application

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Selection in the Information Age: The Impact of Privacy Concerns and Computer Experience on Applicant Reactions</i> – Impact of applicant privacy concerns on perceived justice, and subsequent effects on intention to apply, and perceived attraction of an organization. (Bauer et al., 2006)	Information privacy concerns	Quantitative, online survey	Students (U.S.) N=148 / applicants (U.S.) N=396	SEM	Job application
<i>Will it be Disclosure or Fabrication of Personal Information? An Examination of Persuasion Strategies on Prospective Employees</i> : – Investigating the effects of two different persuasion strategies on applicants' willingness to disclose or falsify information. (Li and Santhanam, 2008)	IUPC, information sensitivity, privacy concerns, willingness to disclose	Experiment multiple treatments	Students (U.S.) N=65	ANOVA, ANCOVA	Job application
<i>Late Payments and Leery Applicants: Credit Checks as a Selection Test</i> – Examining job applicants' perceptions of privacy invasion, fairness, and job relatedness on the use of credit checks by employers as a selection test. (Nielsen and Kuhn, 2009)	Privacy invasion, organizational justice theory	Quantitative, survey, case study	Students (U.S.) N=135	t-test, MANOVA	Job application
<i>Use of Social Networking Websites on Applicants' Privacy</i> – Extending the theoretical model of (Stone and Stone, 1990) to include the SNS context into workplace privacy. (Black et al., 2015)	Model of Stone and Stone 1990	Literature review	n.a.	Non-systematic	Job application

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Examining Applicant Reactions to the Use of Social Networking Websites in Pre-Employment Screening</i> – Impact of social network screening by employers on employees' privacy perceptions and their feeling of attraction towards an organization. (Stoughton et al., 2015)	Privacy invasion	Quantitative, online survey	Applicants (U.S.) N=175 / 208	ANOVA	Job application
<i>Job Applicants' Information Privacy-Protective Response: Exploring the Roles of Technology Readiness and Trust</i> – Job applicants privacy concerns. (Wang et al., 2015)	Privacy threats, technology readiness, trust	Quantitative, online survey	Students (U.S.) N=205	SEM	Job application
<i>Job Applicants' Information Privacy Protection Responses: Using Social Media for Candidate Screening</i> – Social Media for Candidate Screening – Applicants' intentions to protect information privacy of online social networks when requested for login data from potential employers. (Drake et al., 2016)	Information privacy protective responses	Quantitative, online survey	Students (U.S.); N=250	PLS-SEM	Job application
<i>Predicting Self-Disclosure in Recruitment in the Context of Social Media Screening</i> – Examine the potential mediation of applicants' willingness to trust an organization between the relationship of employees' perceived vulnerability to the use of information and overall self-disclosure, and the connection to completing applications. (Jeske et al., 2019)	Global privacy concerns, protection motivation theory, risk calculus, willingness to disclose	Experiment vignettes, online survey	Students (Ireland) N=222	Hierarchical regression	Job application



Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>The development and validation of the Privacy and Data Security Concerns Scale (PDSCS)</i> – Design and validate a scale to assess job applicants’ privacy and data security concerns, including item generation and content validation, item reduction, and construct and criterion validity. (Brady et al., 2021)	Inappropriate use of information, secure connection	Scale development process, multiple quantitative online surveys	Crowd workers N=148 / 452 / 349 / 539	EFA, CFA	Job application
<i>Privacy-preserving self-localization techniques in next generation manufacturing – An interdisciplinary view on the vision and implementation of smart factories</i> – Implementing a client-site semi-automatic computer vision based system, including an architecture, to provide accurate and reliable location information while preserving employees’ privacy in smart factories. (Lucke et al., 2008)	Workplace privacy	System engineering	n.a. (Germany)	n.a.	Privacy engineering
<i>Privacy and security threat analysis of the federal employee personal identity verification (PIV) program</i> – Conducting a formal threat analysis of identity cards being used by governmental employees, including proposing solutions to preserve privacy of cardholders. (Karger, 2006)	Anonymity	Privacy analysis	risk n.a.	Threat analysis	Privacy engineering
<i>Continuous RFID-enabled Authentication and its Privacy Implications</i> – Revealing privacy risks for employees through the use of continuous RFID authentication considering conventional architectures and systems. (Kurkovsky et al., 2010)	Soitude privacy	System engineering, privacy risk analysis	n.a.	Threat analysis	Privacy engineering

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>A Study on Privacy Preserving Data Leakage Prevention System</i> – Examining employee privacy violations caused by Data Leakage Prevention systems, and proposing a log anonymizing method and system architecture. (Kim and Kim, 2012)	Anonymity	System engineering, privacy risk analysis	en- n.a.	Trade-off analysis	Privacy engineering
<i>Preserving Privacy in Production</i> – Proposing two authentication methods, including architectures that use either anonymous credentials or organizational measures to ensure the anonymity or pseudonymity of employee logon behavior. The privacy risks are weighed for use in small and medium-sized enterprises. (Müller, 2014)	Privacy concerns, anonymity	System engineering, privacy risk analysis	en- n.a.	Participatory, Privacy engineering	Privacy engineering
<i>SpotMal: A hybrid malware detection framework with privacy protection for BYOD</i> – Analyzing malware threats in companies adopting BYOD, and developing an employee privacy preserving malware detection framework. (Gudo and Padayachee, 2015)	Anonymity, confidentiality	System engineering, privacy risk analysis	en- n.a.	Threat analysis	Privacy engineering
<i>Privacy Challenges for Process Mining in Human-Centered Industrial Environments</i> – Analyzing the privacy challenges of using process mining for data recorded from employees in industrial environments. Proposing context-based privacy guidelines according to the principles of the GDPR and Privacy by Design. (Mannhardt et al., 2018)	Privacy by design, data subject rights	Privacy risk analysis	n.a.	Requirements analysis	Privacy engineering

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>PRETSA: Event Log Sanitization for Privacy-aware Process Discovery</i> – Proposing an event log sanitization algorithm based on t-closeness to protect employees from trace linking attacks that would allow identity, membership, and attribute disclosure. (Fahrenkrog-Petersen et al., 2019)	Anonymity	System engineering, privacy analysis	en- n.a. risk	Formal threat analysis, experimental evaluation	Privacy engineering
<i>SensiTrack - A Privacy by Design Concept for Industrial IoT Applications</i> – Analysis of employee and company privacy aspects in the architecture and the limited control and configuration options in commercially available Bluetooth-based asset tracking systems. Development of a privacy-friendly asset tracking system using Privacy by Design. (Jandl et al., 2019)	Privacy by design	System engineering, human-centered design, study	en- Experts, Managers (Austria) N=6 case	Requirements analysis, threat analysis	Privacy engineering
<i>Design Principles for Digital Occupational Health Systems</i> – Developing principles for occupational health systems based on factors identified in previous research to reduce employees’ perceived privacy risks, while using ex ante storyboarding tests to determine which principles are most valued by employees. (Yassaee, 2017)	Privacy risk	Quantitative online survey	Employees (Switzerland) N=78	Correlation analysis	Privacy engineering

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Privacy Enhancing Technologies implementation: An investigation of its impact on work processes and employee perception</i> – Understanding effects of PETs implementation on data processing employees' work processes, including workload, communication level, and data access, as well as their perception towards the implementation. ( <a href="#">Gan et al., 2019</a> )	Privacy by design	Qualitative, semi-structured interviews	Data processing employees (Malaysia) N=9	Thematic analysis	Privacy engineering
<i>Company Privacy Dashboards: Employee Needs and Requirements</i> – Investigating employees' requirements towards transparency and self-determination, and designing a requirements model for the development of privacy dashboards. ( <a href="#">Polst et al., 2019</a> )	Privacy by design	Qualitative workshops	Employees (Germany); N=20	Requirements analysis	Privacy engineering
<i>Development of GDPR-Compliant Software: Document Management System for HR Department</i> – Gathering and analyzing requirements for GDPR-compliant software in a human resources department, with particular emphasis on procedures for obtaining consent and enforcing data subject rights of job applicants. ( <a href="#">Gonçalves et al., 2020</a> )	Privacy by design	Qualitative, requirements engineering, usability testing	HR managers N=n.a., users N=38	Requirements analysis, SUS	Privacy engineering
<i>Co-designing Employees' Data Privacy: a Technology Consultancy Company Use Case</i> – Designing a privacy cockpit for employees to enable transparency and control over personal information use. ( <a href="#">Sahqani and Turchet, 2021</a> )	Privacy by design	Qualitative, human-centered design, field study	Employees (Finland) N=15 / 25	Requirements analysis, SUS	Privacy engineering

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Privacy-Centered Design Principles for Employee-Determined Data Collection and Use in Personalized Assistance Systems</i> – Identification of personas and design principles to address requirements for employee-determined personal data collection and use. (Voss et al., 2021)	Control, transparency	Literature survey	n.a.	Systematic review	Privacy engineering
<i>Workplace Surveillance and Managing Privacy Boundaries</i> – Investigation of employees' privacy perceptions on electronic monitoring using privacy boundaries under CPM theory. (Watkins Allen et al., 2007)	CPM	Qualitative, structured interviews	Employees (U.S.) N=154	Grounded theory approach	Workplace monitoring
<i>E-mail Privacy in the Workplace</i> – Design and validate a predictive model for workplace e-mail privacy, employer monitoring activities, social relationship in organizations. (Snyder, 2010)	Communication boundary theory, privacy concerns	Quantitative, online survey	Employees (U.S.) N=324	PLS-SEM	Workplace monitoring
<i>Ethical implications of internet monitoring: A comparative study</i> – Examining differences in attitudes toward monitoring internet activities at the university as compared to the workplace. (Grodzinsky et al., 2010)	Privacy concern	Quantitative online survey	Students (U.S.) N=185	Chi-Sq	Workplace monitoring
<i>When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse</i> – Impact of employer's monitoring on employees perceived privacy invasion and computer abuse. (Posey et al., 2011)	Psychological reactance theory, privacy invasions	Quantitative, online survey	Employees (U.S.); N=439	SEM	Workplace monitoring

