Challenges, Conflicts, and Solution Strategies for the Introduction of Corporate Data Protection Measures

Christian K. Bosse, Denis Feth, and Hartmut Schmitt

1 Introduction

Safeguarding and exercising data subjects' rights by implementing technical and organizational measures are highly important. Accordingly, data protection laws such as the General Data Protection Regulation [24] and the California Privacy Rights Act [18] address these measures. However, it must be considered that privacy and data protection are not only about technical and organizational aspects. There is also a third sphere that has to be considered: the social sphere. Within and between these three spheres—technical, organizational, and social—a variety of conflicts can arise, e.g., due to different interests of various stakeholders [7]. In particular, one must be aware that any data protection measure can also have undesired side effects. For example, backups can negatively influence data minimization or deletion processes in a company. Of course, this does not mean that backups are to be avoided. However, if such dependencies and conflicts are not explicitly considered when designing data protection measures, this can lead to a complete rejection by employees in the worst case [8]. In this chapter, we discuss these challenges and offer appropriate solutions. We focus on the business context, in particular the relationship between employees and employers, and illustrate our discussion with a specific example [47].

C. K. Bosse (✉)
Institut für Technologie und Arbeit e.V., Kaiserslautern, Germany
e-mail: christian.bosse@ita-kl.de

D. Feth
Fraunhofer IESE, Kaiserslautern, Germany
e-mail: denis.feth@iese.fraunhofer.de

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

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_17

Chapter Overview First, Sect. 2 creates an overview of related research in the two relevant topic areas of socio-technological adoption of new technologies and the usability of security and data protection measures. Then, in Sect. 3, we argue why digital transformation needs to be viewed holistically and present our sphere model that shows the multiple interactions between the three spheres. In the following Sect. 4, we address challenges that may arise, whether due to a lack of consideration of the interactions between these spheres, deliberate manipulation of individuals' behavior, or privacy-intrusive data protection measures. In Sect. 5, we use an example to describe the operationalization of our models before drawing a final conclusion in Sect. 6.

2 Related Work

Our work is primarily related to research from two areas: socio-technical aspects of the introduction of new technologies and the usability of security and data protection measures. In the following, we will distinguish ourselves from these works or put them in context.

2.1 Technology Introduction and Acceptance

The adoption of new technologies is not a new field of research in science, although initially, the framework conditions were still different: As early as the 1950s, studies were conducted on the adoption of new technologies in agriculture and their diffusion processes [5]. The diffusion theory resulting from this work describes, among other things, the social system as a relevant factor for the diffusion of an innovation, consisting of its norms, organizational rules, structures, as well as opinion leaders [41]. After this, the effects of various factors on users' attitude regarding the new technology and their interaction became the subject of research. A basic technology acceptance model [19, 20], which has been further developed and supplemented over the years [45, 53], analyzes and describes these. This includes initial approaches to structuring the introduction process as well as controlling interventions by the organization [52].

Due to the dynamics associated with rapid technological progress and the modern megatrend of digitalization, this work is gaining relevance once again. Influencing factors that can increase the success of implementation processes can be derived from this work. These factors include, for example: active involvement of users of the new technology in the introduction process [3], support from managers [57], well-designed training courses [48], or the involvement of internal and/or external experts [30] who actively accompany and help shape the change. These factors must be seen in the context of the current change of work and the digital transformation that goes hand in hand with it [27]. The focus is increasingly shifting toward employees, who are recognized as a central factor that acts in a self-determined and self-organized manner. In addition to corporate goals regarding costs and quality, work design increasingly addresses employee-related goals such as personality development, even if these goals are sometimes in conflict with corporate goals [43]. The increase in self-determination and privacy regarding data in the workplace, which can be enabled by the use of a privacy dashboard, should also be seen in this context [50]. However, previous work has primarily focused on the use of privacy-enhancing technologies (see the chapter "Acceptance Factors of Privacy-Enhancing Technologies on the Basis of Tor and JonDonym") at the interface between companies and end users, mostly with a focus on the latter [6]. The design of a fair exchange of information between companies and employees supported by a technological solution has not been comprehensively researched yet.

