AIS Transactions on Human-Computer Interaction

Volume 14 | Issue 4 Article 2

12-31-2022

Design Principles for Personalized Assistance Systems that Respect Privacy

Marleen Voss
Ruhr University Bochum, marleen.voss@rub.de

Olga Bosak
University of Bremen, lanif@icloud.com

Mark Hoebertz
Ruhr University Bochum, mark.hoebertz@isse.rub.de

Felix Mohsenzadeh
University of Bremen, mohsenzadeh@uni-bremen.de

Maximilian Schnebbe
University of Bremen, schnebbe@uni-bremen.de

See next page for additional authors

Follow this and additional works at: https://aisel.aisnet.org/thci

Recommended Citation

Voss, M., Bosak, O., Hoebertz, M., Mohsenzadeh, F., Schnebbe, M., Poeppelbuss, J., & Eisenbeiss, M. (2022). Design Principles for Personalized Assistance Systems that Respect Privacy. *AIS Transactions on Human-Computer Interaction, 14*(4), 461-489. https://doi.org/10.17705/1thci.00176
DOI: 10.17705/1thci.00176

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in AIS Transactions on Human-Computer Interaction by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Design Principles for Personalized Assistance Systems that Respect Privacy

Authors

Marleen Voss, Olga Bosak, Mark Hoebertz, Felix Mohsenzadeh, Maximilian Schnebbe, Jens Poeppelbuss, and Maik Eisenbeiss

This article is available in AIS Transactions on Human-Computer Interaction: https://aisel.aisnet.org/thci/vol14/iss4/2

Transactions on Human-Computer Interaction

Volume 14 Issue 4

12-2022

Design Principles for Personalized Assistance Systems That Respect Privacy

Marleen Voss

Chair for Industrial Sales and Service Engineering, Ruhr University Bochum, marleen.voss@rub.de

Olga Bosak

markstones Institute of Marketing, Branding & Technology, University of Bremen, bosak@uni-bremen.de

Mark Hoebertz

Chair for Industrial Sales and Service Engineering, Ruhr University Bochum, mark.hoebertz@isse.rub.de

Felix Mohsenzadeh

markstones Institute of Marketing, Branding & Technology, University of Bremen, mohsenzadeh@uni-bremen.de

Maximilian Schnebbe

Institute for Information, Health and Medical Law, University of Bremen, schnebbe@uni-bremen.de

Jens Poeppelbuss

Chair for Industrial Sales and Service Engineering, Ruhr University Bochum, jens.poeppelbuss@isse.rub.de

Maik Eisenbeiss

markstones Institute of Marketing, Branding & Technology, University of Bremen, eisenbeiss@uni-bremen.de

Follow this and additional works at: http://aisel.aisnet.org/thci/

Recommended Citation

Voss, M., Bosak, O., Hoebertz, M., Mohsenzadeh, F., Schnebbe, M., Poeppelbuss, J., & Eisenbeiss, M. (2022). Design principles for personalized assistance systems that respect privacy. *AIS Transactions on Human-Computer Interaction*, *14*(4), pp. 461-489.

DOI: 10.17705/1thci.00176

Available at http://aisel.aisnet.org/thci/vol14/iss4/2

Transactions on Human-Computer Interaction

Research Paper DOI: 10.17705/1thci.00176 ISSN: 1944-3900

Design Principles for Personalized Assistance Systems That Respect Privacy

Marleen Voss
Chair for Industrial Sales and Service Engineering, Ruhr University Bochum
marleen.voss@rub.de

Olga Bosak
markstones Institute of Marketing, Branding & Technology, University of Bremen

Mark Hoebertz
Chair for Industrial Sales and Service Engineering, Ruhr University Bochum

Felix Mohsenzadeh
markstones Institute of Marketing, Branding & Technology, University of Bremen

Maximilian Schnebbe
Institute for Information, Health and Medical Law, University of Bremen

Jens Poeppelbuss
Chair for Industrial Sales and Service Engineering, Ruhr University Bochum

Maik Eisenbeiss
markstones Institute of Marketing, Branding & Technology, University of Bremen

Abstract:

Personalized assistance systems (PAS) provide real-time assistance tailored to individual users to improve efficiency in the workplace. PAS communicate dynamically with users through wearable computing devices. To deliver such personalized assistance, PAS need personal data from the individuals who wear them. However, concerns over data protection and security can negatively influence the extent to which users accept personalized assistance systems. The key aspects in this regard that the literature currently lacks include data protection law and the employee perspective. Hence, we develop seven design principles for PAS that respect user privacy through employee-determined approaches to data collection and use. We developed the principles based on a systematic literature review, user personas, privacy control, and European Union legal requirements for privacy by design and privacy by default. Our design principles, which we evaluated in a focus group and an expert workshop, provide a framework to help practitioners and software developers mitigate adoption barriers due to privacy concerns. Our study also contributes to the theoretical discussion of current developments in personalized assistance in the workplace by providing a new perspective on ensuring employees accept the required data collection and use.

Keywords: Personalized Assistance Systems, Design Principles, Employee-determined Data, Privacy Control, Privacy by Design, Privacy by Default

Jia Shen was the accepting senior editor for this paper.

1 Introduction

The need for assistance systems in the workplace has grown significantly (Ulmer et al., 2020). According to an Allied Market Research study from 2021, the global market for industrial wearables—the devices on which an assistance system runs—will grow by 12.4 percent annually by 2027, and the market size from US$3.79 billion in 2019 to $8.4 billion by 2027 (Savekar, 2021). Assistance systems refer to software programs that provide assistance through pre-defined work tasks, which can improve employee safety and efficiency and enable instant communication in the workplace (Awolusi et al., 2019; Svertoka et al., 2021).

However, as employees usually have different skills and qualifications, they do not need the same type and amount of assistance. Thus, to fully exploit an assistance system's potential, the next logical step is to personalize the system. Personalization enables an assistance system to adapt to an employee's knowledge with respect to a specific task and to help the employee with individual decisions or specific problems (Gil et al., 2017).

Hence, personalized assistance systems (PAS) offer new and unexplored opportunities to foster communication between workers and their environment (Maltseva, 2020). They can increase operational efficiency via features such as hands-free work and instant instructions. Organizations can use the generated data to optimize business processes and lower downtime. Additionally, a PAS can increase workplace safety by guiding workers through complicated situations and enabling instant communication (Awolusi et al., 2019; Svertoka et al., 2021). Using personal data, such as an employee's movements and body functions, photos, videos, and sound recordings from their immediate environment, PAS can even provide real-time support tailored to a specific employee and dynamically adapt to their continuously accumulating knowledge (Kalantari, 2017).

However, organizations must overcome several obstacles to integrate PAS into the workplace. For example, employees may respond negatively to PAS if an organization makes using them mandatory (Lapointe & Rivard, 2005; Laumer et al., 2016), leading to further problems. Hence, organizations might not use PAS to their full potential, or employees might feel less satisfied with their job (Hwang et al., 2016). Additionally, different positions in a company, even different employees with the same job, have different user requirements. Therefore, organizations should take heterogeneous user requirements and preferences into account to integrate PAS successfully. Finally, employees' concerns over data protection and data security can negatively influence PAS adoption and use (Xu et al., 2011; Kalantari, 2017). Therefore, we think that organizations should adopt an employee-centered approach to prevent issues from arising when they introduce PAS and to prioritize users' requirements. Furthermore, when organizations implement PAS in the workplace, they must follow national employee data-protection laws (e.g., the General Data Protection Regulation (GDPR) in Europe). Due to the European setting in which we conducted this study, we operate in the GDPR's legal framework to ensure legally compliant data collection and use. As GDPR regulations focus on employees, extending these legally binding guidelines through additional employee-centered design principles is in employees' best interests.

Prior research shows that employees are more likely to accept assistance systems if they have control over their data's collection and use, which the privacy control concept reflects (Tucker, 2014; Martin et al., 2017). In 2017, by focusing on GDPR, Berkemeier et al. (2017) developed the first set of requirements for smart glasses-based information systems in a work context. Although prior studies have referred to general design guidelines for wearables (Wentzel et al., 2016; Sethumadhavan, 2017), investigated the adoption of wearable technology in a working context (Buenaflor & Kim, 2013; Choi et al., 2017; Jacobs et al., 2019; Spil et al., 2019), and even discussed the relevance of data protection for assistance systems in general (Lee et al., 2018; Klapper et al., 2020), none of them have so far considered personalization features. Moreover, current guidelines for designing PAS fail to consider either legal requirements or users' heterogeneous requirements for appropriately handling personal data—a need that has increased as organizations have increasingly adopted flexible working. Although numerous authors have noted as much some extent, they have not yet fully formulated requirements for PAS and completely closed the gap. On the one hand, studies have considered the digital assistance system context and its associated human-computer interaction (HCI) and ethical aspects alongside purely technical requirements (Benke et al., 2020) but left out data-protection aspects. On the other hand, studies have explored digital assistance systems in a work context and even addressed GDPR (Berkemeier et al., 2017) but have not considered users' heterogeneous requirements. In particular, the data protection aspect and associated legal framework required for compliance with the GDPR has not been sufficiently addressed in other studies (Luse & Burkman, 2020; Mettler & Wulf, 2019; Psychoula et al., 2020). Where studies have made a connection to

GDPR, they have not done so in a work-related context (Ioannidou & Sklavos, 2021; Ziccardi, 2020). To clarify our contribution's unique nature, we summarize these studies' features and highlight the differences between their contributions and our study in Appendix A.

Against this background, in this study, we focused on developing PAS that respect privacy by considering GDPR and employees' heterogeneous requirements. To that end, we developed design principles that specify how one should design an artifact (Chandra et al., 2015). Design principles refer to "statements that guide or constrain actions, are prescriptive in nature, constitute and are an appropriate way to communicate findings to both technology-oriented and management-oriented audiences" (Seidel et al., 2018, p. 225). The resulting design principles should provide guidance for researchers and practitioners that design PAS. They specifically focus on mechanisms for employee-determined data collection and use, which, in turn, should help users accept PAS. To the best of our knowledge, our study constitutes the first work that comprehensively compiles design principles for PAS that also cover the criteria relevant to data protection. Our study contributes to research by providing a first set of universally applicable and empirically grounded design principles for PAS in a workplace context that consider both employees' personal requirements and data-protection laws.