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Organizational Surveillance of Computer-Mediated Workplace Communication: Employee Privacy Concerns and Responses</i> – Examine employees’ perceived fairness depending on employees’ perceived computer-mediated workplace communication privacy. (Chory et al., 2016)	Computer mediated workplace communication privacy, access control, concern organizational infringement	Quantitative, online survey	Employees (U.S.) N=182	Regression	Workplace monitoring
<i>Perceptions of Internet-of-Things Surveillance by Human Resource Managers</i> – Examining HR managers’ opinions on using Internet of Things for monitoring employees’ information system use, location, biometrics, and behavior with and without notice. (Kaupins and Coco, 2017)	n.a.	Quantitative survey	HR managers (U.S.) N=174	Factor analysis, correlation analysis	Workplace monitoring
<i>Context Sensitive Technologies and Electronic Employee Monitoring: a Meta-Analytic Review</i> – Summarizing empirical studies on the impact of electronic surveillance in the workplace and identification of outcome variables. (Backhaus, 2019)	Privacy concerns	Literature review	n.a.	Systematic review	Workplace monitoring

Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>Modifying Consent Procedures to Collect Better Data: The Case of Stress-Monitoring Wearables in the Workplace</i> – Exploring the potential benefits and privacy implications of using wearables to monitor employee workplace stress from a management perspective, along with the implications for employee consent under the GDPR. Proposing enhanced and fine-grained control mechanisms for purposes, types of information, and recipients. (Gauttier, 2019)	Information sensitivity, data subject rights	Qualitative interview study	Managers (Italy, the Netherlands) N=15	n.a.	Workplace monitoring
<i>Dataveillance in the Workplace: Managing the Impact of Innovation</i> – Summarizing workplace surveillance literature and identifying research gaps. (McParland and Connolly, 2020)	non-specific	Literature review	n.a.	Systematic review	Workplace monitoring
<i>Using IoT devices for sensor-based monitoring of employees' mental workload: Investigating managers' expectations and concerns</i> – Examining the prevalence and role of expectations and concerns about mental workload monitoring among managers. (Pütz et al., 2022)	non-specific	Quantitative, online survey	Managers (Germany, UK, Spain) N=702	Bayesian regression analysis, multilevel analysis	Workplace monitoring
<i>Privacy in Organizations: Theoretical Issues, Research, Findings, and Protection Mechanisms</i> – Deriving a theoretical model for workplace privacy that infers from antecedents to (disclosure) behavior, and that is intended to be used to evaluate existing practices in the employee context. (Stone and Stone, 1990)	Expectancy theory, organizational privacy, calculus	Literature review	Employees (U.S.)	Non-systematic	Workplace privacy



Table A.1: Literature review summary

Work: Title – objective (author)	Privacy construct	Method	Sample	Analysis	Topic
<i>To Reveal or Conceal: Using Communication Privacy Management Theory to Understand Disclosures in the Workplace</i> – Examine employee self-disclosure in the workplace using CPM theory, focusing on interpersonal relationships. (Smith and Brunner, 2017)	CPM	Qualitative, online open-ended survey	Employees (U.S.) N=103	Grounded theory approach	Workplace privacy
<i>Privacy at Work: A Review and a Research Agenda for a Contested Terrain</i> – Summarizing workplace privacy and identifying research gaps, focusing on information privacy and work environment privacy. (Bhave et al., 2020)	Privacy work privacy	calculus, environment	sur-vey n.a.	n.a.	Workplace privacy



## APPENDIX STUDY I

## B.1 STUDY I — 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 aspects data
- Personal data
- Personal identifiable data
- 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.\**

## APPENDIX STUDY II

## C.1 STUDY II — ITEMS AND QUESTIONS (TRANSLATED)

The questions are listed below, divided into Part I and Part II of the survey.

## SURVEY PART I Demographics, perceived data sensitivity, and willingness to disclose

*\*All questions had a “do not answer” option.\**

## Demographics

---

Are you or have you been employed within the last few months, but not exclusively in self-employment?	[Yes; No]
Are you employed by more than one employer?	[Yes; No]
In which country are you primarily employed?	[List]
In what industry/sector does your employer operate?	[OECD industries [368]]
How many employees work for the company or organization?	[< 10; < 50; < 250; < 1000; ≥ 1000]
What professional group do you consider yourself to belong to?	[OECD professions [368]]
How long have you been employed by your current employer?	[Number input]
Do you have permanent employment?	[Yes; No]
What is your highest level of education?	[List]
What was your income (net earnings), i.e. wage or salary after deduction of taxes and social security contributions, in the last month?	[< 500; < 1000; < 1500; < 2000; < 2500; < 3000; < 3500; < 4000; ≥ 4000]
What is your age?	[number]
What is your biological sex?	[Diverse; Male; Female]
What is your citizenship (country)?	[List]
Are you currently primarily in education or training?	[Yes; No]

## Perceived data sensitivity

---

*\*All items measured on a six-point scale (“Not sensitive at all” ... “Very sensitive”)\**

Assume your current employer has / would have access to the following information and data about you / from you. How sensitive would you rate each of these pieces of information? [62 items in Figure 6.4]



### Willingness to disclose

---

*\*All items measured on a four-point scale ("No, under no circumstances" ... "Yes, actually always")\**

Suppose you were free to decide what data you would provide to your current employer. Would you give them access to the following information and data? [62 items in Figure 6.4]

### Survey feedback

---

How did you like this survey?	[1 - 5]
How did you process this survey?	
Did you work conscientiously on the questions?	[No, not at all; Rather not; Mostly yes; Yes, very]
Did you answer truthfully?	[No, not at all; Rather not; Mostly yes; Yes, very]
Is there anything else you would like to tell us or provide feedback on the survey?	[free text]

## SURVEY PART II Employee privacy antecedents

### Introduction

---

As an employee, you usually disclose a lot of information and data about yourself to your employer. Such data is also called personal data. Below are some examples of personal data that employers often have about their employees.

Many of your technical work devices also collect and use your personal-related data. Examples include computers, telephones, smart devices, and wi-fi routers. The personal data collected there is often also accessible to employers.

In the following, we ask you some questions about your personal attitude towards your current employer regarding personal data they know or might ask for from you.

### Data processing employee

---

Do you mainly deal with personal data yourself in the course of your job?	
I process personal data of my colleagues.	["Usually not", "Occasionally", "Rather regularly", "Very often"]
I process personal data of external parties (e.g., customer, partner).	["Usually not", "Occasionally", "Rather regularly", "Very often"]

### Antecedents

---

How do you respond to the following statements in relation to your current employer?

*\*All items measured on a six-point scale ("Strongly disagree" ... "Strongly agree")\**

*Benefits*

---

- (1) I have advantages when I disclose personal information to my employer instead of withholding it.
- (2) Withholding personal information from my employer only brings disadvantages. (reversed)
- (3) I benefit from disclosing information about myself to my employer.
- (4) I would suffer disadvantages if I did not disclose my personal information to my employer. (reversed)

*Collection concern*

---

- (1) It usually bothers me when my employer asks me for my personal data.
- (2) When my employer asks me for personal data, I sometimes think twice before providing it.
- (3) It bothers me to give personal data to my employer.
- (4) I'm concerned that my employer collects too much personal data about me.

*Privacy as a right*

---

- (1) Employee privacy laws should be strengthened to protect personal privacy against employers.
- (2) Employees need legal protection against employers' misuse of personal data.
- (3) If I were to write a constitution today, I would probably add employee privacy as a fundamental right.

*Risk beliefs*

---

- (1) In general, it would be risky to give my personal data to my employer.
- (2) There would be high potential for loss associated with giving my personal data to my employer.
- (3) There would be too much uncertainty associated with giving my personal data to my employer.
- (4) Providing my employer with my personal data would involve many unexpected problems.

*Trust*

---

- (1) I trust that my employer would keep my best interests in mind when dealing with my personal data.
- (2) My employer is in general predictable and consistent regarding the usage of my personal data.
- (3) My employer is always honest with me when it comes to using my personal data that I would provide.
- (4) My employer handles the personal data they collect about their employees in a proper and confidential way.

*Unauthorized secondary use*

---

- (1) My employer should not use my personal data for any purpose unless I have authorized it.
- (2) When I disclose my personal data to my employer for some reason, my employer should never use the data for any other reason.
- (3) My employer should never share my personal data with other companies unless it has been authorized by the individuals who provided the information.

*Complex privacy protection*

---

- (1) Employee privacy protection does not work. If my employer wants to, they can still access my data.
- (2) I do not have enough time to keep informed and apply privacy protection at work to protect my data from my employer.
- (3) Privacy protection has become so complex that I do not know how to protect my privacy against my employer anymore.

*Satisfaction with law*

---

- (1) Existing privacy laws and organizational practices provide a reasonable level of protection for employee privacy today.

*Knowledge privacy law*

---

Please answer the following questions truthfully and without help. Your responses will not affect the completion of the survey.

- (1) What is “informational self-determination”?
  - (a) The central demand of data-processing agencies.
  - (b) A fundamental right of German citizens. (correct)
  - (c) The central task of the Federal Data Protection Commissioner.
  - (d) A philosophical term.
  - (e) I do not know
- (2) The core principle of employee data protection is “prohibition subject to permission.” What does this mean?
  - (a) The employer may access employee personal data unless the employee explicitly expresses concern.
  - (b) The employer is prohibited from accessing employee personal data unless the employer has specific permission. (correct)
  - (c) The employer is allowed to access the employees’ personal data - only in some cases there is a reservation.
  - (d) I do not know

*Knowledge privacy law (continued)*

---

Please answer the following questions truthfully and without help. Your responses will not affect the completion of the survey.