2.2 Usable Security and Usable Privacy

Existing literature on usable security shows that the user is an important part of modern security chains. The strongest technical security measure is not effective if attackers can circumvent it by means of social engineering, for example. Well-known case studies have analyzed the usability of email encryption with PGP [56], of file sharing with Kazaa [26], and of authentication mechanisms and password policies [16, 28]. However, such case studies are specific to one technology or application and do not consider conflicts arising from the technologies. Design principles for usable, yet secure systems [23, 33] focus on the development of usable security systems by supporting developers and emphasizing the importance of considering the user. However, these principles ignore the area of technology introduction.

In the area of data protection measures, the so-called privacy dashboards are becoming increasingly important, also in the enterprise context [22, 40]. In general, various projects evaluate the applicability and usability of privacy dashboards. In the myneData project [34], for example, a user-controlled data market for personal data was created. A decentralized solution is offered by the MyData project [38], where a cockpit is only used for transparency and control, but the data remain with the services and can be exchanged via (existing) channels after user consent. In the SPECIAL project [32], a holistic approach was developed where data from various sources are aggregated and harmonized based on machine learning and semantic technologies. Even though usability is an important aspect of these projects, challenges and conflicts were not explicitly considered. For a more detailed summary of research on usable privacy, please refer to the chapter "Empirical Research Methods in Usable Privacy and Security".

3 Digital Transformation as a Holistic Challenge

Companies in all sectors and industries are affected by digital transformation [58], and so are the working environments of their employees. Driven by the rapid progress in technology, traditional jobs are changing, business processes are being re-oriented, and innovative digital business models are emerging. In industrial production, for example, digital innovations often lead to radical change, which is also called digital disruption [7]. The analysis of data, including a lot of personal data, offers the possibility to optimize existing processes and workflows. To successfully master the key challenge of digital transformation, all three of the spheres mentioned in Sect. 1 must be considered as shown in Fig. 1 [10].

The *organizational sphere* roughly comprises everything that has to do with regulations and processes within a company, such as works council agreements, data protection regulations, incentive systems, standards, and laws. This sphere is so relevant because it defines how a company works. Problems within the organizational sphere therefore usually have a direct impact on the effectiveness and/or efficiency of an organization.

The *technical sphere* deals with the tools for implementing organizational regulations. A high level of usability of the tools used according to ISO 9241-11:2018 [29] is essential. This is shown, for example, by a study conducted in Germany among 1000 employees [36], according to which 55% of the participants bypassed their company's security measures at least once a week and 17% even did so daily. The reason: the use of IT security systems is perceived as too complicated and time-consuming. Accordingly, aspects such as ergonomics, interface design, and interaction design of security and data protection tools—summarized under the term "usable security and privacy"—must be taken seriously. Problems with the use of technical tools have a direct impact on their acceptance or hinder employees in the

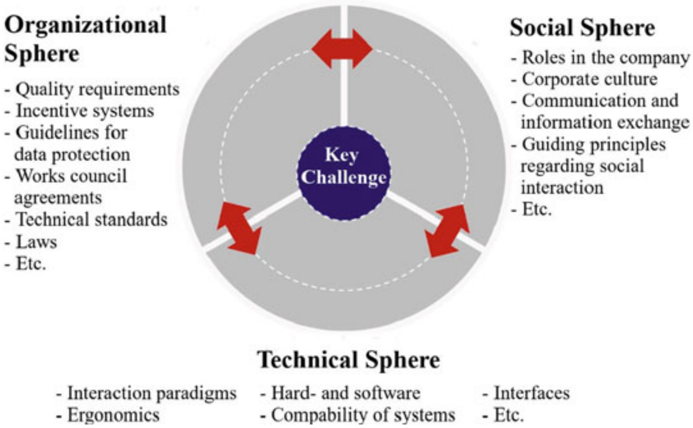

Fig. 1 Interaction in our three-sphere model

performance of their tasks. This can even go as far as employees actively exploring and establishing ways to perform their tasks without the use of the new technology, even if this behavior can be harmful for the company [7, 21].

In the *social sphere*, primarily interpersonal aspects come into play. The attitude of employees toward digital transformation in general and the introduction of new processes or technologies have a significant influence on the success of the implementation. Corporate culture and good communication play a major role here. Problems in this sphere can lead to mistrust and a lack of acceptance and condemn a digitalization project to failure from the outset. Similarly, power struggles or rivalries between individuals or groups in the social sphere of the company, for example, can lead to the success of a technology introduction being jeopardized.