To develop these design principles, we applied a three-step qualitative research process that included multiple methods. First, to identify the requirements for the design principles, we analyzed the literature on technology acceptance and, specifically, on assistance systems; clarified the legal requirements; and conducted a paper-and-pencil survey with representatives of two companies to identify heterogeneous user requirements and preferences. Second, we derived affordances and material properties from these requirements to formulate the design principles. Third, we conducted a focus group discussion and an expert workshop to evaluate the design principles.

We structure this paper as follows: in Section 2, we review the research background and focus on the PAS environment's key economic and legal aspects. In Section 3, we develop and evaluate design principles for employee-determined data collection and PAS use through a three-step research process. In Section 4, we discuss and summarize the results. Finally, in Section 5, we conclude the paper.

2 Research Background

2.1 Personalized Assistance Systems

An assistance system is an interactive communication and information technology that connects humans and machines (Mewes et al., 2020). The machine appears as a mobile or body-worn device that ideally does not impair a user's attention or flexibility (Kasselmann & Willeke, 2016; Niehaus, 2017; Mewes et al., 2020). Examples include smart watches, data glasses, head-mounted displays and headsets, handheld scanners, wristbands with radio-frequency identification (RFID) functionality, tablets, or smartphones (Kasselmann & Willeke, 2016; Niehaus, 2017). In an industrial context, assistance systems provide employees with computer-based support for their tasks, such as providing work-related information, decision support, and instructions that can also advance their skills (Kasselmann & Willeke, 2016; Niehaus, 2017; Mewes et al., 2020). Assistance systems' personalized features allow individuals to tailor their functions and services. Such systems offer and present these functions and services in such a way that they consider individuals' preferences, interests (e.g., individual settings for notifications or displays), behavior, expertise level (e.g., entry-level worker with a need for more support and guidance in comparison to an experienced one), and tasks (Göker & Myrhaug, 2002).

As of 2022, the academic literature does not clearly define PAS. However, based on how existing studies have defined (digital) assistance systems (Kasselmann & Willeke, 2016; Niehaus, 2017; Böckelmann & Minow, 2018; Mewes et al., 2020) and personalization (for an overview, see Adomavicius & Tuzhilin, 2005), we define a PAS as an information technology system that provides users with computer-based and individualized support when performing work tasks. An assistance system adapts the support it offers and presents to specific tasks and situations and to individuals' preferences, interests, behaviors, and expertise (Perugini & Ramakrishnan, 2003). To do so, it retrieves, processes, and transmits user inputs and data from various systems in real time (Kasselmann & Willeke, 2016; Niehaus, 2017; Mewes et al., 2020). The communication between user and device can be visual, acoustic, or haptic (Kasselmann & Willeke, 2016; Mewes et al., 2020).

When developing design principles for PAS that respect privacy, we need to consider the following two dimensions that have a decisive influence on the design process: 1) the business environment at the micro level and 2) the legal environment at the macro level. In the business environment, PAS must not only address employees' privacy concerns but also respect their heterogeneous privacy preferences and requirements. The business environment directly connects to the legal environment and its respective data-protection regulations (in our case, the GDPR). These key determinants and their interrelationship constitute our research framework (see Figure 1).

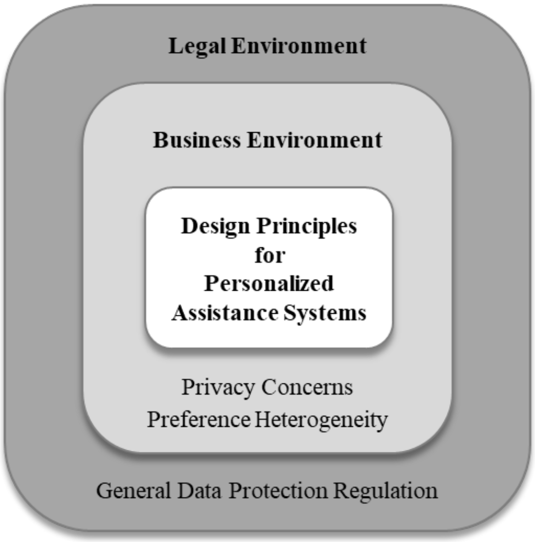
Legal Environment
Business Environment
Design Principles for Personalized Assistance Systems
Privacy Concerns
Preference Heterogeneity
General Data Protection Regulation

Figure 1. Research Framework

2.2 Business Environment: Privacy Concerns and Preferences Heterogeneity

To a certain extent, providing personalized assistance requires data related to individuals as a basic requirement. The need to disclose personal data, however, can increase privacy concerns among employees, which, in turn, can reduce the extent to which they accept PAS adoption and use (Xu et al., 2011; Kalantari, 2017). Thus far, researchers predominantly in digital marketing have investigated privacy concerns and acceptance in connection with PAS and largely adopted a consumer perspective (Bélanger & Crossler, 2001; Bleier & Eisenbeiss, 2015). Findings from digital marketing indicate that one can significantly reduce privacy concerns by applying the so-called privacy control concept (i.e., giving users individual control over how others use data that relates to them) (Martin et al., 2017). For example, Tucker (2014) found that individuals who felt more in control over their personal data were more willing to accept tracking cookies and, thus, personalized advertising. Consequently, by integrating privacy control aspects from the user's perspective, PAS can not only minimize privacy concerns but also increase the extent to which they accept employee-determined data collection and use for providing personalized support.

As we note above, users tend to exhibit heterogeneity to a certain degree in their preferences for privacy control. While one employee may prefer to disclose as little data as possible, another may take a more relaxed attitude towards data privacy and care less about data minimization. Therefore, we gathered and analyzed opinions from different employees to reflect this heterogeneity in our study.

2.3 Legal Environment: General Data Protection Regulation

To establish PAS and ensure they succeed in the long term, organizations need to not only gain acceptance from employees but also ensure legal compliance and, above all, ensure they handle employee data in a data-protection compliant manner. In contrast to consumers, employees in particular, need protection due to their (usually more long-term) ties to their employer. Therefore, a system's design must consider data-protection (and, in particular, employee data-protection) laws. In 2018, the General Data Protection Regulation (GDPR) became the legal framework for data protection and privacy in the European Union (EU) and the European Economic Area (EEA). The process of individual data release must meet the requirements for effective consent under data protection law. Particular attention must be paid to the voluntary and informed nature of the consent (principle of lawfulness, fairness, transparency principle (Article 5(1) lit. a GDPR). Organizations must ensure that no one can use the data in their systems for performance and behavior monitoring or for various other purposes (purpose limitation principle; Article 5(1) lit. b GDPR). Organizations must implement these and other data-protection principles, such as data minimization, accuracy, or storage limitation (Article 5(1) GDPR), and enforce them through appropriate technology design and default settings (Article 25 GDPR).

Privacy by design means that the data controller takes appropriate technical and organizational measures, such as pseudonymization, to implement these data-protection principles and to incorporate necessary safeguards in data processing (Article 25(1) GDPR). This essential GDPR requirement protects data subjects' rights. Privacy by default means that the controller implements appropriate technical and organizational measures to ensure that, by default, data-processing activities use only the necessary personal data that each specific purpose requires (Article 25(2) GDPR).

We acknowledge that the GDPR does not apply to companies outside the EU and the EEA. However, to reach the highest acceptance level and guarantee user data safety, non-EU companies might want to follow them regardless.

2.4 Design Principles

The environmental aspects of our research framework generate various requirements concerning PAS features that design principles can capture. Design principles have become a popular way to provide practical guidance for designing, developing, and using information systems and appropriate solutions (Gregor et al., 2020). Chandra et al. (2015) highlighted three important reasons for developing and using design principles: 1) they serve to capture and communicate design knowledge; 2) they enable one to abstract away from singular settings and, thus, to generalize prescriptive knowledge; and 3) they constitute one step in the process to develop more comprehensive bodies of knowledge.

A design principle refers to "a statement that prescribes what and how to build an artifact to achieve a predefined design goal" (Chandra et al., 2015, p. 4040). In this sense, design principles concern a class of information systems that "encompass knowledge about creating other instances that belong to this class" (Sein et al., 2011, p. 45). Since design principles consider not only technical functionalities but also aspects of use and legal frameworks, they can also make design-relevant regulations explicit (Chandra et al., 2015).

According to Seidel et al. (2018), design principles comprise three aspects at their core: 1) affordances, 2) material properties, and 3) boundary conditions. Affordances describe a user's needs or desires and, thus, their action possibilities. A system's material properties allow users to enact the affordances. Boundary conditions serve to show the limits (especially with regard to generalizability).

Design principles can address technology-oriented and management-oriented target groups (Hevner et al., 2004). For example, they can help one create practice-suitable IT artifacts because they combine descriptive, explanatory, and predictive knowledge (Chandra et al., 2015). In this context, Gregor et al. (2020) mention the requirement that design principles should consider human actors' roles (which include both implementers' and users' perspectives). Furthermore, to ensure their usefulness, one should formulate design principles in such a way that people can easily understand them (Gregor et al., 2020).

3 Development

3.1 Overview of the Research Process

To develop a set of design principles for employee-determined data collection and use in PAS, we followed a three-step empirical research methodology that included a qualitative, multi-method approach (see Figure 2), which various information systems studies have used to develop design principles (Ahmad et al., 2022; Frische et al., 2021; Seidel et al., 2018). In addition, with this approach, we could reliably understand the various requirements that users and regulations demand from PAS in depth.

In the first step, we identified the requirements for PAS. In the second step, we formulated the design principles for PAS based on the affordances and material properties we derived from the requirements. Using a focus group discussion and an expert workshop, we then evaluated the design principles in the third step. We describe the three steps, research methods, and results next.

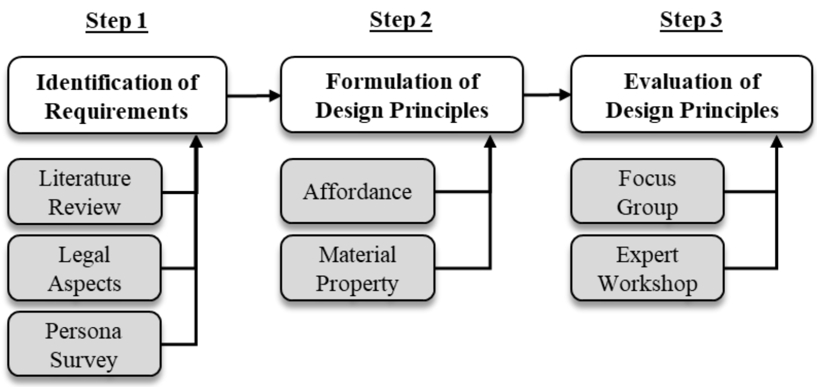

Figure 2. Three-step Research Process

3.2 Step 1: Identification of Requirements

Identifying the requirements to develop our design principles involved three consecutive activities. We first conducted a literature review before analyzing the legal aspects and conducting a survey to develop user personas that reflect employees' heterogeneity.