- (3) According to German law, employees have a right to access all of their personal data that their employers keep about them.
  - (a) True (correct)
  - (b) False
  - (c) I don't know
- (4) Suppose you had given your employer consent to use certain personal data about you. You may revoke this consent at any time.
  - (a) True (correct)
  - (b) False
  - (c) I don't know
- (5) The EU Data Protection Directives only apply to personal data of customers, business partners and other external parties. However, the directives do not apply to the personal data of a company's employees.
  - (a) True
  - (b) False (correct)
  - (c) I don't know

*Survey feedback*

---

How did you like this survey?	[1 - 5]
How did you process this survey?	
Did you work conscientiously on the questions?	[No, not at all'; Rather not; Mostly yes; Yes, very]
Did you answer truthfully?	[No, not at all; Rather not; Mostly yes; Yes, very]
Is there anything else you would like to tell us or provide feedback on the survey?	[free text]

## C.2 STUDY II — ANALYSIS ENVIRONMENT

Statistical analysis was conducted in R. A detailed list of all packages used for analysis is provided in Table C.1.

Table C.1: R packages used for analysis.

Analysis	Package	Version	Src
All	R	4.0.3	<a href="#">[369]</a>
Bootstrapping CI	bootcorci	0.0.0.9000	<a href="#">[370]</a>
Exploratory Factor Analysis ( <a href="#">EFA</a> )	psych	2.1.3	<a href="#">[371]</a>
Exploratory Factor Analysis ( <a href="#">EFA</a> )	EFAtools	0.3.1	<a href="#">[372]</a>
Exploratory Factor Analysis ( <a href="#">EFA</a> )	polycor	0.8.0	<a href="#">[373]</a>
Confirmatory Factor Analysis ( <a href="#">CFA</a> ), Structural Equation Modeling ( <a href="#">SEM</a> )	lavaan	0.6.9	<a href="#">[374]</a>
Confirmatory Factor Analysis ( <a href="#">CFA</a> ), Structural Equation Modeling ( <a href="#">SEM</a> )	semTools	0.5.5	<a href="#">[375]</a>
Univariate and multivariate normality	MVN	5.8	<a href="#">[376]</a>
Imputation	missForest	1.4	<a href="#">[335]</a>
Linear Mixed-effects Model ( <a href="#">LMM</a> )	lme4	1.1.27.1	<a href="#">[377]</a>
Linear Mixed-effects Model ( <a href="#">LMM</a> )	lmerTest	3.1.3	<a href="#">[378]</a>
Robust Linear Mixed-effects Model ( <a href="#">LMM</a> )	robustlmm	2.4.4	<a href="#">[379]</a>
Latent Class Analysis ( <a href="#">LCA</a> )	poLCA	1.4.1	<a href="#">[380]</a>

## C.3 STUDY II — PARTICIPANT DEMOGRAPHICS

The full participants demographics are reported in Table C.2 below.

Table C.2: Participants' complete demographic data.

Description	Part 1	Part 2	Germany
Participants	N: 553	N: 393	
Sex	%	%	%
Diverse	0.2	0.0	<i>n. a.</i>
Female	39.6	41.7	46.5
Male	59.7	58.3	53.5
Age (years)	%	%	%
≤ 24	8.7	9.9	1.3
25 – 34	32.4	3.5	22.1
35 – 44	27.1	29.0	21.9
45 – 54	14.6	14.0	23.6
55 – 64	16.5	15.8	29.9
≥ 65	.7	.8	1.2
Education	%	%	%
University degree	58.2	58.3	16.9
Doctorate degree	5.4	4.6	<i>n. a.</i>
Master's degree	20.1	23.9	<i>n. a.</i>
Diploma's degree	13.9	11.7	<i>n. a.</i>
Bachelor's degree	18.8	18.1	<i>n. a.</i>
Technical school degree	5.2	3.8	<i>n. a.</i>
Apprenticeship / vocational training	14.6	16.8	<i>n. a.</i>
Advanced technical college or university entrance qualification	13.0	13.2	<i>n. a.</i>
Intermediate diploma	6.1	5.6	<i>n. a.</i>
Secondary school leaving certificate	5.4	4.6	<i>n. a.</i>
No general school degree	1.1	1.0	<i>n. a.</i>
No specification / other	1.8	1.3	<i>n. a.</i>
Job tenure (years)	%	%	%
≤ 4	47.3	46.6	27.6
5 – 9	24.1	24.4	19.1
≥ 10	28.6	29.0	44.3

*Table continues on the next page*

Participants' complete demographic data (*continued*).

Description	Part 1	Part 2	Germany
Participants	N: 553	N: 393	
Org. size	%	%	%
< 10	8.0	7.1	18.0
10 – 249	34.4	32.8	38.0
250 – 999	25.7	26.7	44.0
≥ 1k	31.6	33.1	
Net income (€ / month)	%	%	%
< 1k	9.2	12.2	13.0
1k < 2k	36.7	31.6	42.0
2k < 3k	36.9	36.4	29.0
3k < 4k	11.4	12.7	10.0
≥ 4k	5.8	7.1	6.0
Other	%	%	%
Permanent employment	75.8	75.6	<i>n. a.</i>
Multiple jobs	7.6	7.6	5.4
Nationality	%	%	%
Germany <sup>1</sup>	88.2	86.0	87.5
United States	2.0	2.0	<i>n. a.</i>
United Kingdom	1.5	1.5	<i>n. a.</i>
Greece	1.1	1.1	<i>n. a.</i>
Portugal	0.6	0.6	<i>n. a.</i>
Australia	0.5	0.5	<i>n. a.</i>
Bulgaria	0.5	0.5	<i>n. a.</i>
Egypt	0.5	0.5	<i>n. a.</i>
India	0.5	0.5	<i>n. a.</i>
Ireland	0.5	0.5	<i>n. a.</i>
Ukraine	0.5	0.5	<i>n. a.</i>
Argentina	0.3	0.3	<i>n. a.</i>
Brazil	0.3	0.3	<i>n. a.</i>
Colombia	0.3	0.3	<i>n. a.</i>
Estonia	0.3	0.3	<i>n. a.</i>
France	0.3	0.3	<i>n. a.</i>
Hungary	0.3	0.3	<i>n. a.</i>
Indonesia	0.3	0.3	<i>n. a.</i>

*Table continues on the next page*



Participants' complete demographic data (*continued*).

Description	Part 1	Part 2	Germany
Participants	N: 553	N: 393	
Italy	0.3	0.3	<i>n. a.</i>
Japan	0.3	0.3	<i>n. a.</i>
Lebanon	0.3	0.3	<i>n. a.</i>
Malaysia	0.3	0.3	<i>n. a.</i>
Mexico	0.3	0.3	<i>n. a.</i>
Pakistan	0.3	0.3	<i>n. a.</i>
Poland	0.3	0.3	<i>n. a.</i>
Romania	0.3	0.3	<i>n. a.</i>
Russian Federation	0.3	0.3	<i>n. a.</i>
Serbia	0.3	0.3	<i>n. a.</i>
Spain	0.3	0.3	<i>n. a.</i>
Switzerland	0.3	0.3	<i>n. a.</i>
Turkey	0.3	0.3	<i>n. a.</i>
Turkmenistan	0.3	0.3	<i>n. a.</i>
Vietnam	0.3	0.3	<i>n. a.</i>
Zimbabwe	0.3	0.3	<i>n. a.</i>
Industry (OECD, [368])	%	%	%
Information and communication	14.6	15.3	3.7
Professional, scientific and technical activities	12.5	14.2	5.8
Education	11.2	11.7	6.8
Human health and social work activities	9.2	10.4	13.2
Financial & insurance activities	9.0	6.9	2.9
Public administration and defense; Compulsory social security	7.8	8.4	6.9
Manufacturing	11.0	9.5	19.0
Wholesale & retail trade	6.0	6.1	13.6
Transportation and storage	3.4	3.3	5.1
Administrative and support service activities	3.3	4.1	5.1
Electricity, gas, steam, air con. and water supply; sewerage, waste management and remediation activities	1.8	1.3	1.4
Accommodation and food service activities	1.8	1.5	3.7
Arts, entertainment and recreation	1.8	1.8	1.4
Construction	1.4	1.3	6.7

Table continues on the next page

Participants' complete demographic data (*continued*).

Description	Part 1	Part 2	Germany
Participants	N: 553	N: 393	
Real estate activities	1.3	1.0	0.5
Other service activities	1.1	0.5	2.8
Agriculture, hunting, forestry and fishing	0.7	1.0	1.2
Professional group (Federal Labor Office, [381])	%	%	%
Science, geography & information technology	21.0	19.3	4.2
Business org., accounting, law & administration	21.0	17.8	20.4
Health, social services, teaching & education	16.5	18.1	18.8
Commercial services, trade, hotel & tourism	10.5	12.2	11.4
Linguistics, literature, humanities, social sciences, economics, media, arts, culture & design	8.1	9.4	2.7
Mining, production & manufacturing	6.0	6.1	21.0
Transport, logistics	3.1	3.1	6.4
Construction, architecture, geodetic surveying and construction engineering	2.7	3.1	6.1
Protection, security and surveillance	1.8	2.0	1.1
Military	0.5	0.3	n. a.
Agriculture, forestry and animal husbandry	0.8	0.8	0.7
Cleaning	0.5	0.5	2.5

Note. Part 1  $\supset$  Part 2; Percentages include missing responses (omitted for brevity). Max. non-response rate is  $\leq 2\%$ .