4 Challenges in the Operational Introduction of Data Protection Measures in Companies

In this section, we use three examples to illustrate the challenges that can arise in the context of introducing data protection measures in companies. In doing so, we draw on the 3-sphere model already presented, in which the challenges can be located. We also highlight apparent contradictions that can arise in this context. The three challenges presented are underpinned with the help of fictitious examples based on practical experience, so that the relevance for practice becomes more apparent.

4.1 Lack of Considering the Interactions of the Spheres

It is easy to understand that each of the three spheres is relevant individually, and however, strong interactions between the spheres exist. If only one sphere, e.g., the technical one, is considered when introducing data protection measures, gaps and backdoors can arise due to the close links with the other spheres. The interaction of the spheres offers a wide range of opportunities to obtain sensitive employee data or personal information even without direct technical access [46]. For this reason, when implementing a new technology, various domain- and company-specific regulations, standards, and legal requirements must be considered. It may even become necessary to adjust internal regulations or processes to support the new technologies [10, 54].

Also, all relevant employees must be involved as early as possible. Involvement in the selection and design of technology is just as important as training on their application. Without employee participation and process adaptation, the monitoring that employees may perceive can have a variety of unintended effects. For example, employees may feel that they are under constant scrutiny and may adapt their actions or behaviors in ways that may be detrimental to organizational processes and workflows. Under certain circumstances, this can even pose a risk to the company if, for example, the protection of employee data is not ensured as a result [9, 10]. How quickly is sensitive employee data printed out shortly before the weekend and taken home instead of being retrieved from home via a protected connection to the company's IT system, whose use is both cumbersome and logged?

The emotional impact of new technologies should also not be underestimated. While some employees welcome them in principle, others reject them completely or even fear for their jobs. Such fears must be addressed openly, taken seriously, and resolved. Otherwise, fronts can quickly form that can only be overcome with great difficulty. In practice, however, the social impact is often neglected or considered much too late, possibly resulting in user requirements not being met, users being overwhelmed, or the works council intervening [9].

Example

To illustrate the extent to which the technical, organizational, and social spheres of a company interlock and influence each other, one might consider the example of the necessarily hasty establishment of remote work during the Covid-19 pandemic. If employees are expected to work from home, the company must provide the necessary technical equipment and make sure that it is usable, privacy-friendly, and secure. Furthermore, it has to ensure compliance with legal regulations, such as the Working Hours Act or occupational safety, as well as data protection [54]. In addition, works council agreements and, if necessary, further company standards and processes must be adapted accordingly and complied with [1]. Employees must also be trained on how to access company data securely from home and how to handle internal data in a private or publicly viewable environment—for example, when working with mobile devices in the home office or on business trips [13, 31]. Furthermore, effects on cooperation among colleagues as well as on the corporate culture are to be expected, necessitating guiding intervention by the management level. Managing at a distance, as is needed in decentralized and digitally working teams, presents a new challenge for managers. Strict guidelines and control no longer represent the contemporary style of leadership. A manager must be a supporter of the team and is responsible for promoting the ability to work [26, 37].

4.2 Exploiting the Gray Areas of Data Protection

New possibilities for data collection and processing in connection with employees' personal data are arousing new desires, not least on the employers' side [7]. For example, changed models of work like the home office boom triggered by the Covid-19 pandemic are fueling the desire of many employers to monitor those employees who are no longer working on the company's premises [35]. In order to obtain the desired data, employers often use practices that are not prohibited but are nonetheless ethically questionable because they violate the basic principles of self-determination and privacy protection. This can be achieved by exploiting basic psychological principles, exploiting the so-called privacy paradox or by a deceptive design of the user interface (see also the chapter "The Hows and Whys of Dark Patterns: Categorizations and Privacy"). In the following subsections, we describe these gray areas in more detail.

The practices described are comparable to practices that are referred to as social engineering in IT security. Social engineering refers to methods of behavioral manipulation in which human characteristics such as helpfulness, trust, or respect for authority are exploited to gain unauthorized access to information or IT systems [2]. However, the target of attacks is usually not employees' personal data, but other companies' data of high value. In most cases, the attackers are also external to the company, such as industrial spies, blackmailers, competitors, or disruptors.

Recognizing that gray areas are being entered can lead employees to reject newly introduced technologies, and the damage done may be greater than the benefits hoped for. In addition, there are also several examples where actual data protection violations became known and were also fined. For example, H&M was fined 35 million euros for illegal surveillance of its employees [44].