3.2.1 Literature Review

For our literature review, we followed the five-phase framework for IS literature reviews that vom Brocke et al. (2009) proposed. In the first phase, we defined the review's scope (e.g., by highlighting categories that characterize the literature review) (Cooper, 1988). We conducted our literature review to summarize central issues concerning the user-centric requirements for PAS, privacy control, privacy by design, and privacy by default. The second phase involves conceptualizing the research topic, which means that one should acquire broad knowledge and clarify what important constructs mean. To identify the key concepts, terms, and synonyms used for the literature review, we analyzed relevant research on the topics of PAS, privacy control, privacy by design, privacy by default, and design principles (see Section 2). We depict our literature research process (i.e., the third phase) in Figure 3. We searched the Google Scholar and ScienceDirect databases with keywords such as “privacy control”, “workplace privacy”, “employee privacy” and “information privacy”. Additionally, we used these keywords in combination with the terms “review”, “meta”, “organizational”, “personalized advertising”, “personalization”, “advertising”, “information systems”, “digitals”, and “wearables”. We removed duplicates, inaccessible papers, and sources that did not contain specific findings on user-centric requirements for data collection and use, particularly in the HCI, wearables, or assistance systems areas. In addition, we sorted out literature that understood our keywords in a different way, applied them in a different context, or did not provide empirical results. In total, we identified 23 relevant studies.

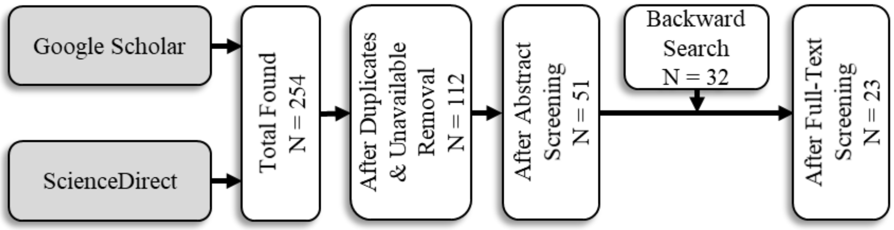
Google Scholar
ScienceDirect
Total Found N = 254
After Duplicates & Unavailable Removal N = 112
After Abstract Screening N = 51
Backward Search N = 32
After Full-Text Screening N = 23

Figure 3. Search Process of the Relevant Literature

We show the results from reviewing and synthesizing the literature (the fourth phase) in Table 1. In particular, we show the derived user-centric requirements for PAS, which we used to derive material properties and affordances to formulate design principles. We describe further research opportunities (i.e., the fifth phase) in Section 5.

Table 1. User-centric Requirements for Personalized Assistance Systems

Reference	Requirements
Allen et al. (2007)	Users are more willing to disclose personal data if they see a benefit in personalizing the system or storing the data.
Bandara et al. (2019)	Users who trust a personalized service provider are more likely to be positive about personalization. Privacy and security concerns increase risk beliefs. Users want protection against data misuse.
Bélanger & Crossler (2011)	Users must perceive organizational policies or practices regarding data processing and storage as fair. The perception that an organization adopts fair information practices can increase users' trust in a personalized service.
Berkemeier et al. (2017)	Users want their personal data to be anonymized and pseudonymized.
Bleier & Eisenbeiss (2015)	Users who trust a personalized service provider are more likely to be positive about personalization. Providers can build trust through transparency about privacy policies. Users perceive personalized services as effective when the personalization is appropriate.
Buchanan et al. (2013)	Users often do not want organizations to collect and store location-tracking data.
Chellappa & Sin (2005)	Users who trust a personalized service provider are more likely to be positive about personalization. Users are more likely to use personalized services if they know their benefits.
Culnan & Armstrong (1999)	A provider can mitigate privacy concerns about personalization by providing explicit disclosure to users about how it uses fair information practices. Users who perceive a company that provides personalized services to engage in fair information practices can increase the extent to which users trust them. Users are less likely to perceive personalized services as invading their privacy if they feel that they can control how actors use the information in the future.
Hui et al. (2007)	Related to privacy statements: the more personal information that one requests from users, the less likely users are to disclose it.
Jacobs et al. (2019)	Users want to be involved and informed by their organizations in efforts to introduce assistance systems. This involvement increases user acceptance of such systems and the sharing of personal data.
Kolter & Pernul (2009)	To mitigate concerns that someone will identify them when they release their personal data, users want pseudonymous personalization.
Landau (2015)	Users do not want their personal data to be used for any purpose other than the original one without their consent.
Malhotra et al. (2004)	Personalized service users perceive existing procedural justice as fair when they have control over their personal data.
Maltseva (2020)	Users are interested in enriching and expanding their (work) experience when using assistance systems. Therefore, users want to be informed about the benefits and challenges of (personalized) assistance systems.
Merhar et al. (2018)	The extent to which users accept personalized services increases when providers provide safety features.
Rosenthal et al. (2019)	Users who trust personalized service providers have fewer concerns about data privacy.
Schall et al. (2018)	An unbalanced cost/benefit ratio influences concerns to use assistance systems. Users need to be informed about personalized technology's benefits and potential.
Sethumadhavan (2017)	Users are more likely to trust assistance systems if organizations provide transparency about how they collect and use personal data.
Shubina et al. (2019)	Users want providers to anonymize their data so that third parties cannot identify them.
Tucker (2014)	Users want control over what data is stored about them and what happens to that data.
White et al. (2008)	An appropriate and justifiable fit between the personal data collected and a provider's purpose for it can minimize reactions to personalization
Xu et al. (2011)	Privacy and security concerns increase risk beliefs. Users want protection against data misuse.
Yildirim & Ali-Eldin (2019)	Assistance systems' perceived usefulness should be apparent to users.

3.2.2 Legal Aspects

To ensure that one designs a PAS in compliance with data protection, one must implement GDPR requirements for processing person-related data. As such, these principles constitute mandatory ones. Therefore, in addition to the academic literature, we also considered GDPR requirements. Article 5 of the GDPR contains the core of these requirements, which set out the principles for processing personal data. The GDPR obliges the responsible party to design the processing and the implemented technology in such a way that they comply with these principles (Articles 25 and 32). Furthermore, the GDPR assigns individuals who use the assistance system various data subject rights (Articles 12 to 23), which the responsible party must guarantee through the technical and organizational measures they implement (Article 12). Furthermore, we added seven law articles that specify and explain various GDPR regulations. We used these articles to derive requirements for employee-determined data collection and use in PAS (see Table 2).

Table 2. User-centric Requirements for Personalized Assistance Systems

Reference	Requirements
Herbst (2020)	Data subjects shall be fully informed about the processing operations during the processing.
Riesenhuber (2020)	Data subjects must give written or electronic consent.
Rost (2020)	Rost describes the standard data protection model with which the legal requirements for the processing of personal data and the effectiveness of the implementation of data protection measures can be put into a systematically verifiable relationship.
Roßnagel (2019)	If personal data are not adequate for the purpose, not substantial and not limited to what it needs for processing, an organization needs to conduct data minimization.
Schantz (2020)	The controller must not only comply with Article 5(1) but also be able to demonstrate compliance with it.
Schnebbe (2020a)	The authors discuss the relevant legal basis for implementing digital assistance systems in the employee context.
Schnebbe (2020b)	When implementing digital assistance systems in a work context, organizations must consider data-processing principles.

3.2.3 Persona Survey

While identifying requirements for PAS from the scientific literature, we found that studies tended to focus on personalization aspects in the marketing context (e.g., personalized advertising or email communication) (Tucker, 2014; Bleier & Eisenbeiss, 2015) but rarely in the digital or personalized assistance system context. Moreover, because the scientific literature would likely not have covered all potential PAS users' requirements, we conducted a survey in two companies to identify employee-centric requirements in a real-world setting, which informed our efforts to develop user personas. Personas describe hypothetical users in a given context with their needs, goals, and tasks (Cooper, 1999). They represent a particularly relevant and powerful technique in user-centric design that involves human-computer interactions to meet user needs, expectations, goals, and concerns (Salminen et al., 2021).

We approached two team leaders in two companies we knew about through collaborative research. Both had already begun implementing PAS and gaining initial experience with such systems. Company A operated in the mechanical engineering area, employed more than 350 people, and had introduced assistance systems in its maintenance service to make hands-free logging easier for technicians. Company B operated in the production and assembly technology area, employed 30 people, and had introduced assistance systems in its assembly process so that employees could receive assistance along the individual steps of the process. We sent a paper-and-pencil survey to the team leader in each company and asked them to fill it out. The team leader in company A led a team of 15 employees, while the team leader of company B led a team of 11 employees.

The survey comprised a questionnaire with 36 open-ended questions (see Appendix B). The team leaders had to answer all the questions from their perspective. The first part (questions 1-4) asked about the significance of PAS in the company and about the user groups that used such systems. All further questions concerned these user groups. The second part (questions 5-21) asked for information about the user groups, such as demographics, background, expectations, and goals. The third part (questions 22-36) gathered context-related data and included questions on challenges and solutions in using PAS in the workplace and what concerns and expectations individuals had related to employee-determined data collection and use.

An early question in the persona survey asked the respondents to think about user groups that already used, or would use, a PAS for their tasks, according to a chosen primary characteristic (e.g., work experience or area, see question 4 in Appendix B). Both respondents mentioned three user groups working in different areas. We assigned the six user groups to four personas based on their work objectives, their willingness to use PAS, and the stated feelings that each user group had towards using such systems (see Table 3). We called the four identified personas Alex, Billie, Chris, and Dale. Alex and Billie both had a managerial position and shared a high willingness to use PAS to increase work efficiency. However, as a team leader, the Billie persona sometimes views such systems more skeptically than Alex, a quality manager. As for why, team leaders, as middle managers, often find themselves positioned between their superiors and the employees they manage and, thus, are accountable to both. As a team leader, the Billie persona describes team leaders who find it more important for the organization to handle their teams' data responsibly. The Chris persona describes employees who view PAS use more skeptically due to concerns about surveillance and data misuse. On the other hand, the Dale persona describes employees who remain relatively curious about such systems and would willingly use them if they found that it could increase their efficiency.