*End of table*

#### C.4 STUDY II — PERSONAL DATA ELEMENTS AND GROUPS OF PERSONAL DATA

A summary of the five different studies and contexts compared in Section 6.3 is provided in Table C.3. The table also includes the descriptive statistics about the scores for Perceived Data Sensitivity (PDS) and Willingness to Disclose (WTD) from this study, as well as the scores extracted from related work. Furthermore, the average scores for all personal data items and for all studies compared in Section 6.3 and depicted in Figure 6.4 are reported in Table C.4. In addition, Table C.4 also includes a mapping between the different personal data items and the eight different groups of personal data investigated in Section 6.4.2.

Table C.3: Study II - Comparison of different studies and personal data items.

Description		This study	[274]	[274]	[271]	[273]
Study and sample	Year	2021	2017	2017	2018	2020
	Context	Employees	Marketing	Marketing	Online users	Online users
	Country	DEU	USA	BRA	DEU	SAU
	N	553	406	401	592	508
All personal data items by study						
Items and scores	Num. items	62	42	42	40	35
	Perceived data sensitivity					
	min	2.5	4.5	3.0	2.8	2.4
	max	9.6	9.4	9.1	9.3	9.7
	average	6.0	7.0	5.6	6.4	6.1
	median	6.0	6.9	5.7	6.7	6.3
	Willingness to disclose					
	min	1.5	1.7	1.7	n. a.	n. a.
	max	9.1	6	6.3	n. a.	n. a.
	average	5.4	3.8	4.2	n. a.	n. a.
	median	5.4	3.8	4.4	n. a.	n. a.
	Intersection of the studied personal data items between all studies					
	Num. items	28	28	28	28	28
	Perceived data sensitivity					
	min	3.0	2.9	4.5	3.0	3.8
	max	9.7	9.6	9.4	9.1	9.3
	average	6.2	6.5	6.9	5.6	6.6
	median	6.4	6.7	6.9	5.6	7.0
	Willingness to disclose					
	min	1.5	1.7	1.7	n. a.	n. a.
	max	9.1	5.9	6.3	n. a.	n. a.
	average	4.7	3.7	4.1	n. a.	n. a.
	median	4.0	3.5	4.4	n. a.	n. a.

Table C.4: Study II - Personal data elements' average scores in different studies and assignment to different groups of personal data.

Personal data	Scaled average scores ( $1 \leq \bar{x} \leq 10$ )								Groups of personal data					
	Employment		Marketing		Marketing		Online		Predefined groups			Latent groups		
	DEU [this]		USA [274]		BRA [274]		DEU [271]	SAU [273]	IDENT	MASTER	GDPR	SENS	NOTSENS	PII WORK
	PDS	WTD	PDS	WTD	PDS	WTD	PDS	PDS						
Hair color	2.5	8.1					3.2					✓		
Profession	2.9	9.1	4.6	5.9	4.0	6.0	4.3	3.1	✓					✓
Language skills	3.0	8.9							✓					
Business trip	3.2	8.8												✓
Employment	3.2	8.6							✓					✓
Shift plans	3.2	8.6												✓
Education	3.3	8.9							✓					
Professional appoint.	3.4	8.6												✓
Priv. postal code	3.5	7.9	4.9	5.6	4.4	5.2	4.6	4.3	✓					
Place of birth	3.5	8.0	5.8	4.8	3.9	5.8	4.5		✓					
Working hours	3.5	8.8							✓					
Body size	3.6	7.2	4.5	5.9	3.2	6.1	3.8	3.4				✓		
No. of children	3.9	7.4	4.6	5.7	3.7	5.9	4.3	3.5	✓					
Driving license	4.0	7.5	8.4	2.2	7.1	2.8			✓					
Name of pet	4.0	5.8					2.8	2.4						
Professional contacts	4.3	7.3												
Family status	4.4	7.4							✓					
Work contract	4.5	8.3							✓					
Picture	4.6	7.1	6.4	4.0	5.5	4.3	7.0	6.9						
Home address	4.7	7.8	6.9	4.4	6.0	4.5	7.5	6.4	✓	✓				✓
Application documents	4.8	8.2								✓				
Social security No.	4.9	7.6	9.4	1.7	7.7	2.7	7.9	7.7	✓	✓				✓
Health insurance No.	5.0	7.5	8.4	2.1	6.5	2.9	7.9	7.1	✓	✓	✓			✓
Priv. license plate	5.2	5.4	6.6	3.0	6.1	3.1	5.7	5.0	✓					
Income level	5.3	6.2	6.7	4.6	5.7	3.8	6.9	7.3						
Union membership	5.4	5.5									✓			
Account No.	5.5	7.5	9.2	1.7	7.8	2.2	9.3	8.8	✓	✓				✓
Priv. phone No.	5.6	6.3	6.8	4.1	5.0	5.0	7.5	5.1	✓	✓				
Performance data	5.6	6.9								✓				
Mother's maiden name	5.8	4.3	7.2	3.5	4.9	4.4	5.0	4.1						
Body weight	6.0	4.7	5.6	5.1	3.8	5.6	5.0	3.7			✓			
Priv. email address	6.0	5.8	6.4	5.1	4.8	5.7	6.0	5.1	✓	✓				
Vacation resort	6.0	4.5												
Sideline activities	6.3	5.5								✓				
Fitness	6.6	3.8					4.5	3.1			✓			
Religious affiliation	6.7	3.6	5.0	5.6	3.2	6.3	4.0	3.0	✓		✓			
Pregnancy	6.7	5.3									✓			
Formal warning	6.8	4.2												
Passport No.	7.0	4.0	8.4	2.1	6.5	2.7	8.2	8.7	✓					
Social network profile	7.1	2.8	6.1	4.0	4.8	4.8	6.0	5.4						
Digital signature	7.2	4.1	8.2	2.6	7.4	2.6	8.0	8.6	✓					
Voiceprint	7.3	3.4	7.3	2.7	6.0	3.5	7.0	7.2	✓		✓			
Shopping behavior	7.5	2.6					5.5	4.9						
Political opinion	7.7	3.0	4.7	5.3	3.0	5.7	5.3	5.9			✓			
Sexual Orientation	7.7	3.0	5.3	5.3	3.4	6.0	6.0				✓			
IP add.	7.7	3.0	7.6	3.0	6.8	3.0	8.0	7.8	✓					
Criminal record	7.7	4.0									✓			
Intention changing job	7.8	3.6												
Alcohol consumption	7.9	2.6					5.0							
Law enforcement rec.	8.2	3.5	7.6	2.9	4.3	4.7	7.0	8.2			✓			
Creditworthiness	8.5	2.8	7.9	2.9	7.2	2.4	7.7	8.6				✓		
Medical history	8.5	3.2	8.4	3.0	5.2	4.7	7.5	6.7			✓	✓		
Browsing history	8.6	2.3					7.0	6.4						
Medication	8.6	2.9					6.5	5.8			✓	✓		
GPS location	8.7	2.4	6.8	3.4	5.9	3.4	7.5	7.1	✓			✓		
Fingerprint	8.7	2.7	8.5	2.3	7.1	2.6	8.0	9.2	✓		✓			
Credit card No.	8.7	2.6	9.2	1.9	8.3	2.1	8.7		✓					
Priv. appointments	8.7	2.7												
Online dating activities	8.9	1.5					6.5	6.2			✓			
Personal problems	9.0	2.4										✓		
Genetic data	9.2	1.7	8.4	2.2	6.0	3.3	8.0		✓		✓	✓		
Passwords	9.6	1.7	9.3	1.7	9.1	1.7	9.3	9.7	✓					

## C.5 STUDY II — DEMOGRAPHIC DIFFERENCES PRIVACY ANTECEDENTS

Results of our analysis for differences in our participants' demographics between the five different privacy antecedents investigated as part of our causal model are presented in Table C.6 and in Table C.5, respectively. To test for differences in age (younger vs. older), nationality (German vs. not German), sex (male vs. not male), job tenure ( $\leq 6$  years vs.  $> 6$  years), number of employers (one vs. more than one), permanent employment (yes vs. no), education (university degree vs. no university degree), and company size (working in SME vs. not working in SME), demographics were included as binary exogenous variables in a SEM that included all five privacy antecedents. The SEM was run with polychoric correlations and the robust estimator WLSMV. Differences with respect to participants' industry and professional group were tested using Kruskal-Wallis test.

Table C.5: Results Kruskal-Wallis test demographic differences by privacy antecedents.

Demographics		COLL	PRGT	RSKB	TRST	UNAU	CPLX	KNWL
Industry	H	23.126	16.96	24.913	31.33	32.674	19.315	18.662
	df	17	17	17	17	17	17	17
	p	0.145	0.457	0.097	0.0182	0.0124	0.311	0.348
	$\eta^2$	0.017	0.038	0.021	0.038	0.043	0.006	0.004
Professional group	H	9.347	10.895	8.067	2.933	15.526	11.174	22.706
	df	11	11	11	11	11	11	11
	p	0.59	0.452	0.707	0.992	0.16	0.429	0.019
	$\eta^2$	-0.004	-0.004	-0.008	-0.004	0.012	0.000	0.031

Note. N = 393

Table C.6: Results covariates analysis of demographic differences by privacy antecedents.