Exploitation of Basic Psychological Principles Possible points of attack that employers can exploit in a rather subtle way to obtain their employees' data are certain psychological principles, which the social psychologist Cialdini called "weapons of influence" [17]:

- *Reciprocity:* When someone does us a favor or gives us a gift, we feel obligated to return the favor and often give back even more than we initially received.
- *Scarcity:* We consider things that are only available in limited quantities or only for a certain time to be particularly valuable.
- *Authority:* We are more likely to agree with people we consider authorities because they are assumed to have more knowledge, experience, or expertise than we do.
- *Consistency:* Once we have made a decision or taken a position on something, we tend to stick to it.
- *Liking:* We are more likely to help other persons out if we like them. Similarity, compliments, and physical attractiveness contribute to liking.
- *Social Proof:* When we are uncertain, we often look at how others behave. The more people behave in a certain way, the higher the chance we consider this behavior appropriate. In other words, humans adapt to the (supposed) social norm.

In addition, there are several similar factors [15] that employers can use, such as:

- Appealing to values such as helpfulness and loyalty
- Exploiting personal or professional trust

- Short reflection time for requests, so that the individual cannot think about possible consequences of their action
- Greek gifts (example: permission for private use of company cell phones, which are then used to spy on employees)

The following fictitious example shows how these principles and factors can be used to compromise employee data protection.

Example

Christine E. Owens presides over approximately 70 employees as the chief executive officer of a start-up company. She would like to make company processes more efficient using data analysis. Her data protection officer, who has since been dismissed, said that because of the personal reference to employees, she may only use certain data with their consent. Christine is confident that all her employees will consent. She writes the following email to her employees:

"Most start-ups evaluate process data. A random survey in our company showed that 89% of the respondents think it would be good if we also evaluated process data. By giving your consent, you help to save costs, which contributes to the success of the company. The success of our company is very important to all of us. Please give me your consent for the collection and analysis of the data by 3 p.m. today. Tomorrow morning, I will approach everyone whose consent I have not received until then to find out more about the reasons for this. As your CEO, I am counting on you! Yours, Christine E. Owens"

There are several forms of influence in this fictitious example:

- *Authority: Christine emphasizes her position as CEO to gain the consent of the employees and builds up a threatening gesture ("I will approach everyone").*
- *Social proof: Using phrases such as "most startups" and "89% of respondents," Christine points to the social norm.*
- *Short reflection time: Instructing people to respond on the same day builds up time pressure.*
- *Appealing to loyalty: Christine points out the common vision ("success of the company") and that everyone's consent is expected ("I am counting on you!").*

Exploiting the Privacy Paradox The privacy paradox [4] describes a discrepancy between what users want and what users do regarding their privacy. Several studies [42] confirm that users do care about their privacy but do not act accordingly. There are several reasons for this: For example, security and data protection measures typically require a certain level of knowledge and certain skills, which some users do not possess [25]. Solutions for resolving the privacy paradox are still being heavily researched.

Deceptive Design of User Interfaces Further opportunities for behavioral manipulation to lower the level of employee privacy are opened up by digital *nudging* [55] (see also the chapter "Privacy Nudges and Informed Consent? Challenges for Privacy Nudge Design") and the use of dark patterns [11] (see also the chapter "The Hows and Whys of Dark Patterns: Categorizations and Privacy"). These phenomena can be exploited to weaken employee data protection already in the design of internally used IT systems. The aim of nudging is to (subtly) give an impetus to certain socially desirable behavior, i.e., to bring about "better" decisions [49]. This is done without coercion or financial incentives. One of the most effective digital nudges is the setting of default rules and preferences, such as the privacy-friendly defaults required in Art. 25 (2) GDPR. However, the same techniques can also be used to make users act contrary to their actual intentions, such as agreeing to permissive privacy settings. *Dark patterns* are patterns that are used in the design of user interfaces to mislead or entice the user to perform unwanted actions. These are actually anti-patterns—examples of how things should not be done—but are deliberately used in an unethical or deceptive manner. The systematic use of such dark patterns is described by Bösch et al. [14] as Dark Strategies.

4.3 Data Protection Measures Counteracting Privacy

It may seem counter-intuitive, but it is actually a real risk: Data protection measures can counteract privacy. We give three examples originally presented in [39]:

Transparency vs. Surveillance Data subjects may have the desire to know who is processing their personal data. Providing this information to the data subject can affect the privacy of data users (e.g., employees in customer service). For example, if the exact time and person of a data use is revealed, the data subject can draw conclusions about the data user's work behavior. Anonymization can at least partially resolve this conflict.