Based on the answers from the second part of the persona survey, the questions about challenges and solutions in using PAS in the workplace and related concerns and expectations (in particular, see questions 22-36 in Appendix B), we derived requirements for each persona in terms of employee-determined data collection and use in PAS (see Table 3).

Table 3. Development of Personas

Persona	User group & company	Working objective	Willingness to use PAS	Feelings associated with PAS use	Requirements
1 (Alex)	Quality manager (company A)	Fulfillment of good quality orders	High to very high	Curiosity, enthusiasm	• Protection against unauthorized access • Uncomplicated understanding of data • Collection and use collection of only necessary data
2 (Billie)	Team leader (company A)	Efficient coordination & allocation of employees & resources	High, partial skepticism present	Curiosity, skepticism	• Superiors handle data in a trustworthy manner • Transparency about the data-collection and -use process • Possibility to inspect (own) stored data • Possibility to delete data at any time
3 (Chris)	Production employee (company A)	Provide efficient manufacturing	Low to medium, increased skepticism	Insecurity, skepticism	• Ease of understanding the data-collection and -use process • Possibility to delete data at any time • Understand the benefits of data collection and use • Personal data should be anonymized • Protection against unauthorized access • Secure data storage
	Assembly employee (company B)	Provide efficient assembly	Low to medium, increased skepticism	Insecurity	
4 (Dale)	Service technician (internal, company B)	Provide efficient maintenance, inspection & repair	Medium to high	Curiosity	• No spying and performance tracking • Collection of only necessary data • Personal data should be anonymized • Sufficient education about the data-collection and -use process • Understand the benefits of data collection and use • Ease of understanding the data-collection and -use process • Native language understanding of the data-collection and -use process
	Service technician (external, company B)				

3.3 Step 2: Formulation of Design Principles

In the second step of our research, we formulated initial design principles for employee-determined data collection and use in PAS by consolidating the requirements from literature, the GDPR with further legal articles, and the identified personas. In formulating our design principles (DP), we followed the structure from Seidel et al. (2018), which follows the following scheme: "Provide the system with [material properties such as specific features] to afford users [activity of user/group of users], given that [boundary conditions]" (Seidel et al., 2018, p. 225, square brackets as illustrative placeholders in the original quote). In our case, we can consider the GDPR a boundary condition for employee-determined data collection and use in PAS.

To integrate the data-protection requirements, we considered the guarantee objectives in the standard data-protection model (Rost, 2020). One principle about processing personal data in the standard data-protection model, as defined in Article 5(1) of the GDPR, is transparency for affected persons in the processing of personal data. Transparency means that data subjects and responsible parties can understand which data are collected and processed and for what purpose (Herbst, 2020). Sethumadhavan (2017) has shown that transparency increases the extent users accept wearables. In addition, a privacy policy demonstrates that an employee observes fair information practices, which contributes to the extent to which an employee perceives the organizational procedures as fair, which leads users to accept data processing and storage more (Culnan & Armstrong, 1999; Bélanger & Crossler, 2011). Employees in the companies that participated in the persona survey also required transparency about the data-collection and -use process (Billie, Chris). To afford users transparency about how an organization collects, uses, and stores their personal data, it must provide features to make the privacy policy transparent to users. Hence, we formulate:

DP1: Provide the system with features that clearly demonstrate the privacy policy to afford users transparency about data-collection, -use, and -storage processes.

In addition to transparency, users also find it important for data-protection regulations to adopt simple and understandable language (Alex, Chris, Dale). This aspect is also defined in relation to the declaration of consent in the employment sector (Article 88 of the GDPR, considering the requirements of Article 4. no. 11, 6(1) para. 1 lit. a, and Article 7). In addition, the declaration of consent must be in an understandable and easily accessible format and in clear and simple language (Riesenhuber, 2020). The employer must prepare and present information to users accordingly (Herbst, 2020; Rost, 2020). Further, providing an easy-to-understand privacy policy can increase employees' trust in their employer since the latter can better understand and control how the former collects, uses, and stores data. Research has shown that trust in an employer leads employees to accept personalized services more (Chellappa & Sin, 2005; Bélanger & Crossler, 2011; Bleier & Eisenbeiss, 2015; Bandara et al., 2019). To share how they collect, use, and store data in a user-friendly manner, employers need to formulate their privacy policy in simple and understandable language. Correspondingly, we formulate:

DP2: Provide the system with features for simple and understandable language in the privacy policy to afford users the ability to comprehend the data-collection, -use, and -storage processes.

Another important aspect concerns the control that users have over the data-collection process. Users should receive information and control about what data an organization collects since they perceive the relevant data-collection procedure as less privacy invasive (Culnan & Armstrong, 1999; Tucker, 2014). In addition, when individuals have control over personal data, they perceive the procedure as justice and fair, which, in turn, increases their trust in their company (Malhotra et al., 2004). In this context, we note that the more personal data an organization wants to collect, the less likely the user will disclose it (Hui et al., 2007). Users should be able to decide which data an assistance system collects and which data it does not (Schnebbe, 2020a). In addition, the principles related to processing personal data come into play here (Rost, 2020), which means that the data processing has to be adequate, relevant, and limited to what an organization needs in relation to why it processed it (Roßnagel, 2019; Alex, Chris). Hence, we formulate:

DP3: Provide the system with functions that show the type and extent of the collection of data to afford users control over the collected data.

In addition to the control over data collection, another important factor concerns control over how others use data (especially as it relates to protecting users' privacy) (Landau, 2015). Furthermore, organizations must only use data for the purpose they collected it for (Landau, 2015). For example, users often do not want organizations (especially service providers they do not trust) to collect storage or location-tracking data about them (Buchanan et al., 2013). Additionally, the fit between collected personal data and why an organization collected it must be appropriate and justified (White et al., 2008; Bleier and Eisenbeiss, 2015).

The three assurance objectives confidentiality, transparency, and non-linkage often reflect these aspects. Confidentiality means that an organization takes technical and organizational measures to ensure they have appropriately secured personal data (Schantz, 2020). As mentioned above, transparency should, among other things, make it possible for users to understand why an organization has collected and processed data (Herbst, 2020). Non-linking means that an organization may not combine personal data if not absolutely necessary, and this point applies in particular to combined data that an organization collects for different purposes (Rost, 2020). To ensure users can control how an organization uses their data (Tucker, 2014), an organization needs to provide features to show the type and extent of data use. Accordingly, we formulate:

DP4: Provide the system with features that show the type and extent of the data use to afford users control over the use of their data.

To increase the extent to which users accept and adopt an assistance system, employers need to inform and involve employees in the implementation process to consider data subjects' rights (Jacobs et al., 2019). These rights provide an opportunity to access, rectify, erase and transfer the collected personal data (Schnebbe, 2020b). Employees also want the possibility to view and delete collected and stored personal data to protect their information privacy (Billie, Dale). To ensure users can consider their data subject rights, employers need to provide features that allow employees to exercise the right to access, rectify, delete, and transfer collected data about them. Accordingly, we formulate:

DP5: Provide the system with features that enable the right to access, rectify, delete, and transfer the collected data to afford users the ability to exercise their data subject rights.

Data collection can provide an opportunity to enhance employees' performance and efficiency (Maltseva, 2020). Due to these enhancements, employers need to inform their employees about the potential for an assistance system to improve their work performance or their working conditions (Schall et al., 2018); particularly those users with a rather low to medium willingness to use an assistance system (Chris, Dale). In regard to whether employees accept employee-determined data collection and use, Allen et al. (2007) found that they develop better attitudes toward workplace monitoring when they understand the reason for it. In addition, Chellappa and Sin (2005) have argued that, when it comes to using online personalization services, users perceive personalization's benefits to outweigh the negative impact from privacy concerns. In the same context, Rosenthal et al. (2019) found that users' trust in the service provider increased when they could see the value of the information personalization. Moreover, individuals are more likely to use assistance systems in the workplace if they believe they will improve their efficiency and increase their productivity (Yildirim & Ali-Eldin, 2019). Thus, to enable users to understand the benefits associated with data, employees need to incorporate features in their systems that show the potential benefits associated with data collection and use. On the other hand, data collection also entails some disadvantages, such as the potential for an employer to monitor an individual's working performance, with the associated consequences for the subject's employment, which the employer has to take into consideration (Maltseva, 2020). To mitigate these disadvantages, employers can provide information about potential risks to promote transparency about their data-collection, -use, and -storage processes, which, in turn, can increase the extent to which employees trust their employers by showing that the latter recognize the risks and take them seriously (Bleier & Eisenbeiss, 2015). To enable users to understand data collection's disadvantages, employers need to provide features that show the potential risks associated with data collection and use. Correspondingly, we formulate:

DP6a: Provide the system with features that show the potential benefits of data collection and use to afford users the ability to recognize the associated advantages.

DP6b: Provide the system with features that show the potential risks of data collection and use to afford users the ability to recognize the associated disadvantages.

The participants who conducted our persona survey also mentioned the demand for protection against data security breaches and data misuse (Alex, Billie, Dale). Both privacy concerns and security concerns can lead employees to perceive increased risk (Xu et al., 2011; Bandara et al., 2019), which may decrease their trust in the employer and in the overall data-collection, -use, and -storage process. To avoid unexpected interference with data integrity, organizations must implement additional security functions (Merhar et al., 2018). These functions ensure they can restore a compromised data set. To afford protection against data misuse for users, organizations need to provide features to secure data. Hence, we formulate:

DP7: Provide the system with data security features to afford users protection against data misuse.

To improve trust in an assistance system, other users should not be able to identify data gained from using it (Kolter & Pernul, 2009; Berkemeier et al., 2017). By anonymizing and pseudonymizing personal data, organizations ensure that third parties cannot track a user's behavior (Shubina et al., 2019). In particular, employees with a low to medium willingness to use PAS and increased skepticism towards the employee-determined data collection and use need to implement data anonymization and pseudonymization (Chris, Dale). To protect users against other users from drawing conclusions about them, employers need to provide features that anonymize and pseudonymize personal data. Hence, we formulate:

DP8: Provide the system with features for anonymizing and pseudonymizing personal data to afford users protection against other system users individually identifying them.

3.4 Step 3: Evaluation of Design Principles

In the final step of our research process, we evaluated the eight design principles in a focus group discussion with potential PAS users and a workshop with experts from different work domains.