		BFTS			COLL			RSKB		
		Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
Regressions										
Is male	→	-.08	[-.35, .19]	-.04	.16	[-.10, .42]	.08	.24	[-.04, .52]	.12
German	→	.09	[-.28, .46]	.03	-.02	[-.39, .35]	-.01	-.12	[-.50, .26]	-.04
Works for SME	→	.28	[.03, .54]	.14*	-.07	[-.31, .17]	-.03	-.12	[-.37, .13]	-.06
University deg.	→	.23	[-.02, .48]	.11	.10	[-.14, .34]	.05	-.10	[-.35, .15]	-.05
Age (is older)	→	-.06	[-.36, .24]	-.03	-.16	[-.44, .12]	-.08	-.07	[-.36, .22]	-.04
Permanent empl.	→	.18	[-.11, .47]	.08	-.07	[-.36, .22]	-.03	-.04	[-.35, .27]	-.02
Job tenure (longer)	→	-.13	[-.42, .16]	-.06	-.08	[-.36, .19]	-.04	.03	[-.25, .31]	.02
Multiple employers	→	-.01	[-.41, .39]	.00	-.29	[-.71, .13]	-.07	-.45	[-.95, .05]	-.12
Pers. data processor	→	.17	[-.08, .41]	.08	.06	[-.17, .30]	.03	.01	[-.24, .26]	.00
		TRST			UNAU			CPLX		
		Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
Regressions										
Is male	→	-.04	[-.30, .21]	-.02	-.13	[-.41, .16]	-.06	-.10	[-.36, .17]	-.05
German	→	.03	[-.33, .38]	.01	-.12	[-.54, .29]	-.04	-.20	[-.57, .17]	-.07
Works for SME	→	.12	[-.11, .36]	.06	-.12	[-.39, .15]	-.06	-.12	[-.36, .13]	-.06
University deg.	→	.00	[-.25, .25]	.00	-.21	[-.49, .08]	-.10	.15	[-.10, .40]	.07
Age (is older)	→	.16	[-.11, .43]	.08	.47	[.15, .78]	.22**	-.16	[-.44, .12]	-.08
Permanent empl.	→	.04	[-.24, .32]	.02	-.07	[-.38, .25]	-.03	-.04	[-.33, .25]	-.02
Job tenure (longer)	→	.09	[-.18, .35]	.04	-.02	[-.32, .29]	-.01	.06	[-.21, .32]	.03
Multiple employers	→	.30	[-.16, .76]	.08	-.03	[-.50, .45]	-.01	.28	[-.15, .72]	.07
Pers. data processor	→	-.08	[-.31, .16]	-.04	.11	[-.16, .38]	.05	.12	[-.12, .35]	.06
		KNWL			PRGT			SATL		
		Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$	Est.	CI <sub>95</sub>	$\beta$
Regressions										
Is male	→	.11	[-.16, .38]	.05	.27	[-.01, .55]	.13	.05	[-.23, .32]	.02
German	→	.49	[.10, .88]	.17*	-.38	[-.72, -.04]	-.13*	.03	[-.34, .40]	.01
Works for SME	→	.23	[-.01, .48]	.11	-.06	[-.30, .19]	-.03	-.24	[-.50, .02]	-.1
University deg.	→	.18	[-.07, .43]	.09	-.14	[-.39, .11]	-.06	-.01	[-.27, .25]	.00
Age (is older)	→	-.06	[-.33, .22]	-.03	-.26	[-.54, .02]	-.12	.26	[-.05, .58]	.11
Permanent empl.	→	.18	[-.14, .50]	.07	-.02	[-.31, .28]	-.01	.13	[-.18, .44]	.05
Job tenure (longer)	→	-.14	[-.42, .14]	-.06	.04	[-.23, .32]	.02	-.07	[-.39, .26]	-.03
Multiple employers	→	.10	[-.44, .64]	.03	.57	[.12, 1.02]	.14*	-.04	[-.47, .39]	-.01
Pers. data processor	→	.36	[.11, .60]	.17**	.30	[.06, .54]	.14*	.10	[-.15, .36]	.04



## C.6 STUDY II — COVARIATES SEM ANALYSIS

Results of our analysis for differences in our participants' demographics between the [WTD](#) and the [PDS](#) for different groups of personal data are presented in Table [C.7](#). To test for differences in age (younger vs. older), nationality (German vs. not German), sex (male vs. not male), job tenure ( $\leq 6$  years vs.  $> 6$  years), number of employers (one vs. more than one), permanent employment (yes vs. no), education (university degree vs. no university degree), and company size (working in SME vs. not working in SME), demographics were included as binary exogenous variables in the [SEM](#) used for analysis in Section [6.5](#). The results presented in Table [C.7](#) thus complement the results presented in Table [6.7](#) and Table [6.8](#).

Table C.7: Results SEM analysis demographic variables.

Regressions demographics on WTD and PDS for different groups of personal data: DEMO → {WTD, PDS}													
Regressions		ALL			GDPR			IDENT			MASTER		
		Est.	CI <sub>95</sub>	β	Est.	CI <sub>95</sub>	β	Est.	CI <sub>95</sub>	β	Est.	CI <sub>95</sub>	β
Is male	→ WTD	-.09	[-.36, .17]	-.04	-.07	[-.32, .18]	-.03	-.10	[-.35, .16]	-.04	-.08	[-.33, .16]	-.03
Is German	→ WTD	.49	[.10, .88]	.13*	.35	[-.07, .78]	.09	.34	[-.01, .69]	.09	.57	[.22, .93]	.16**
Works for SME	→ WTD	-.01	[-.24, .22]	.00	.04	[-.18, .26]	.01	-.02	[-.26, .22]	-.01	-.01	[-.24, .21]	.00
University deg.	→ WTD	.08	[-.16, .32]	.03	-.15	[-.38, .08]	-.06	.06	[-.18, .29]	.02	.13	[-.10, .37]	.05
Age (is older)	→ WTD	.12	[-.14, .39]	.05	-.02	[-.25, .21]	-.01	.17	[-.10, .44]	.07	.06	[-.20, .33]	.03
Fulltime	→ WTD	.19	[-.10, .48]	.06	.24	[-.08, .56]	.08	.18	[-.12, .48]	.06	.01	[-.26, .29]	.00
Job tenure	→ WTD	-.12	[-.37, .14]	-.04	.03	[-.20, .26]	.01	-.02	[-.29, .26]	-.01	-.15	[-.41, .10]	-.06
Mult. employers	→ WTD	-.09	[-.54, .36]	-.02	.14	[-.30, .59]	.03	-.16	[-.67, .34]	-.03	-.32	[-.78, .14]	-.07
Data processor	→ WTD	.08	[-.14, .31]	.03	.13	[-.09, .35]	.05	.04	[-.18, .27]	.02	.08	[-.13, .30]	.03
Is male	→ PDS	-.33	[-.58, -.07]	-.14*	-.30	[-.56, -.04]	-.13*	-.21	[-.47, .04]	-.10	-.31	[-.56, -.07]	-.15*
Is German	→ PDS	.06	[-.30, .41]	.02	.42	[.05, .79]	.13*	-.12	[-.47, .22]	-.04	-.08	[-.39, .22]	-.03
Works for SME	→ PDS	-.12	[-.34, .11]	-.05	-.19	[-.41, .04]	-.08	.00	[-.23, .23]	.00	-.05	[-.28, .17]	-.02
University deg.	→ PDS	-.06	[-.29, .18]	-.03	.25	[.00, .49]	.11	-.21	[-.45, .04]	-.09	-.14	[-.37, .09]	-.07
Age (is older)	→ PDS	-.19	[-.48, .09]	-.09	-.16	[-.44, .12]	-.07	-.24	[-.52, .03]	-.11	-.15	[-.42, .11]	-.07
Fulltime	→ PDS	.16	[-.12, .42]	.06	.14	[-.15, .43]	.05	.16	[-.11, .43]	.06	.15	[-.11, .41]	.06
Job tenure	→ PDS	-.04	[-.30, .22]	-.02	-.13	[-.40, .14]	-.06	-.04	[-.30, .22]	-.02	.01	[-.23, .25]	.00
Mult. employers	→ PDS	.11	[-.28, .49]	.03	-.12	[-.48, .24]	-.03	-.08	[-.52, .36]	-.02	.13	[-.32, .59]	.03
Data processor	→ PDS	-.02	[-.25, .21]	-.01	-.02	[-.26, .22]	-.01	.00	[-.22, .23]	.00	-.01	[-.22, .20]	.00
Regressions		NOTSENS <sup>L</sup>			PII <sup>L</sup>			SENS <sup>L</sup>			WORK <sup>L</sup>		
		Est.	CI <sub>95</sub>	β	Est.	CI <sub>95</sub>	β	Est.	CI <sub>95</sub>	β	Est.	CI <sub>95</sub>	β
Is male	→ WTD	-.21	[-.44, .03]	-.09	-.09	[-.33, .15]	-.04	.02	[-.22, .26]	.01	-.06	[-.33, .21]	-.03
Is German	→ WTD	.14	[-.16, .44]	.04	-.01	[-.35, .33]	.00	.12	[-.20, .44]	.03	.23	[-.10, .55]	.07
Works for SME	→ WTD	.02	[-.20, .24]	.01	-.22	[-.43, -.01]	-.1*	.12	[-.12, .35]	.05	-.11	[-.33, .12]	-.05
University deg.	→ WTD	.18	[-.05, .41]	.08	.07	[-.16, .30]	.03	-.03	[-.29, .24]	-.01	.11	[-.11, .34]	.05
Age (is older)	→ WTD	-.07	[-.32, .18]	-.03	-.12	[-.38, .13]	-.06	-.27	[-.55, .01]	-.11	-.01	[-.27, .25]	.00
Fulltime	→ WTD	-.13	[-.43, .17]	-.05	-.32	[-.59, -.05]	-.12*	-.31	[-.56, -.06]	-.11*	-.14	[-.40, .13]	-.05
Job tenure	→ WTD	.19	[-.04, .42]	.08	-.04	[-.28, .20]	-.02	.33	[.05, .61]	.14*	.12	[-.11, .35]	.05
Mult. employers	→ WTD	-.20	[-.59, .20]	-.04	.06	[-.28, .40]	.01	-.20	[-.62, .22]	-.04	.07	[-.40, .53]	.02
Data processor	→ WTD	-.07	[-.27, .14]	-.03	-.16	[-.38, .06]	-.07	-.21	[-.44, .01]	-.09	-.16	[-.40, .07]	-.07
Is male	→ PDS	.00	[-.22, .23]	.00	.14	[-.09, .37]	.07	.04	[-.21, .28]	.02	.08	[-.16, .32]	.04
Is German	→ PDS	.09	[-.22, .40]	.03	-.23	[-.56, .09]	-.08	.07	[-.21, .35]	.02	-.14	[-.48, .20]	-.05
Works for SME	→ PDS	.09	[-.12, .31]	.04	.17	[-.05, .38]	.08	-.02	[-.24, .20]	-.01	.03	[-.19, .26]	.02
University deg.	→ PDS	-.02	[-.24, .21]	-.01	.00	[-.23, .22]	.00	-.05	[-.28, .18]	-.03	.02	[-.22, .25]	.01
Age (is older)	→ PDS	-.08	[-.34, .18]	-.04	.05	[-.20, .30]	.03	-.07	[-.34, .19]	-.04	.13	[-.13, .39]	.06
Fulltime	→ PDS	.11	[-.16, .38]	.05	.00	[-.25, .25]	.00	-.07	[-.35, .21]	-.03	-.04	[-.29, .22]	-.02
Job tenure	→ PDS	.12	[-.13, .37]	.06	-.06	[-.31, .19]	-.03	.23	[-.03, .48]	.11	-.02	[-.29, .24]	-.01
Mult. employers	→ PDS	-.23	[-.64, .18]	-.06	-.36	[-.75, .04]	-.09	-.27	[-.66, .12]	-.07	-.43	[-.88, .02]	-.11
Data processor	→ PDS	.04	[-.17, .25]	.02	.11	[-.10, .32]	.05	-.04	[-.26, .19]	-.02	.12	[-.10, .33]	.06