Trust vs. Mistrust Technical and organizational measures normally increase trust in an information system and its provider. However, information meant to increase transparency could cause resentment as data subjects become aware of the use of their personal data. Also, the sudden introduction of privacy-enhancing technology could arouse mistrust. Data subjects may wonder whether there has been a privacy incident that led to this rollout. Therefore, the objectives of the introduction of privacy-enhancing technology should be made clear.

Self-determination vs. Social Pressure Data subjects have the right of self-determination. For example, they could specify that their usage data must not be analyzed for the purpose of system optimization, or they may object to the publication of a picture on social media, which the marketing department would love to share. If data subject and data user know each other—for instance, if they are colleagues or have a business relationship—the data subject may experience social pressure to provide these data. This can be especially critical if the data user is an authority. A respectful work culture or respectful business relationship could resolve such a conflict.

These examples illustrate that an "ideal" solution does not or cannot exist. Even if a security or data protection measure initially appears ideal from the users' point of view and the users also employ it to implement their data protection, the introduction of such a tool alone may lead to new problems.

5 Operationalization in Practice

A research project [51] examined the challenges described above and developed application-oriented solutions, with the overarching goal of balancing the interests of employees and their employers and helping to strengthen a culture of trust in companies by improving employee privacy. Through the interaction of the various spheres, data protection is to be ensured in the long term not only through fair reconciliation of interests, but also with the help of extensive user awareness. The following example will further illustrate this.

Example

In the development project for a business-critical software, a call center company is trying to alleviate reservations about data protection and achieve the best possible acceptance among internal users. It therefore gives high priority to the quality characteristic of data minimization. At the same time, the company's business operations must be maintained at all times, even in the event of data loss. Accordingly, the quality characteristic of recoverability is also prioritized. Therefore, backups containing sensitive personal data of call center agents are indispensable for its fulfillment. This illustrates at least one conflict of objectives—data minimization vs. recoverability—which may be supplemented by interactions with other quality characteristics such as transparency or intervenability for the employees involved.

As a solution to this conflict of objectives, it was decided to develop a detailed backup and deletion concept for the various backup generations and to implement corresponding deletion routines at the technical level. To implement this procedure successfully, it is also necessary to plan and implement complementary activities in the company's organizational and social sphere. One starting point, for example, is to define appropriate operating instructions at the organizational level: What data are stored where and for how long in which backups? Are the backups encrypted? Who is allowed to access them? A criteria catalog or corresponding guiding questions can provide support here, such as "Is the number of backup systems required specified?," "In the case of additional redundant backup systems, have the redundancy mechanisms been specified?," and "Has the way in which the backups are created been determined?."

Corresponding measures should always be taken with the involvement of the works council or employee representatives, who should ideally be involved in resolving the conflict of objectives from the very beginning. Here, it is important to comply with the existing law, which stipulates a duty of co-determination as part of the introduction of technology as soon as there is a risk that employers could control the performance and behavior of their employees. Furthermore, it should be checked whether additional works council agreements are needed in which employees agree to the temporary storage of their sensitive personal data. In addition, all affected employees should be made aware of the measures (e.g., the backup and archiving systems from the given example) at an early stage and trained in their operation.

Thus, recognizing the issue allows a company to find a balance of interests between all those involved already during the development phase and to maintain it more easily during the implementation and operation phases.

Involving the works council or employee representatives is also a first step toward addressing the social level in the company. However, this alone is not sufficient to achieve high acceptance of the new technical solution. The first step is to raise employees' awareness of the need for the new technical solution and to make clear the importance of their contribution to data protection and security through the successful introduction of this new technology. Internal information events to which management invites the employees are first step of doing this. This highlights the relevance of the development project for the company and the role of managers as good role models who support the project. In addition, employees should be regularly informed about the progress and kept up to date. To this end, the appropriate communication channels and formats must be selected, which may vary depending on the company. Another step is to participate employees in the early phases of technology introduction, for example, in requirements analysis (see also the chapter "Achieving Usable Security and Privacy Through Human-Centered Design"). Furthermore, it is essential that employees receive training on the use of the new digital solution well in advance of the go live. Well-structured training should show both the general scope of functions and their limitations as well as the specific procedure in practical use cases. This will ensure that employees are not initially overwhelmed by the use of the new technology and the resulting changes in workflows.