3.4.1 Focus Group

A focus group refers to a moderated discussion among several participants on a specific topic that seeks to elicit participants' personal opinions, experiences, and assessments of the topic at hand. By using focus groups, one can allow participants to exchange in-depth information through an open discussion; understand individual argumentations, value systems, and possible fears; and gain new insights into and shed light on previously defined questions from different perspectives (Stewart & Shamdasani, 2017; Schulz et al., 2012). We conducted a focus group discussion with practitioners to gain their feedback on the eight design principles and asked them to rank them in importance. Furthermore, we conducted the focus group to reveal whether we should dismiss the design principles we formulated, adjust them, or even add new ones. To recruit the focus group, we contacted 20 educational institutions, explained our research aim, and asked for interested participants.

We conducted the focus group to facilitate interactions among participants and maximize how much quality information we could collect in the limited time available, as recommended by Acocella (2012). Therefore, the focus group comprised six male participants (average age 25) from a mechatronics trainee class. According to Gill et al. (2008), a focus group with six participants ensures that a lively discussion takes place while remaining manageable for the moderator. All participants had worked for at least three years in various manufacturing and technical service companies. Three participants indicated they already used wearables and assistance systems such as a tablet or smart glass for single work steps. Three participants had no experience at all with assistance systems in the workplace. In terms of age, professional background, and experience, we can describe the focus group as homogeneous, which should facilitate interaction (Acocella, 2012). However, in terms of experience with (personalized) assistance systems, we can describe the focus group as heterogeneous, which means we could collect different views and opinions on the topic (Acocella, 2012).

To introduce the topic, we defined PAS and used the Vuzix M400 smart glass to exemplify a wearable device that could be part of a PAS. In addition, we asked the participants to give examples of applications from their everyday working life in which they could imagine using smart glasses.

After the focus group had finished its discussion and they had discussed all design principles, we asked each participant to prioritize the design principles according to their importance to them (1 = highest priority; 8 = lowest priority). We used the "Slido" live ranking survey tool to ask for prioritization. We determined the prioritization ranking in the following manner: a design principle that a participant ranked as the highest priority (i.e., 1) received eight points, while a design principle that a participant ranked as the lowest priority (i.e., 8) received one point. At the end, we summed the points and divided them by six (i.e., the number of participants). We worded the design principles in a simpler manner for this task to help participants read and understand them. We audio-recorded the focus group. We obtained written informed consent for recording from all participants. The discussion lasted 60 minutes.

We found that participants prioritized protection against data misuse (DP7) as the most important aspect. In second and third place, respectively, they found it important for an assistance system to provide functions for displaying the type and extent to which it uses data (DP4) and offer users options to view, correct, and delete collected data themselves (DP5). In contrast, they ranked the advantages and disadvantages of data collection and use (DP6a and DP6b) and the provision of a privacy statement with each use of the PAS (DP1) as the second-least and least important aspects, respectively. We provide the results in Appendix C.

Generally, the participants indicated that they felt fine with their employer collecting and using their personal data if they could ensure that their employer sufficiently protected the data against unauthorized access and misuse. The stronger the users' sense of security, the fewer concerns they would have about the type of data that their employer collected and the extent to which the employer used it. Suggestions for what employers would need to fulfill for users to feel more secure include:

- Being transparent in communicating access rights to data collected
- Providing employees with information or confirmation each time someone accessed employee-determined data
- Storing data in secure (encrypted) databases, and
- An external agency, organization, or authority audited the company's IT and security infrastructure to verify that it sufficiently protected against data misuse.

The focus group agreed that trust in employers about how they handle employee-determined data plays a central role in whether they accept data sharing in PAS. Should employers abuse or violate this trust even just once, their willingness to disclose data would no longer exist. Furthermore, focus group participants found it more important to know why their employer collected data and to be able to access, rectify, or even delete the collected data at any time than they found deciding which data their employer should collect. Accordingly, an assistance system should show users what data it will collect and how the organization will use it before they use it for the first time.

When we asked participants what data an employer might collect (i.e., the type and extent of data collection), they noted that the employer should collect people's real names rather than a pseudonym. As for why, they noted that colleagues in a company usually know each other and lack anonymity anyway. They also noted that it would be helpful to know who has completed which tasks so that they could more easily and quickly identify who to contact about any questions, problems, or ambiguities. Therefore, they placed lesser importance on data anonymization compared to other privacy aspects. According to the focus group, employers could collect the following employee-determined data in justified cases:

- Physiological data, such as blood pressure, to send an emergency signal when people work alone to allow first responders to find them in emergency situations
- Body measurements, such as body weight and height or shoe and clothing size, for providing work clothes or personal protective equipment,
- User preferences for languages other than the main language that the company uses to allow users to automatically adjust the system language.

However, the participants also had skeptical opinions about the following employee-determined data:

- Location-tracking data
- Time records
- Audio and image recordings.

The participants expressed increased concerns that users might feel as though their employer monitored or observed them if they collected such data. Participants seemed particularly sensitive to a PAS's recording functions. For remote maintenance, recordings or audio and video transmissions would be practical and even desirable to reduce service costs and repair or maintenance time. Beyond that, users tended to express aversion to recording functions. If a PAS had recording options, the focus group participants felt that the system's display would need to show clearly whether, for example, the microphone or the camera were switched on or off. Furthermore, they suggested that systems should retain audio and video recordings only temporarily and automatically delete them after a few hours or days (similar to a public surveillance camera, which overrides or deletes recordings after a certain amount of time).

The participants noted that a PAS should have a data-protection declaration and show it on first use. Additionally, they noted a supervisor or the data-protection officer should verbally explain and sign it. According to the focus group, the data-protection statement should not exceed three pages and be easy to understand (i.e., plain language).

In conclusion, the focus group evaluation confirmed the need for all eight design principles to enable employee-determined data collection and use for PAS. Furthermore, it confirmed the existing principles as sufficient since participants did not raise any further aspects or topics that the design principles did not already cover. Accordingly, we had no need to either delete any design principle or to add new ones.

3.4.2 Expert Workshop

We further evaluated the design principles as the focus group prioritized them in an expert workshop that brought together this paper's authors and six experts from the engineering (one expert), law (one expert), technical service (three experts), and IT science (one expert) domains. We conducted the workshop to review and interpret the results from the focus group. Furthermore, we discussed implementation options for each design principle to find out which principles we could merge and which lacked technical feasibility and, thus, could be discarded. The workshop lasted for four hours.

Based on the expert workshop, we made three adjustments to the design principles' number and wording (see Table 4). First, we noticed that the focus group made no major distinctions between the type of data that an assistance system collected and the extent to which it collected data (the second and fourth prioritized DPs; see Appendix C)). These two design principles involve the affordance to control the collected data to promote transparency and only differed in terms of the material property. However, the experts believed that the same feature would probably cover the affordance to offer users more control in the data-collection and -use process (i.e., material property) when implemented (e.g., by presenting the type and extent of data use and collection in a concise format that allows users to quickly overview the PAS at any time). Therefore, we merged these two design principles to avoid unnecessary complexity. As a result, the total number of design principles was reduced from eight to seven (see Table 4, DP2).

Second, we reformulated the initial DP2. Previously, simple and understandable language referred in particular to the privacy policy. In the focus group, it became clear that all information processing and communication related to the data-collection and -use process should be simple and easy to understand (see Table 4, DP4). Furthermore, in addition to any text, users should be easily able to understand any presentation concerning the data-collection and -use process given that PAS could use videos or graphics to present the required information.

Table 4. Final Set of Design Principles*

No. (1 = highest priority)	**Design principle** (italicized = material properties, bold = affordances)
1	Provide the system with *data security features* to afford users **protection against data misuse.**
2	Provide the system with *features that show the type and extent of data use and collection* to afford users **control over the use of their data.**
3	Provide the system with *features that enable the right to access, rectify, delete, and transfer the collected data* to afford users **the ability to exercise their data subject rights.**
4	Provide the system with *features for simple and understandable presentation of information* to afford users **the ability to comprehend data-collection, -use, and -storage processes.**
5	Provide the system with *features for pseudonymizing personal data* to afford users **protection against other system users individually identifying them.**
6	a) Provide the system with *features that show the potential benefits of data collection and use* to afford users **the ability to recognize the associated advantages.**
	b) Provide the system with *features that show the potential risks of data collection and use* to afford users **the ability** to **recognize the associated disadvantages.**
7	Provide the system with *features that clearly demonstrate the privacy policy* to afford users **transparency about data-collection, -use, and –storage processes.**
* Note: we refer to these principles as "prioritized design principles" in the paper.	

Third, we changed the initial DP8 to refer to pseudonymization rather than anonymization since, according to the experts, in order to enable personalization, a PAS can never be completely anonymous (see Table 4, DP5).

4 Discussion

In this study, we developed seven design principles for PAS that respect privacy. We followed a multi-method research process in which we searched the literature, gathered requirements, and conducted a focus group and an expert workshop to evaluate the design principles we developed. The proposed design principles consider the GDPR legal environment and guidelines for privacy by design and privacy by control. Moreover, our design principles extend these guidelines with further requirements as potential PAS users in a business environment indicated. In particular, the design principles suggest that employers should implement material properties in their PAS that allow users to determine the extent to which the PAS collect and use data for personalization.

Concerning the skeptical opinions in the focus group, we also found conflicting statements. On the one hand, users accept data storage to run the PAS. However, on the other hand, they feel quite uncomfortable when a PAS records their own voice or dialogue with colleagues. This conflict manifests itself in another example: some employees feel that their company could spy on them. Simultaneously, the same people normally trust their employer. Possible reasons for these conflicting opinions could be different subjective perceptions towards privacy concerns or different character traits.

Our study integrates and extends previous research on PAS in the workplace. Previous studies have investigated factors that influence the willingness to use wearable devices (Buenafor & Kim, 2013; Choi et al., 2017; Jacobs et al., 2019; Kalantari, 2017; Sergueeva et al., 2019). Our study goes beyond these influencing factors by considering the business environment and the legal environment for PAS. By listing the differences between our study and other publications (see Appendix A), we point out that our contribution offers unique added value.