Note. N = 393

\*: p &lt; .05 \*\*: p &lt; .01 \*\*\*: p &lt; .001








β: standardized path coefficient (measure of effect size [339])

<sup>L</sup>: Latent groups



## APPENDIX STUDY III

## D.1 STUDY III — PROTOCOL STUDY 2: USER GOALS AND REQUIREMENTS (TRANSLATED)

 <p>Workshop Privacy tools for daily work</p> 	 <p>We would like to have a discussion in which...</p> <p>...all perspectives...</p> <p>...your opinions...</p> <p>are important and should be addressed</p>
 <p>It is okay to follow up on what others have said or to present a different opinion.</p> <p>In doing so, please allow everyone to express themselves and to speak up.</p>	<p>1</p> <p>What is <b>your name</b> and what is <b>the first thing</b> that comes to mind when you think of <b>data protection</b> in connection with your <b>everyday work</b>?</p>
<p>2</p> <p>In what cases would such a tool have been...</p> <ul style="list-style-type: none"> <li>• useful during the last week?</li> <li>• useful at all in everyday work?</li> </ul>	<p>3</p> <p>Suppose you need to process data.</p> <p>Where do you encounter these tasks in your everyday working life?</p> <p>You would like to:</p> <ul style="list-style-type: none"> <li>• collect missing data</li> <li>• obtain permission to use the data</li> <li>• inform about the transfer of this data to third parties</li> </ul> 
<p>3</p> <p>Suppose you need to process data.</p> <p>What aspects are particularly important or helpful in solving these tasks in your daily work?</p> <p>Collect your initial ideas, write each answer on a single <b>green</b> card.</p> 	<p>3</p> <p>Suppose you need to process data.</p> <p>Which aspects are particularly disturbing and hinder you in your work?</p> <p>Collect your initial ideas, write each answer on a single <b>red</b> card</p> 

3

Suppose you need to process data.

... and make a processing request to

- collect missing data
- obtain consent for data use
- inform about the transfer of this data to third parties

3

Suppose you make a **processing request**.

What specific

- information / instructions
- input / answer options

would you like to have or could be helpful?

*Collect your initial ideas, write each answer on a single white card.*

3

Suppose you make a **processing request**.

Collect your ideas on the whiteboard!

3


Suppose you make a **processing request**.

Which aspects are of

- primary
- secondary

importance?

Break



4

Inspect data handling and use.

- Data overview
- Access rights & accesses
- Data use / disclosure

4

You would like to check **possibilities of use** and **usage of data**.

What specific

- information / instructions
- input / answer options

would you like to have or could be helpful?

*Collect your initial ideas, write each answer on a single yellow card.*

4

You would like to check **possibilities of use** and **usage of data**.

Collect your ideas on the whiteboard!

4

You would like to check **possibilities of use** and **usage of data**.

Which aspects are of


- primary
- secondary

importance?

5

Suppose you had a privacy tool at your disposal.

What **information and content** would you like to see when you **open** the tool?




*Collect your initial ideas, write each answer on a single blue card.*

**5**

Suppose you had a privacy tool at your disposal.

What do you think a **helpful representation** looks like?



*Use the whiteboard to synthesize your collected ideas into a helpful representation.*


**5** We would like you to help us make the information flows of a privacy tool as useful as possible. And we would like to know the reasons why the tool becomes a burden.

Is the summary **complete**?

What have we **missed**?

Are there **other aspects** we should have talked about more?

## D.2 STUDY III — PROTOCOL STUDY 3: USABILITY WALKTHROUGH (TRANSLATED)

We would like to have a discussion in which...


...all perspectives...

...your opinions...

are important and should be addressed

**1**

What is your **name** and have you already encountered **data protection issues** this year?



It is okay to follow up on what others have said or to present a different opinion.

In doing so, please allow everyone to express themselves and to speak up.

**1 Corporate privacy tools**

- Central tools for all employees
- Overview of how their own data are used
- Permission and revocation of processing requests
- Collection and preparation of data protection-relevant information

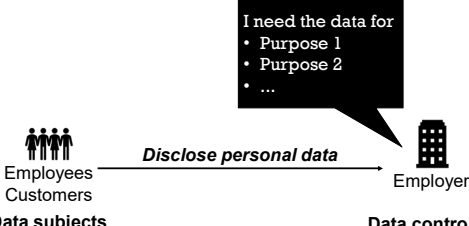
**2 Scenario**

You need to process personal data.

It is unclear

- what is the legal basis for the processing;
- whether permission is required;
- whether the required data are incomplete or outdated.

**2 Aspects of data protection law**




Employees  
Customers  
Data subjects

Disclose personal data

Employer  
Data controller

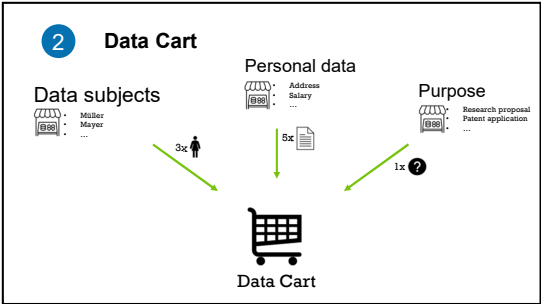
**2 Aspects of data protection law**



Categories of data subjects  
Categories of personal data  
Purpose  
Recipients

Record of processing activities  
e.g. research proposal

Real processing activity



**2 Data Cart**

When you think about your everyday work, how would you fill **your Data Cart**?

- How many data subjects, data categories, and purposes end up in your Data Cart?
- How do your Data Cards differ?
- What do you pack first?

**3 Processing data with Data Cart**

Data Cart enables you to process personal data in a legally compliant and transparent manner.

In Data Cart, the various elements and aspects of the processing are compiled and organized until the processing is completed.

**3 Processing data with Data Cart**

- 1 Purpose selection
- 2 Select personal data and data subjects
- 3 Provide additional information
- 4 Verify and send request
- 5 Receive permission and manage data

**3 Processing data with Data Cart**

- 1 Purpose selection
- 2 Select personal data and data subjects
- 3 Provide additional information
- 4 Verify and send request
- 5 Receive permission and manage data

**3 Processing data with Data Cart**

- 1 Purpose selection
- 2 Select personal data and data subjects
- 3 Provide additional information
- 4 Verify and send request
- 5 Receive permission and manage data

**3 Processing data with Data Cart**

- 1 Purpose selection
- 2 Select personal data and data subjects
- 3 Provide additional information
- 4 Verify and send request
- 5 Receive permission and manage data

**3 Processing data with Data Cart**

- 1 Purpose selection
- 2 Select personal data and data subjects
- 3 Provide additional information
- 4 Verify and send request
- 5 Receive permission and manage data

**3 Processing data with Data Cart**

**3 Processing data with Data Cart**



### 3 Processing data with Data Cart

- 1 Purpose selection
- 2 Select personal data and data subjects
- 3 Provide additional information
- 4 Verify and send request
- 5 Receive permission and manage data

### 3 Processing data with Data Cart

Suppose you had Data Cart available to you at work.

Use the tool to plan processing and obtain any data and permissions you may need.

### 3 Processing data with Data Cart

Online survey

Task description

Sketches of the user interface

Your notes: describe procedure, note questions and comments

Navigate to the next screen

### 3 Processing data with Data Cart

How did you proceed?

### 3 Processing data with Data Cart

Which functions / input options were missing?

### 3 Processing data with Data Cart

Which information was:

- helpful?
- missing?
- unintelligible?

### 3 Processing data with Data Cart

What information / input options are missing?

### 3 Processing data with Data Cart

How does this information help you perform your task?

### 3 Processing data with Data Cart

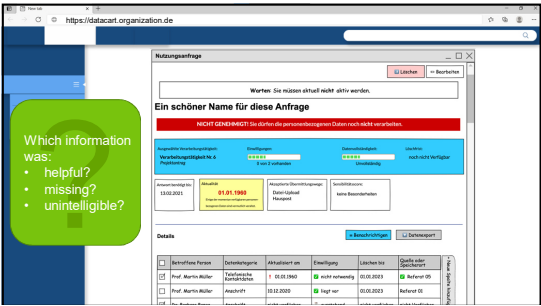
Which information is relevant?