Further general measures for maintaining a high level of data protection are the establishment of organizational regulations (e.g., locking one's screen when leaving the desk) and raising awareness for behavioral manipulation similar to social engineering attacks. Regarding social engineering, there are special kinds of training that expose employees to a trap, such as a pretend phishing email. Trapped employees are then informed about countermeasures. The German Federal Office for Information Security (BSI) provides current examples of phishing attacks and informs about countermeasures [12].

6 Summary

The introduction of new technologies or processes in a company is often subject to reservations and conflicts. In the case of data protection, this is particularly challenging due to the criticality, sensitivity, and legal requirements in this area. In this chapter, we therefore first looked at the challenges that must be considered when introducing corporate data protection measures. In particular, a lack of attention to the interactions between the technical, organizational, and social spheres of a company can lead to unintended interactions, up to and including rejection of the new technology and harmful behavior of employees. We presented possible solutions as to how a holistic approach considering all three spheres can contribute to successful technology introduction.

Acknowledgments This work is funded by the German Federal Ministry of Education and Research (grant numbers 16KIS1506K, 16KIS1507, and 16KIS1509).

References

1. Alipour, J.-V., Falck, O., & Schüller, S. (2020). Homeoffice während der Pandemie und die Implikationen für eine Zeit nach der Krise. ifo Institut – Leibniz-Institut für Wirtschaftsforschung an der Universität München (Vol. 73, pp. 30–36).
2. Anderson, R. (2008). *Security engineering: A guide to building dependable distributed systems*. Wiley
3. Barki, H., & Hartwick, J. (1994). Measuring user participation, user involvement, and user attitude. *MIS Quarterly, 18*(1), 59–82.
4. Barnes, S. (2006). A privacy paradox: Social networking in the United States. *First Monday, 11*(9).
5. Beal, G., & Rogers, E. (1960). The adoption of two farm practices in a central Iowa community. Special report 26, Iowa Agricultural and Home Economics Experiment Station Publications, Iowa.
6. Blumberg, V., & Kauffeld, S. (2020). Anwendungsszenarien und Technologiebewertung von digitalen Werkerassistenzsystemen in der Produktion. *GIO Gruppe. Interaktion. Organisation. Zeitschrift für Angewandte Organisationspsychologie, 51*(1), 5–24.
7. Bosse, C. K., Dietrich, A., Kelbert, P., Küchler, H., Schmitt, H., Tolsdorf, J., & Weßner, A. (2020). Beschäftigtendatenschutz: Rechtliche Anforderungen und Technische Lösungskonzepte. In W. Kummer, F. Schweighofer, E. Hötzendorf (Eds.), *Conference volume of the 23rd Edition of the Conference International Legal Informatics Symposions IRIS*. Vachendorf.
8. Bosse, C. K., Dietrich, A., & Schmitt, H. (2021). IT-Rahmenwerk für den eschäftigtendatenschutz. Technologieeinführung aus rechtlicher und arbeitswissenschaftlicher Perspektive. *Informatik, 2020*, 815–828.
9. Bosse, C. K., Dietrich, A., & Weßner, A. (2021). Selbstbewertungsinstrument für den betrieblichen Datenschutz. Unterstützung für die Umsetzung des Beschäftigtendatenschutzes in KMU. *Datenschutz und Datensicherheit-DuD, 45*(1), 23–27.
10. Bosse, C. K., Hellge, V., Schröder, D., & Dupont, S. (2019). Digitalisierung im Mittelstand erfolgreich gestalten. In C. Bosse & K. Zink (Eds.), *Arbeit 4.0 im Mittelstand. Chancen und Herausforderungen des digitalen Wandels für KMU* (pp. 13–34). Springer-Gabler.
11. Brignull, H. (2011). Dark patterns: Deception vs honesty in UI design. https://alistapart.com/article/dark-patterns-deception-vs.-honesty-in-ui-design/
12. Bundesamt für Sicherheit in der Informationstechnik (BSI). (2011). Aktuelle Beispiele für Phishing-Angriffe. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/Aktuelle-Beispiele-fuer-Phishing/aktuelle-beispiele-fuer-phishing_node.html
13. Bruhn, P. (2020). IT-Sicherheit und Datenschutz. In *Homeoffice und mobiles Arbeiten im Team effektiv umsetzen. Essentials*. Springer Vieweg.
14. Bösch, C., Erb, B., Kargl, F., Kopp, H., & Pfattheicher, S. (2016). Tales from the dark side: Privacy dark strategies and privacy dark patterns. In *Proceedings on Privacy Enhancing Technologies* (pp. 237–254).