Our design principles reflect previous knowledge about technology acceptance as we found in the literature, which we extended with our own empirical research. From our findings, we can see that PAS users perceive protection against data misuse as particularly important, which prioritized DP1 reflects (see Table 4). The focus group expressed the view that organizations need to implement suitable material properties in a PAS for users to accept the system, which means we can consider it mandatory. Prior studies have shown organizational safety climate as a common factor that predicts whether users accept assistance systems (Choi et al., 2017; Jacobs et al., 2019). Consequently, focusing on data protection leads users to accept personalized services such as assistance systems at higher levels (Chellappa and Sin, 2005; Bélanger & Crossler, 2011; Bleier & Eisenbeiss, 2015; Bandara et al., 2019). Especially in relation to person-related data, users perceive control over the type and extent of data use as particularly important.

Prioritized DP2 reflects the notion that employees can reduce the fear of losing autonomy when working with PAS by providing them with material properties that show the type and extent of data use and collection and let them control the use of their data (see Table 4). For example, an organization could ask users if they it could use their data to improve workflows or for data evaluations, such as how much time the organization spent on one project. That lower levels of self-determination can have a negative influence on users' intrinsic motivation, which, in turn, affects the extent to which they accept assistance systems concurs with previous studies (Attig et al., 2018; Oesterle et al., 2019). A perceived loss of autonomy can lead to significantly lower motivation and, therefore, to lower PAS acceptance (Haerens et al., 2010).

Prioritized DP3 (see Table 4) affords the highest possible degree of self-determination regarding data usage. Other research studies have already shown that control over data collection leads to greater acceptance among users (Frische et al., 2021). Increased acceptance, in turn, leads to a greater willingness to use PAS in the first place (Buenaflor & Kim, 2013). Users attach special importance to the degree of self-determination about what data one may collect from them, especially when it comes to recording and tracking data (e.g., location tracking data, time records, audio and image recordings) (Ryan & Deci, 2000; Teixeira et al., 2012). Particularly with regard to this sensitive data, users need to know the purpose for which the employer will use it.

Prioritized DP4 (see Table 4) reflects the need for simple communication, which includes, for example, understandable language and easily accessible information. Understanding leads to trust, an important factor for people to adopt wearable technologies in the workplace (Jacobs et al., 2019). The focus group agreed with prior literature (Segura Anaya et al., 2018) that everything the PAS communicates to users must be clearly and easily understandable.

Prioritized DP5 (see Table 4) affords users the ability to pseudonymize personal data, which represents another way to give them more control over their data. The reason why focus group participants prioritized this design principle lower than other ones this aspect from the focus group, compared to other security-related design principles, might be that people perceive pseudonymization as a feature that protects against internal violations, whereas prioritized DP1 (see Table 4) protects data security from both internal and external violations.

Prioritized DP6 (see Table 4) reflects the advantages and disadvantages of collecting and using personal data. Informing employees about potential risks helps to increase perceived transparency and, thus, trust in the employer (Woźniak et al., 2020). Further, it can lead employees to better understand why the employer uses an assistance system, which improves their attitudes towards it (Allen et al., 2007). However, our focus group participants did not see the function of communicating potential benefits and risks comprehensively as a necessary feature for a PAS (see Table 4, DP 6).

Prioritized DP7 (see Table 4) affords users the ability to view an employer's privacy policy on request, which gives them greater autonomy and increases transparency. The focus group did not perceive this DP as especially necessary as they felt they needed to see the information only once to feel sufficiently informed.

By providing seven employee-determined design principles for data collection and use, this study also yields practical relevance. To the best of our knowledge, this study constitutes the first comprehensive work that compiles design principles that an organization should fulfill to sufficiently cover all criteria relevant to data protection in PAS. We legitimize our contribution via clearly and practically implementing legal requirements and adopting further measures to improve user acceptance. The design principles correspond and extend to legal requirements such as the GDPR. In presenting our design principles, we provide, among other things, a framework for software designers developing PAS so that they can make design processes more efficiently. This framework can ensure that organizations can introduce PAS that respect privacy more quickly into work environments. Additionally, developing PAS by applying our design principles can increase the extent to which employees accept their employers collecting and processing their personal data and reduce their concerns over data privacy. In a next step, we plan to implement these seven design principles in the two companies from the industrial sector in Germany that took part in the persona survey.

5 Conclusion, Limitations, and Further Research

With this study, we developed seven design principles for PAS that respect privacy. Through our three-step multi-method approach, we provide in-depth, empirically derived insights regarding the challenges in collecting and using data from a user's point of view. We developed our set of design principles based on employee-centered approaches to privacy control, privacy by design, and privacy by default (i.e., legally compliant data collection and processing). In our research process, we first collected and clustered requirements from the literature and from four user personas that we derived from a qualitative survey with practitioners. Furthermore, we derived affordances and material properties and formulated initial eight design principles based on the identified requirements. Finally, we evaluated and prioritized these design principles with a focus group and further refined them in an expert workshop. This process resulted in seven final design principles that pertain to employee-centric data collection and use processes in PAS.

As with any study, this one has some limitations. First, we developed the user personas based on statements from two informants from two companies (both team leaders). Therefore, we cannot rule out that greater variety in respondents might have resulted in slightly altered user personas. Second, we cannot rule out a possible age or gender bias in the focus group as all participants were male and 25 years old on average. Greater variety in age, gender, and occupation might have resulted in further or other opinions on the developed design principles. Generally, a higher number of informants in the empirical steps of our research process could have resulted in our developing more reliable and generalizable findings. Third, we used the tool “Slido” to prioritize the design principles in the focus groups. This tool displayed only the end results but no individual prioritization rankings. Therefore, we could not possibly make statements about conflicting opinions based on individual rankings. Fourth, some of our findings resulted from the subjective manner in which we interpreted the literature, law articles, and survey data. When dealing with these data sources, we as researchers engaged in a joint sensemaking process to consensually understand user requirements in order to derive meaningful design principles for PAS. Other researchers might have interpreted the underlying data differently and formulated different design principles. However, the two evaluation steps in our research process support our impression that we have identified a meaningful set of design principles. Another limitation concerns the legal environment we considered. To develop our design principles, we oriented ourselves to the GDPR, which countries outside the EU do not need to follow.

Nevertheless, we think that, due to the GDPR's high standard, the design principles also offer added value for non-EU countries.

We believe that the presented design principles will inspire future research. For instance, researchers could validate them for a wider range of different industries (e.g., some with even higher default data-protection standards, such as healthcare or work with classified information). In such settings, users might deviate from data protection and control over that data as the most important PAS aspects and emphasize other design principles as more important due to a generally higher data protection standard. As a next step for our research, we plan to implement the design principles with a prototype assistance system. Through the expert workshop, we gathered possible implementation options for each design principle. We plan to test the design principles and the specific design options in practical experiments with a functioning prototype. Moreover, we also plan to research the specific features for personalized assistance in more detail (e.g., regarding the identification of a worker's expertise level).

Acknowledgments

This contribution is part of the project "Development of a Privacy Management System for Personalized Assistance Systems in Production and Service" (PersonA) and funded by the German Federal Ministry of Education and Research (promotional codes: 02L18B550 and 02L18B551).

References

Acocella, I. (2012). The focus groups in social research: Advantages and disadvantages. *Quality & Quantity*, *46*(4), 1125-1136.

Adomavicius, G., & Tuzhilin, A. (2005). Personalization technologies: A process-oriented perspective. *Communications of the ACM*, *48*(10), 83-90.

Ahmad, R., Siemon, D., Gnewuch, U., & Robra-Bissantz, S. (2022). Designing personality-adaptive conversational agents for mental health care. *Information Systems Frontiers*, 1-21.

Allen, M., Coopman, S. J., Hart, J. L., & Walker, K. L. (2007). Workplace surveillance and managing privacy boundaries. *Management Communication Quarterly*, *21*(2), 172-200.

Attig C., Karp A., Franke T. (2018). User diversity in the motivation for wearable activity tracking: A predictor for usage intensity? In *Proceedings of the 20th Congress of the International Ergonomics Association.*

Awolusi, I., Nnaji, C., Marks, E., Hallowell, M. (2019). Enhancing construction safety monitoring through the application of Internet of things and wearable sensing devices: A review. In Y. K. Cho, F. Leite, A. Behzadan, & C. Wang (Eds.), *Computing in civil engineering 2019* (pp. 530-538). ASCE.

Bandara, R., Fernando, M., & Akter, S. (2019). Privacy concerns in E-commerce: A taxonomy and a future research agenda. Electronic Markets.

Bélanger, F., & Crossler, R.E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017-1042.

Benke, I., Feine, J., Venable, J. R., & Maedche, A. (2020). On implementing ethical principles in design science research. *AIS Transactions on Human-Computer Interaction*, *12*(4), 206-227.

Berkemeier, L., McGuire, M. R., Steinmann, S., Niemöller, C., & Thomas, O. (2017). Datenschutzrechtliche Anforderungen an Smart Glasses-basierende Informationssysteme in der Logistik. In *Proceedings of Informatik.*

Bleier, A., & Eisenbeiss, M. (2015). The importance of trust for personalized online advertising. *Journal of Retailing*, *91*(3), 390-409.

Böckelmann, I., & Minow, A. (2018). Nutzung digitaler Assistenzsysteme. *Arbeitsmed Sozialmed Umweltmed*, *53*, 705-710.

Buchanan, W. J., Kwecka, Z., & Ekonomou, E. (2013). A privacy preserving method using privacy enhancing techniques for location based services. *Mobile Networks and Applications*, *18*(5), 728-737.

Buenaflor, C., & Kim, H. (2013). Six human factors to acceptability of wearable computers. *International Journal of Multimedia and Ubiquitous Engineering*, *8*, 103-225.

Chandra, L., Seidel, S., & Gregor, S. (2015). Prescriptive knowledge in IS research: Conceptualizing design principles in terms of materiality, action, and boundary conditions. In *Proceedings of the 48th Hawaii International Conference on System Sciences.*

Chellappa, R. K., & Sin, R. G. (2005). Personalization versus privacy: An empirical examination of the online consumer's dilemma. *Information Technology and Management*, *6*(2-3), 181-202.

Choi, B., Hwang, S., & Lee, S. (2017). 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.

Cooper, A. (1999). *The inmates are running the asylum: Why high-tech products drive us crazy and how to restore the sanity*. Sams.

Cooper, H. M. (1988). Organizing knowledge syntheses: A taxonomy of literature reviews. *Knowledge in Society*, *1*(1), 104-126.

Culnan, M. J., & Armstrong, P. K. (1999). Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science*, *10*(1), 104-115.