- helpful?
- missing?
- unintelligible?

### 3 Processing data with Data Cart

Which information was:

- helpful?
- missing?
- unintelligible?



**6 Data Cart in your department**

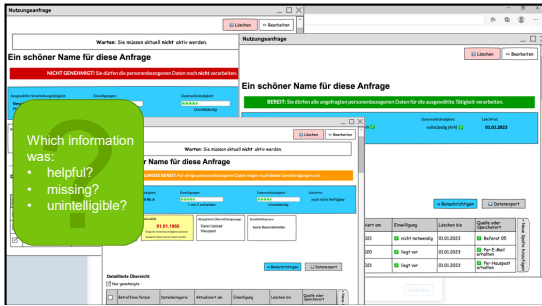
How **useful** or **helpful** would this tool be in your everyday work?

**7** We would like you to help us make the information flows of a privacy tool as useful as possible. And we would like to know the reasons why the tool becomes a burden.

Is the summary **complete**?

What have we **missed**?

Are there **other aspects** we should have talked about more?



**6 Data Cart in your department**

What **problems** do you see with the use of such a tool in your everyday work?

D.3 STUDY III — PROTOCOL STUDY 4: FORMATIVE USABILITY STUDY (TRANSLATED)

Usability study  
Privacy tools for  
daily work

Scenario

Ms Wagner-Müller has to **process personal data**.

It is often unclear to her

- what the **legal basis** looks like;
- whether **permission** is required;
- whether the required data are **incomplete** or **outdated**.

Your profile

Name: Verena Wagner-Müller Age: 41

Job: University  
University Road 1-10  
51234 University city

Occupation: Research consultant in Unit R01 Science and Technology Transfer

Study procedure

Solve tasks using Data Cart      Questionnaire      Short interview

### Study procedure



Think out loud!



You do things right -  
always!

### A new working day begins

Open the Data Cart tool and get a quick overview first:

[https://\[removed\].com/tool](https://[removed].com/tool)

Login data:

User name: Verena Wagner-Müller

Password: mww0954

### Event planning

You are planning an event on patent law in the near future. Just now, **Dr. Josefa Hauser** from the **department F04** confirmed that she would like to be a speaker at the event.

You are pleased about the acceptance and would like to **advertise** the event **on** your university's **website**. In the article, Dr. Hauser should be mentioned with her **full name, title, and office address**. Unfortunately, you do not know the official address by heart. You also know that personal data may only be processed with permission.

**Task:** Create a new Data Cart and obtain **all** personal data and permissions **mentioned** that you can create the **post for the website**.

### Invitations

The planned event is to be held in **3 weeks** and the entire **Unit 01** is to attend the event. For the list of participants you need the **full name, title and email address**.

**Pictures** are also to be taken at the event.

You need all data and consents **at least one week** in advance. You remember that your supervisor once said that you can invite people to events directly via Data Cart.

**Task:** Create a new data basket to invite Unit 01 to the event and obtain the required personal data and permissions.

### Check changes and updates

You just have some spare time and want to check if something has changed in one of the active Data Carts.

Respond to Data Carts with notifications and new messages.

**Task:** Respond to new messages.

### Further invitation to the event

Your supervisor asks you to also invite the following external people to the event you created earlier:

• Bernd Schmurz (schmurz@patente.net)

• Anja Rot (rot@patente.net)

For external participants, you additionally require their **business address, a telephone number, and the date of birth**.

**Task:** Invite the two people to the event by adding them to the respective Data Cart.

### Export personal data

Dr. Josefa Hauser reacted immediately and added a photo.

**Task:** Export all personal data and then check the data for completeness. Also, check how you need to protect the downloaded data, and when you have to delete the data.

### Invention disclosure

A colleague asks you if you could take over an invention disclosure. She has made the scanned form available to you as a PDF on the file-drop server:

[https://\[removed\].de/fileserver/file](https://[removed].de/fileserver/file)

**Task:** Download the scanned form.

Then import the form using the data basket tool to record the receipt of the data and store it in the data basket.

### Invention disclosure

It has been a while since you have processed an invention disclosure.

#### Task

Look at the information provided to determine,

- for which purposes you may use the data;
- under which legal basis you may process the data;
- to whom you may pass on the data;
- and when you have to delete the data again.

### Invention disclosure

In order to have the invention disclosure examined, some of the data collected must be transmitted to PatentePrüf GmbH. The company asks you to provide the following data on the persons: First and last name, title, private address, professional address, e-mail, private and professional telephone number.

**Task:** Check whether you are allowed to pass on the requested personal data. Then export the personal data for forwarding to PatentePrüf GmbH and check the completeness of the export.

### Invention disclosure

The invention was extremely good and the test was successful.

**Task:** Request the account information for the **external** inventors so that you can initiate the compensation the next day.

Finally, closing time.

Thank you for your support, Mrs Wagner-Müller!

Please fill out the short questionnaire:

[https:// \[Link to System Usability Scale\].de/](https://[Link to System Usability Scale].de/)

### Post-study interview

- Could you put yourself in the place of Verena Wagner-Müller?
- How did you feel about using the data basket?
- How did you feel about the privacy compliant handling of personal data?

### Post-study interview

Assume that the data basket is available to you:

- How do you think this would change the way you work?
- How do you think this would change the way you handle personal data?

## D.4 STUDY III — NON-FUNCTIONAL REQUIREMENTS

In the following, we report the non-functional requirements elicited in our studies. The requirements are grouped according to the categories of ISO/IEC 25010 [356].

## Compatibility:

- Mapping of existing authorization concepts
- Support of common data exchange formats
- Interfaces to other systems

## Performance efficiency:

- Parallel use
- Fast loading times
- Low implementation costs

## Reliability:

- No technical weaknesses
- High availability
- Low susceptibility to errors

## Maintainability:

- Automatic updating

## Usability:

- User-friendly interface
- Easy to understand content
- Intuitive and self-explanatory
- Little effort much benefit
- Low time expenditure
- Low training effort
- Clarity
- Little text
- Individualization
- Quick access to content
- Context sensitive support
- Visualizations

D.5 STUDY III — SCREENSHOTS DATA CART PROTOTYPE (TRANSLATED)

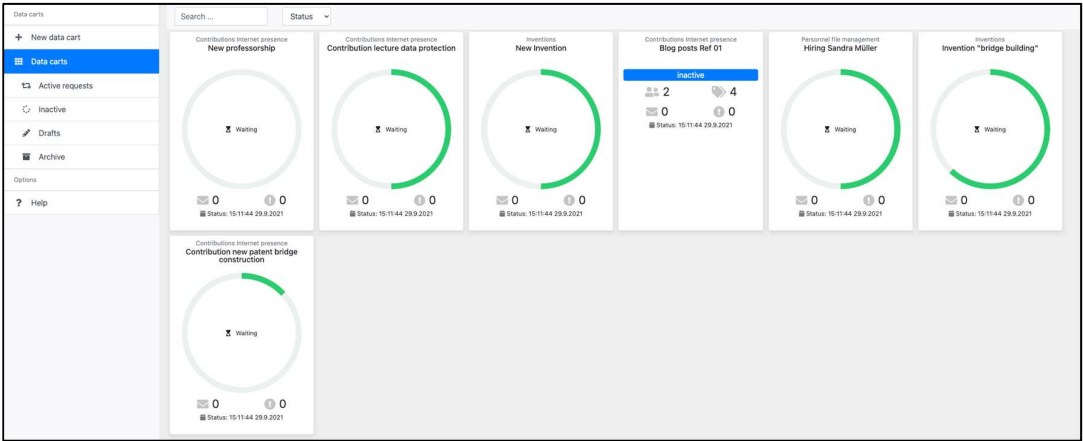


Figure D.1: Screenshot *Data Cart* landing page: The landing page provides data processing employees an overview of active, inactive, and archived personal data requests. Each request is summarized in a widget, including status information.

Basic information | Select persons and data | Specify data query | Check and send

Please select the purpose or reason of the planned data processing activity:\*

Inventions  
Patenting, Exploitation

Please give a name to the planned data processing activity:\*

New Invention

Please describe as precisely as possible what you want to process the data for:\*

Patenting the new invention

Select data and data subjects >

**Directory of permitted processing activities**

Inven

Inventions  
Patenting, Exploitation often used

Information on selected processing activity

Permitted purposes

Patenting

Processing of the invention disclosure according to the Employee Invention Act and forwarding of the invention disclosure for evaluation of the invention as well as patenting, if necessary.

Exploitation

Financial management of the exploitation of the invention after successful evaluation.

Categories of data subjects

- Employees
- External Inventors

Categories of personal data

- First Name
- Surname
- Title
- Nationality
- Address (Private)
- Phone number (Private)
- Profession / Activity
- Business address
- Phone number (Business)
- Business e-mail address
- IBAN
- BIC
- Bank Institute

Legal basis

- GDPR Art. 6 (1) b

Cancel Save

Figure D.2: Screenshot *Data Cart* processing activity selection: Data processing employees are to choose a processing activity from the organizations' records of processing activities. The UI summarizes important key facts about the selected processing activity.