15. Caraban, A., Karapanos, E., Gonçalves, D., & Campos, P. (2019). 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19 (pp. 1–15). Association for Computing Machinery.
16. Choong, Y.-Y., & Theofanos, M. (2015). What 4,500+ people can tell you—employees' attitudes toward organizational password policy do matter. In T. Tryfonas & I. Askoxylakis (Eds.), *International Conference on Human Aspects of Information Security, Privacy, and Trust* (pp. 299–310). Springer.
17. Cialdini, R. B. (2009). *Influence: The psychology of persuasion, revised edition*. Harper Business.
18. CPRA. (2019). The California Privacy Rights Act of 2020. https://oag.ca.gov/system/files/initiatives/pdfs/19-0021A1. Consumer Privacy—Version 3.
19. Davis, F. (1985). *A technology acceptance model for empirically testing new end-user information systems—theory and results*. PhD thesis, Massachusetts Inst. of Technology.
20. Davis, F., Bagozzi, R., & Warshaw, P. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982–1003.
21. Dietrich, A., Bosse, C. K., & Schmitt, H. (2021). Kontrolle und Überwachung von Beschäftigten. *Datenschutz und Datensicherheit-DuD, 45*(1), 5–10.
22. Feth, D., & Schmitt, H. (2020). Requirement and quality models for privacy dashboards. In *2020 IEEE 7th International Workshop on Evolving Security & Privacy Requirements Engineering (ESPRE)* (pp. 1–6). IEEE.
23. Garfinkel, S. (2005). *Design principles and patterns for computer systems that are simultaneously secure and usable*. PhD thesis, Massachusetts Institute of Technology.
24. GDPR. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation. https://eur-lex.europa.eu/eli/reg/2016/679/oj
25. Gerber, P., Volkamer, M., & Gerber, N. (2017). Das Privacy-Paradoxon–Ein Erklärungsversuch und Handlungsempfehlungen. In *Dialogmarketing Perspektiven 2016/2017* (pp. 139–167). Springer Gabler.
26. Good, N. S., & Krekelberg, A. (2003). Usability and privacy: A study of Kazaa P2P file-sharing. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '03 (pp. 137–144). Association for Computing Machinery.
27. Hasenbein, M. (2020). *Der Mensch im Fokus der digitalen Arbeitswelt*. Springer.
28. Inglesant, P. G., & Sasse, M. A. (2010). The true cost of unusable password policies: Password use in the wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10 (pp. 383–392). Association for Computing Machinery.
29. ISO 9241-11. (2018). Ergonomics of human-system interaction—part 11: Usability: Definitions and concepts (ISO 9241-11:2018).
30. Jasperson, J., Carter, P. E., & Zmud, R. W. (2005). A comprehensive conceptualization of post-adoptive behaviors associated with information technology enabled work systems. *MIS Quarterly, 29*(3), 525–557.
31. Kanzenbach, K. (2020). Rechtliche Grundlagen zum Homeoffice und der Telearbeit. In *DGUV forum* (Vol. 8, pp. 18–24).
32. Kirrane, S., Fernández, J. D., Dullaert, W., Milosevic, U., Polleres, A., Bonatti, P. A., Wenning, R., Drozd, O., & Raschke, P. (2018). A scalable consent, transparency and compliance architecture. In *European semantic web conference* (pp. 131–136). Springer.
33. Lo Iacono, L., Smith, M., von Zezschwitz, E., Gorski, P. L., & Nehren, P. (2018). Consolidating principles and patterns for human-centred usable security research and development. In *European workshop on usable security*.
34. Matzutt, R., Müllmann, D., Zeissig, E.-M., Horst, C., Kasugai, K., Lidynia, S., Wieninger, S., Ziegeldorf, J. H., Gudergan, G., Spiecker gen. Döhmann, I., Wehrle, K., & Ziefle, M. (2017). myneData: Towards a trusted and user-controlled ecosystem for sharing personal data. In *INFORMATIK 2017*.