Frische, A. K., Kirchner, J. F., Pawlowski, C., Halsbenning, S., & Becker, J. (2021). Leave no one behind: Design principles for public warning systems in federalism. In *Proceedings of the International Conference on Wirtschaftsinformatik.*

Gil, D., Hernández-Sabaté, A., Castells-Rufas, D., & Carrabina, J. (2017). CYBERH: Cyber-physical systems in health for personalized assistance. In *Proceedings of the 19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing.*

Gill, P., Stewart, K., Treasure, E., & Chadwick, B. (2008). Methods of data collection in qualitative research: Interviews and focus groups. *British Dental Journal*, *204*(6), 291-295.

Göker, A., & Myrhaug, H. I. (2002). *User context and personalisation*. Retrieved from https://www.researchgate.net/profile/Ayse-Goker/publication/220831661_User_Context_and_Personalisation/links/0deec53a90ff3598c5000000/User-Context-and-Personalisation.pdf#page=4

Gregor, S., Chandra Kruse, L., & Seidel, S. (2020). Research perspectives: The anatomy of a design principle. *Journal of the Association for Information Systems*, *21*(6), 1622-1652.

Haerens, L., Kirk, D., Cardon, G., De Bourdeaudhuij, I., & Vansteenkiste, M. (2010). Motivational profiles for secondary school physical education and its relationship to the adoption of a physically active lifestyle among university students. *European Physical Education Review*, *16*(2), 117-139.

Herbst. (2020). Article 5 Grundsätze für die Verarbeitung personenbezogener Daten, Rn. 18f. In J. Kühling & B. Buchner (Eds.), *Datenschutz-Grundverordnung/Bundesdatenschutzgesetz*. CH Beck.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly*, *28*(1), 75-105.

Hui, K. L., Teo, H. H., & Lee, S.-Y. T. (2007). The value of privacy assurance: An exploratory field experiment. *MIS Quarterly*, *31*(1), 19-33.

Hwang, Y., Al-Arabiat, M., & Shin, D.-H. (2016). Understanding technology acceptance in a mandatory environment. *Information Development*, *32*(4), 1266-1283.

Ioannidou, I., & Sklavos, N. (2021). On general data protection regulation vulnerabilities and privacy issues, for wearable devices and fitness Tracking Applications. *Cryptography*, *5*(4).

Jacobs, J. V., Hettinger, L. J., Huang, Y.-H., Jeffries, S., Lesch, M. F., Simmons, L. A., Verma, S. K., & Willetts, J. L. (2019). Employee acceptance of wearable technology in the workplace. *Applied Ergonomics*, *78*, 148-156.

Kalantari, M. (2017). Consumers' adoption of wearable technologies: Literature review, synthesis, and future research agenda. *International Journal of Technology Marketing*, 12(3), 274-307.

Kasselmann, S., & Willeke, S. (2016). 4.0 ready. *International Performance Research Institute*. Retrieved from https://www.iph-hannover.de/_media/files/downloads/Projekt_40-Ready_Technologie-Kompendium.pdf

Klapper, J., Pokorni, B., & Hämmerle, M. (2020). A potential analysis of cognitive assistance systems in production areas. In *Proceedings of the 3rd International Conference on Intelligent Human Systems Integration.*

Kolter, J., & Pernul, G. (2009). Generating user-understandable privacy preferences. In *Proceedings of the International Conference on Availability, Reliability and Security.*

Landau, S. (2015). Control use of data to protect privacy. *Science*, *347*(6221), 504-506.

Lapointe, L., & Rivard, S.A. (2005). Multilevel model of resistance to information technology implementation. MIS *Quarterly*, *29*(3), 461-491.

Laumer, S., Maier, C., Eckhardt, A., & Weitzel, T. (2016). User personality and resistance to mandatory information systems in organizations: A theoretical model and empirical test of dispositional resistance to change. *Journal of Information Technology*, *31*(1), 67-82.

Lee, Y., Yang, W., & Kwon, T. (2018). Data transfusion: Pairing wearable devices and its implication on security for internet of things. *IEEE Access, 6*, 48994-49006.

Luse, A., & Burkman, J. (2020). Wearables in the workplace: Examination using a privacy boundary model. *Journal of the Midwest Association for Information Systems*, *2*(7), 7-15.

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336-355.

Maltseva, K. (2020). Wearables in the workplace: The brave new world of employee engagement. *Business Horizons*, *63*(4), 493-505.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. *Journal of Marketing*, *81*(1), 36-58.

Merhar, L., Berger, C., Braunreuther, S., & Reinhart, G. (2018). Digitization of manufacturing companies: Employee acceptance towards mobile and wearable devices. In T. Ahram (Ed.), *Advances in intelligent systems and computing* (AISC vol. 795, pp. 187-197). Springer.

Mettler, T., & Wulf, J. (2019). Physiolytics at the workplace: Affordances and constraints of wearables use from an employee's perspective. *Information Systems Journal*, *29*(1), 245-273.

Mewes, E., Bergmüller, A., Minow, A., Waßmann, S., Weigel, M., Eichholz, S., Adler, S., Böckelmann, I., Schmicker, S., & Mecke, R. (2020). *Digitale assistenzsysteme zur mobilen verwendung im technischen service: Ein leitfaden für die gestaltung und nutzung*. Otto von Guericke University Library.

Niehaus, J. (2017). Mobile *assistenzsysteme für industrie* 4.0: Gestaltungsoptionen zwischen Autonomie und Kontrolle. Retrieved from https://www.fgw-nrw.de/fileadmin/user_upload/FGW-Studie-I40-04-Niehaus-A1-web-komplett.pdf

Oesterle, S., Trübenbach, B., & Buck, C. (2019). Intent and the use of wearables in the workplace: A model development. In *Proceedings of the 14th International Conference on Wirtschaftsinformatik.*

Perugini, S., & Ramakrishnan, N. (2003). Personalizing web sites with mixed-initiative interaction. *IT Professional*, *5*(2), 9-15.

Psychoula, I., Chen, L., & Amft, O. (2020). Privacy risk awareness in wearables and the internet of things. *IEEE Pervasive Computing*, *19*(3), 60-66.

Riesenhuber. (2020). Wirksamkeitsvoraussetzungen, BDSG § 26 Rn. 45. In H. Wolff & S. Brink (Eds.), *BeckOK Datenschutz* (34th ed.).

Rosenthal, S., Wasenden, O.-C., Gronnevet, G.-A., & Ling, R. (2019). A tripartite model of trust in Facebook: Acceptance of information personalization, privacy concern, and privacy literacy. Media *Psychology*, *23*(2), 1-25.

Roßnagel. (2019). Gründe der Datenminimierung, Article 5 Rn. 118. In S. Simitis, G. Hornung, & I. Spiecker (Eds.), *Datenschutzrecht*.

Rost, M. (2020). Handbuch zum Standard-Datenschutzmodell—Version 2.0. *Freie Hansestadt Bremen*. Retrieved from https://www.transparenz.bremen.de/metainformationen/handbuch-zum-standard-datenschutzmodell-version-2-0-59249?asl=bremen02.c.732.de

Ryan, R. M., & Deci, E. L. (2000). Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *American Psychologist*, *55*(1), 68-78.

Salminen, J., Guan, K., Jung, S. G., & Jansen, B. J. (2021). A survey of 15 years of data-driven persona development. *International Journal of Human-Computer Interaction*, *37*(18).

Savekar, A. (2021). Industrial wearables market expected to reach $8.40 billion by 2027. *Allied Market Research*. Retrieved from https://www.alliedmarketresearch.com/press-release/industrial-wearables-market.html

Schall, M. C. Jr., Sesek, R. F., & Cavuoto, L. A. (2018). Barriers to the adoption of wearable sensors in the workplace: A survey of occupational safety and health professionals. *Human Factors*, *60*(3), 351-362.

Schantz. (2020). Rechenschaftspflicht, DS-GVO article 5 Rn. 37-39. In H. Wolff & S. Brink (Eds.), *BeckOK datenschutzrecht* (34th ed.).

Schnebbe, M. (2020a). Digitale Assistenzsysteme in der Industrie und Produktion. *Datenschutz und Datensicherheit-DuD*, *44*, 398-400.

Schnebbe, M. (2020b). *Privatsphäre-Management-Systeme für digitale Assistenzsysteme in Industrie und Produktion.* Retrieved from https://dsrinas.synology.me/herbstakademie/ha20/maximilian_schnebbe/maximilian_schnebbe.pdf

Schulz, M., Mack, B., & Renn, O. (Eds.). (2012). *Fokusgruppen in der empirischen Sozialwissenschaft: Von der Konzeption bis zur Auswertung.* Springer.

Segura Anaya, L. H., Alsadoon, A., Costadopoulos, N., Prasad, P. W. C. (2018). Ethical Implications of user perceptions of wearable devices. *Science and Engineering Ethics*, *24*, 1-28.

Seidel, S., Chandra Kruse, L., Székely, N., Gau, M., & Stieger, D. (2018). Design principles for sensemaking support systems in environmental sustainability transformations. *European Journal of Information Systems*, *27*(2), 221-247.

Sein, M. K., Henfridsson, O., Purao, S., Rossi, M., & Lindgren, R. (2011). Action design research. *MIS Quarterly*, *35*(1), 37-56.

Sergueeva, K., Shaw, N., & Lee, S. H. (2019). Understanding the barriers and factors associated with consumer adoption of wearable technology devices in managing personal health. *Canadian Journal of Administrative Sciences*, *37*(1), 45-60.

Sethumadhavan, A. (2017). Designing wearables that users will wear. *Ergonomics in Design*, *26*(1), 29.

Shubina, V., Ometov, A., Niculescu, D., & Lohan, E-S. (2019). Challenges of privacy-aware localization on wearable devices. In *Proceedings of XXXV Finnish URSI Convention on Radio Science.*

Spil, T. A., Kijl, B., & Romijnders, V. (2019). The adoption and diffusion of wearables. In *Proceedings of the International Working Conference on Transfer and Diffusion of IT.*

Stewart, D. W., & Shamdasani, P. (2017). Online focus groups. *Journal of Advertising*, *46*(1), 48-60.

Svertoka, E., Saafi, S., Rusu-Casandra, A., Burget, R., Marghescu, I., Hosek, J., & Ometov, A. (2021). Wearables for industrial work safety: A survey. *Sensors*, *21*(11), 1-25.

Teixeira, P.J., Carraça, E. V., Markland, D., Silva, M. N., & Ryan, M. (2012). Exercise, physical activity, and self-determination theory: A systematic review. *International Journal of Behavioral Nutrition and Physical Activity*, *9*, 1-30.