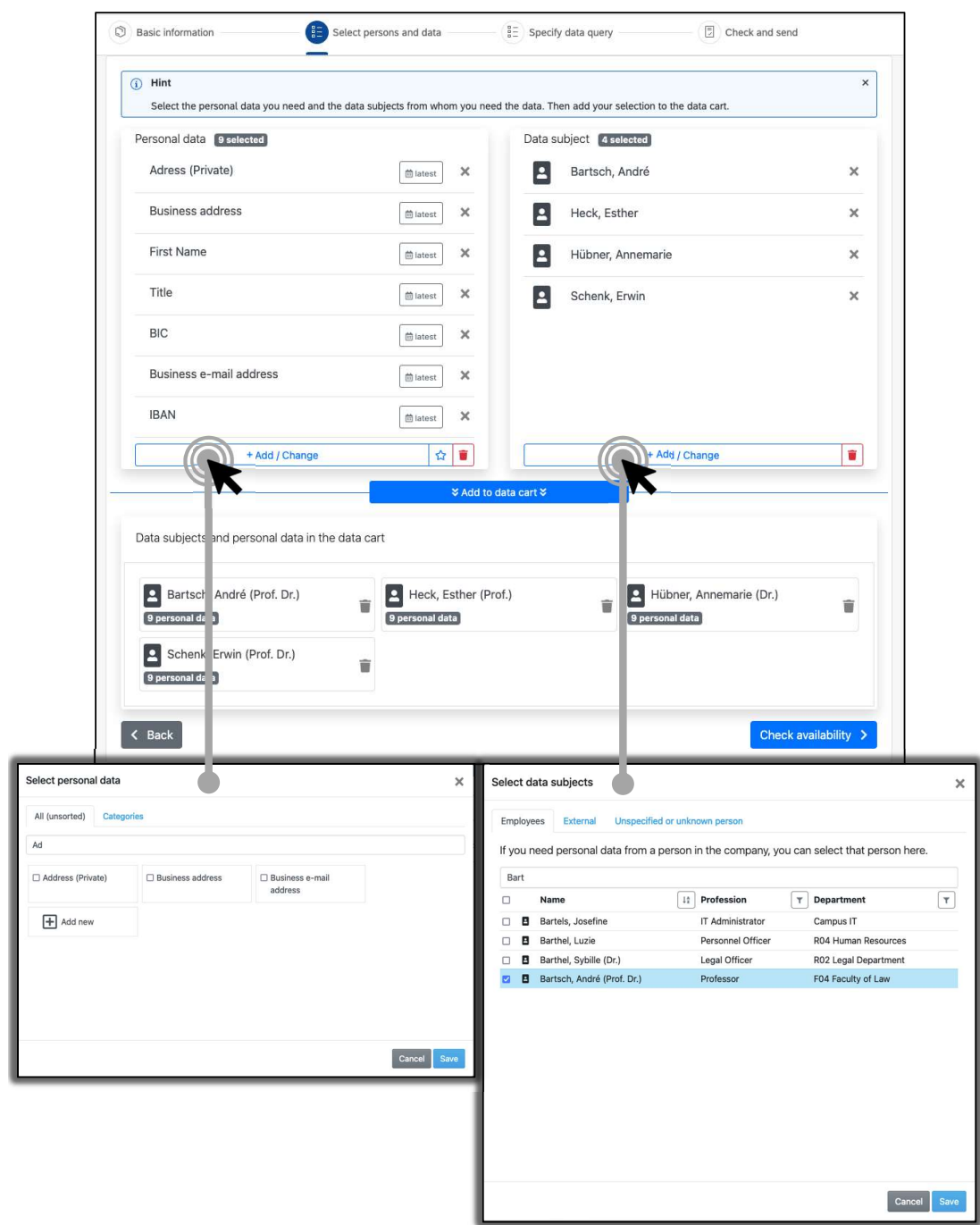


Figure D.3: Screenshot *Data Cart* tuple specification: Data processing employees add combinations of personal data and data subjects. Predefined lists of allowed categories of data are derived from the selected record entry and are offered as a pre-selection. Data processing employees may select data subjects from a list of employees in the organization, or add them as externals by providing contact details.

Basic information

Select persons and data

Specify data query

Check and send

Availability

4 Incomplete

Approved

Show details (4 data subject(s) concerned)

#	Name of the data subject	Approval	Data completeness	Update
+	Bartsch, André (Prof. Dr.)	✓	0 / 9	not available
+	Heck, Esther (Prof.)	✓	0 / 9	not available
+	Hübner, Annemarie (Dr.)	✓	0 / 9	not available
+	Schenk, Erwin (Prof. Dr.)	✓	0 / 9	not available

How would you like to request the unavailable data?\*

The current option was automatically determined by data cart

☒ Request directly from data subjects
 ☐ Request from another person / department
 ☐ I request the data elsewhere myself

Personal message to the data subjects (optional):

Until when do you need the personal data and approvals? (optional)

DD.MM.YYYY

< Back

next >

Figure D.4: Screenshot *Data Cart* request customization: Data processing employees customize the request for personal data and permissions. The tool validates the processing activity (1) by verifying for lawfulness of processing against the processing policies extracted from the record of processing activities, and (2) by checking the availability and timeliness of the data. The validation results are displayed in an overview.

Basic information

Select persons and data

Specify data query

Check and send

⚠ Edit mode. This data cart is not active yet and you can still customize the content.

Selected data processing activity

Inventions  
Patenting, Exploitation

Name of the planned data processing activity

New Invention

Description of the purpose of the planned data processing activity

Patenting the new invention

Data subjects and personal data

0%  
Data completeness:  
Incomplete

Requests to:  
Data subject

Update:  
Unknown

Response deadline:  
No deadline set

Personal message to the data subjects (optional):

▼ 4 Show data subject(s) concerned

#	Name of the data subject	Approval	Data completeness	Update
+	<div>Bartsch, André (Prof. Dr.)</div>	✓	0 / 9	not available
+	<div>Heck, Esther (Prof.)</div>	✓	0 / 9	not available
+	<div>Hübner, Annemarie (Dr.)</div>	✓	0 / 9	not available
+	<div>Schenk, Erwin (Prof. Dr.)</div>	✓	0 / 9	not available

Discard

Save as draft

Send requests and activate data cart

Figure D.5: Screenshot *Data Cart* request verification: Data processing employees may check the request before sending it.

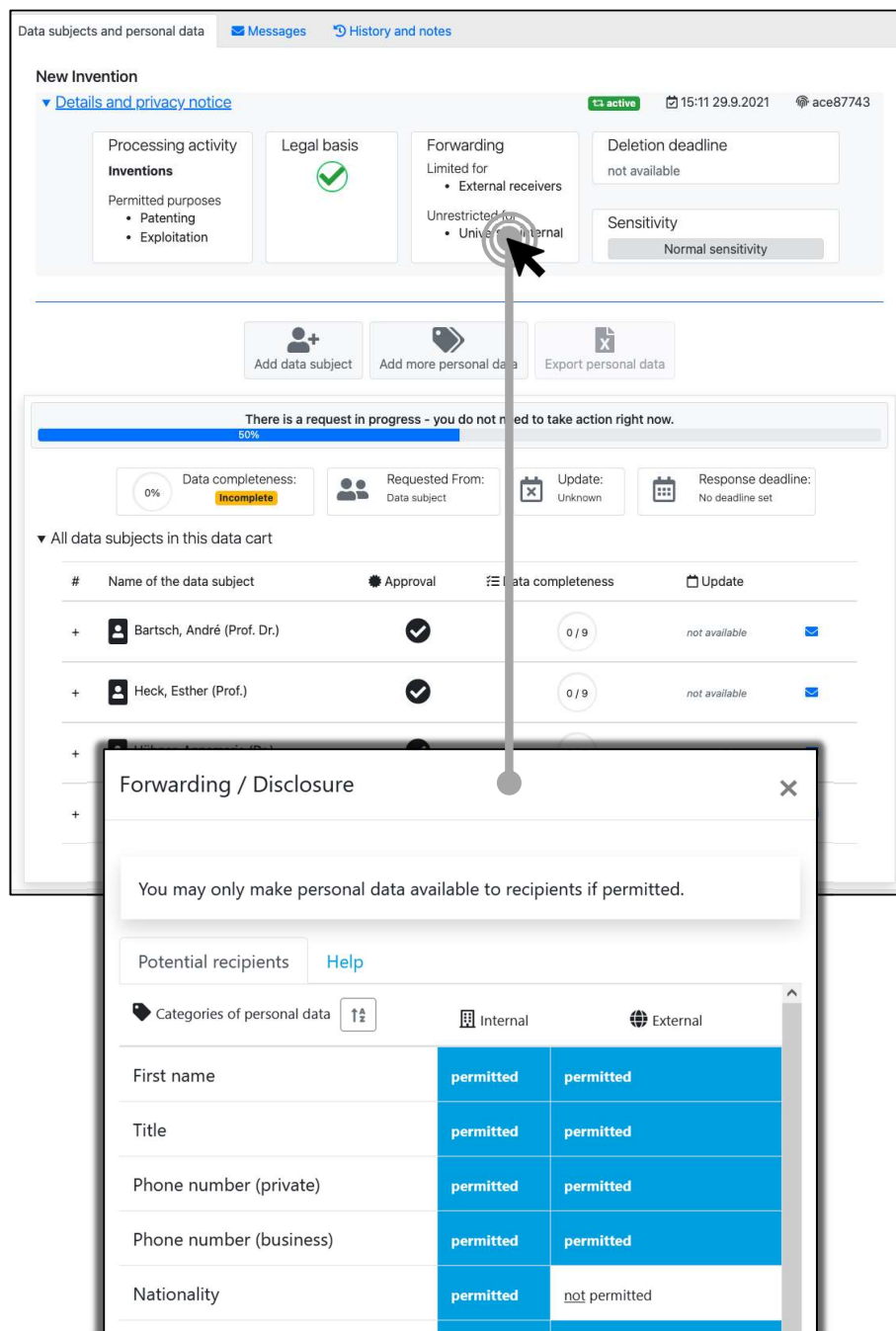


Figure D.6: Screenshot *Data Cart* personal data management interface: Personal data processing employees are provided detailed information on the status of pending requests, as well as the ability to request additional combinations of personal data and data subjects, or to export the data. The interface provides frequently needed or important practical information on data protection tailored to stakeholders' information needs. This includes information on allowed processing operations, whether processing has been approved, to whom data may be disclosed, deletion periods, the sensitivity of the data, and how data must be safeguarded.