35. Moorstedt, M. (2020). Tracking von Mitarbeitern. In der Krise boomt auch die Überwachung durch den Chef. https://www.sueddeutsche.de/digital/home-office-ueberwachung-tracking-chef-zoom-1.4868739
36. KES Online. (2022). Jeder zweite Angestellte umgeht Security-Lösungen. https://www.kes.info/archiv/schlaglichter/schlaglicht/?tx_ttnews%5Byear%5D=2022&tx_ttnews%5Bmonth%5D=06&tx_ttnews%5Bday%5D=10&tx_ttnews%5Btt_news%5D=228&cHash=9153da146aff24a9c080c4347cdb1fc8
37. Osranek, R., & Staat, P. (2020). *Moderne Führung als Ausdruck neuer Werte* (2nd ed.). Ayway media GmbH.
38. Poikola, A., Kuikkaniemi, K., & Honko, H. (2015). MyData. A Nordic model for human-centered personal data management and processing. Finnish Ministry of Transport and Communications.
39. Polst, S., & Feth, D. (2020). Privacy ad absurdum-how workplace privacy dashboards compromise privacy. In *Mensch und Computer 2020-Workshopband*.
40. Polst, S., Kelbert, P., & Feth, D. (2019). Company privacy dashboards: Employee needs and requirements. In *International Conference on Human-Computer Interaction* (pp. 429–440). Springer.
41. Rogers, E. (2003). *Diffusion of innovations* (5th ed.). Free Press.
42. Rudolph, M., Feth, D., & Polst, S. (2018). Why users ignore privacy policies—a survey and intention model for explaining user privacy behavior. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*.
43. Schaper, N. (2019). Arbeitsgestaltung in Produktion und Verwaltung. In G. Schaper, N. Nerdinger, & F.W. Blickle (Eds.), *Arbeits-und Organisationspsychologie* (pp. 411–434). Springer.
44. Schemm, M. (2020). Bußgeld wegen Datenschutzverstößen bei H&M. https://datenschutz-hamburg.de/pressemitteilungen/2020/10/2020-10-01-h-m-verfahren
45. Schepers, J., & Wetzels, M. (2007). A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects. *Information & Management, 44*(1), 90–103.
46. Schmitt, H., Bosse, C. K., Dietrich, A., & Polst, S. (2021). Wie ich an deine Daten kam oder Dark Patterns und Phishing im Beschäftigtenkontext. In *Jusletter IT 27*.
47. Schmitt, H., & Groen, E. C. (2021). Qualitätsmodell zur Förderung des Beschäftigtendatenschutzes. *Datenschutz und Datensicherheit-DuD, 45*(1), 28–32.
48. Sharma, R., & Yetton, P. (2007). The contingent effects of training, technical complexity, and task interdependence on successful information systems implementation. *MIS Quarterly, 31*(2), 219–238.
49. Thaler, R., & Sunstein, C. (2008). *Nudge: Improvising decisions about health, wealth, and happiness*. Yale University Press.
50. Tolsdorf, J., Bosse, C. K., Dietrich, A., Feth, D., & Schmitt, H. (2020). Privatheit am Arbeitsplatz. Transparenz und Selbstbestimmung bei Arbeit 4.0. *Datenschutz und Datensicherheit-DuD, 44*(3), 176–181.
51. TrUSD Project Consortium. (2022). TrUSD—Transparente und selbstbestimmte Ausgestaltung der Datennutzung im Unternehmen. https://www.trusd-projekt.de/
52. Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273–315.
53. Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the technology acceptance model: Four longitudinal field studies. *Management Science, 46*(2), 186–204.
54. Visser, L., Voigt, P., & Vraetz, M. (2021). *Das Recht auf Homeoffice in der Pandemie* (1st ed.). Baden-Baden.
55. Weinmann, M., Schneider, C., & Brocke, J. v. (2016). Digital nudging. *Business & Information Systems Engineering, 58*, 433–436.
56. Whitten, A., & Tygar, J. D. (1999). Why Johnny can't encrypt: A usability evaluation of PGP 5.0. In *8th USENIX Security Symposium (USENIX Security 99)*, Washington, D.C. USENIX Association.

57. Wieseke, J., Kraus, F., & Rajab, T. (2010). Ein interdisziplinärer Ansatz zur Überwindung von Technologieadaptionsbarrieren. *Zeitschrift für betriebswirtschaftliche Forschung, 62*(7), 822–859.
58. Zink, K., Schröder, D., Hellge, V., & Bosse, C. (2019). Zukunft der Arbeit = Arbeit 4.0? In K.J. Zink (Ed.), *Arbeit und Organisation im digitalen Wandel* (pp. 53–93). Baden-Baden.