Tucker, C. E. (2014). Social networks, personalized advertising, and privacy controls. *Journal of Marketing Research*, *51*(5), 546-562.

Ulmer, J., Braun, S., Cheng, C.-T., Dowey, S., & Wollert, J. (2020). Human-centered gamification framework for manufacturing systems. *Procedia CIRP*, *93*, 670-675.

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R., & Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *Proceedings of the European Conference on Information Systems.*

Wentzel, J., Velleman, E., & van der Geest, T. (2016). Developing accessibility design guidelines for wearables: Accessibility standards for multimodal wearable devices. In M. Antona & C. Stephanidis (Eds)*, Universal access in human-computer interaction: Methods, techniques, and best practices* (LNCS vol. 9737, pp. 109-119). Springer.

White, T. B., Zahay, D. L., Thorbjørnsen, H., & Shavitt, S. (2008). Getting too personal: Reactance to highly personalized email solicitations. *Marketing Letters*, *19*(1), 39-50.

Woźniak, P. W., Kucharski, P. P., de Graaf, M. M. A., & Niess, J. (2020). Exploring understandable algorithms to suggest fitness tracker goals that foster commitment. In *Proceedings of the 11th Nordic Conference on Human-Computer Interaction.*

Xu, H., Dinev, T., Smith, J., & Hart, P. (2011). Information privacy concerns: Linking individual perceptions with institutional privacy assurances. *Journal of the Association for Information Systems*, *12*(12), 798-824.

Yildirim, H., & Ali-Eldin, A. M. (2019). A model for predicting user intention to use wearable IoT devices at the workplace. *Journal of King Saud University—Computer and Information Sciences*, *31*(4), 497-505.

Ziccardi, G. (2020). Wearable technologies and smart clothes in the fashion business: Some issues concerning cybersecurity and data protection. *Laws*, *9*(2).

Appendix A: Differentiation from Other Relevant Publications

Table A1. How the Top Six Topic-relevant Publications Differ from our Contribution

Reference	Contribution	Differences to our contribution
Berkemeier et al. (2017)	The authors provide requirements for smart glasses-based information systems in a working context by focusing on the GDPR	Berkemeier et al. (2017) address the work context and the GDPR. However, they do not holistically consider different motivational reasons for employees to use personalized assistance systems (e.g., via different user personas).
Ioannidou & Sklavos (2021)	The authors list the most critical privacy and security aspects in popular commercial fitness-tracking applications.	Ioannidou and Sklavos (2021) omit deeper implications related to GDPR-compliant design of wearables and have no work-relevant context.
Luse & Burkman (2020)	The authors investigate the use of RFID wearables in a corporate environment by using a privacy boundary model. Greater buy-in from employees can be generated with greater transparency in implementing wearables and the associated data processing.	Luse and Burkman (2020) show impact that using RFID wearables has on consent to use or implement wearables in the work context. However, they do not consider data-protection aspects and the necessary criteria in detail.
Mettler & Wulf (2019)	The authors use an affordance theory lens to identify five distinct user types of physiolytics wearables. In doing so, they better explain the broader implications and possible responses to introducing wearable technologies in professional contexts.	Mettler and Wulf (2019) focus primarily on the increasing the extent to which user groups accept using wearables. In contrast to our contribution, they do not consider the legal conditions that have to be fulfilled in detail.
Psychoula et al. (2020)	The authors discuss privacy risk awareness and provides a corresponding privacy risk aware framework. This framework has four parts: 1) initial Set up, 2) privacy risk aware negotiation, 3) data transformation, and 4) data sharing.	Psychoula et al. (2020) focus in particular on a technical implementation in the form of a framework. As in the three previous papers, they do not consider GDPR aspects and so cannot provide any guidance for compliance in this respect.
Ziccardi (2020)	The author addresses the discrepancy of the advantages of using wearables and the issues of guaranteeing data security and the need to comply with General Data Protection Regulation No. 2016/679.	In contrast to the four previous publications, Ziccardi (2020) mentions central GDPR content. However, the author primarily focuses on consumers and does not offer any explicit implications for employees.

Appendix B: Persona Survey

Part 1: Introduction

The aim of the survey is to identify different user groups of the personalized assistance system.

Think about your respective company when answering the questions.

1) In which areas or for which tasks is the use of a personalized assistance system required?
2) In addition, are there areas/tasks that could be added in the near future (within a year) to this?

Think about all users who use (or should/will use) the personalized assistance system.

Can you form one or more user groups that you can distinguish from each other?

Think of a primary characteristic by which users could be grouped and distinguished.

Note: A user group can also consist of only one person.

Example 1: primary characteristic: work experience → user groups: trainee, young professional, experienced professional, expert.

Example 2: primary characteristic: work area → user groups: assembly work, installation work, maintenance work

3) By what primary characteristic would you distinguish your users?
4) According to the stated primary characteristic (question 3), which user groups would you create? Give a name to a user group (e.g., trainees) and list them all here. Please name no more than five user groups.

Part 2: User Group Questionnaire

Demographics/ user group background

5) Please state the (estimated) average age of each user group.
6) What activities does each user group perform within the company?
7) How much professional experience does each user group have? (an estimate is sufficient)
8) Who influences each user group? How does each user group itself have influence? (e.g., advisors on specific topics, opinion leaders, etc.)
9) What language(s) does each user group speak?
10) What is the appearance of each user group?
11) What values are important to each user group in the company?
12) What technical skills does each user group possess? How is the use of technical devices or programs to be classified?
13) Which channels does each user group primarily use to communicate?
14) Which channels does the company use to communicate with each user group?

Expectations, goals, and demands—general

15) What does each user group want to achieve? What problems does each user group want to solve? (related to the professional)
16) What benefit does each user group want to achieve? What does each user group want to achieve with its activity?
17) What is each user group's attitude toward digitalization?
18) How important is the quality of the company's products and processes for each user group?
19) What comfort does each user group desire to perform their work activities?
20) Is each user group more interested in security and staying in familiar surroundings/routines? Is the user group willing to take a risk?
21) How does each user group react to change? What does each user group want to change?

Challenges and solutions—related to personalized assistance systems

For clarification: personalized assistance system = An information technology system that provides users with computer-based and individualized support when performing their work tasks. The personalized support of the assistance system is offered and presented via its terminal in such a way that it is adapted to the tasks and situations as well as preferences, interests, behaviors, and expertise of the user. Communication to provide support to the user, as well as user input, can be visual, acoustic, or haptic.

22) What challenges does each user group currently face in its tasks?
23) What challenges does each user group face from previous experiences?
24) What challenges does each user group see for the company in terms of digitalization?
25) What is generally difficult for each user group (in terms of new technologies, digitalization)?
26) How can each user group in general be helped to overcome the challenges mentioned above?

Use of a personalized assistance system

27) What activities does the user group perform (or would perform in the future) with the help of a personalized assistance system?
28) What would the support of the work (steps) look like with the help of the personalized assistance system? (showing info windows, time tracking, etc.)
29) Does it make sense for each user group to have their own user accounts and to use them to log in to the assistance system before using it? Why?
30) Do individual users within each user group require different support from the personalized assistance system? (or do they all always need the same instructions etc.)
31) What goal(s) should be achieved by the use of personalized assistance systems for each user group?
32) What goal is the company pursuing through the use of personalized assistance systems by each user group?
33) How would you rate each user group's willingness to use a personalized assistance system?
34) What feelings accompany each user group in connection with personalized assistance systems? (e.g. curiosity, insecurity, fears, enthusiasm, etc.)
35) Why would each user group not use a personalized assistance system? What could unsettle or disturb each user group?
36) If you have any further comments to each user group, please state them here:

Appendix C: Prioritization of Design Principles

Table C1. Prioritized Design Principles for Employee-determined Data Collection and Use in Personalized Assistance Systems

Ranking points	**Prioritization** (1 = highest priority)	**Initial DP number**	**Design principles** (italicized = material properties, bold = affordances)
7.50	1	7	Provide the system with *data security features* to afford users **protection against data misuse.**
6.17	2	4	Provide the system with *features that show the type and extent of data use* to afford users **control over the use of their data.**
5.00	3	5	Provide the system with *features that enable the right to access, rectify, delete, and transfer the collected data* to afford users **the ability to exercise their data subject rights.**
4.50	4	3	Provide the system with *functions that show the type and extent of the collection of data* to afford users **control over the collected data.**
3.83	5	2	Provide the system with *features for simple and understandable language in the privacy policy* to afford users **the ability to comprehend the data-collection, -use, and -storage processes.**
3.33	6	8	Provide the system with *features for anonymizing and pseudonymizing personal data* to afford users **protection against other system users individually identifying them.**
3.17	7	6a	a) Provide the system with *features that show the potential benefits of data collection and use* to afford users **the ability to recognize the associated advantages.**
		6b	b) Provide the system with *features that show the potential risks of data collection and use* to afford users **the ability to recognize the associated disadvantages.**
2.50	8	1	Provide the system with *features that clearly demonstrate the privacy policy* to afford users **transparency about data-collection, -use, and -storage processes.**

About the Authors

Marleen Voss is research associate and PhD student at the Chair for Industrial Sales and Service Engineering at the Faculty of Mechanical Engineering at the Ruhr University Bochum, Germany. She completed her B.Sc. and M.Sc. in industrial engineering (focus on mechanical engineering). In the context of her PhD, she is working on the use of artificial intelligence in B2B sales. Her research interests also include smart services and the design of trust.

Olga Bosak is a PhD student at the markstones Institute of Marketing, Branding & Technology of the University of Bremen, Germany, since 2019. Her research interests involve understanding the privacy control approach in work contexts and exploring the extent to which privacy concerns influence the intention to use new technologies. Furthermore, she conducts research in the area of voice marketing, investigating how brand voices can be designed more efficiently for voice technologies.

Mark Hoebertz completed an apprenticeship as a wholesale salesman before studying Sales Engineering and Product Management. He is a research associate at the Chair of Industrial Sales and Service Engineering at the Faculty of Mechanical Engineering at the Ruhr University Bochum, Germany. In addition to the topic of service portfolio management, he also conducts research on the application of digital assistance systems, especially in industrial service companies.

Felix Mohsenzadeh currently works as a research assistant and doctoral student in the Digital Marketing research group at the markstones Institute of Marketing, Branding & Technology at the University of Bremen, Germany. His areas of research are privacy management and persuasive system design. Previously, he studied economics at the Friedrich-Alexander University Erlangen-Nuremberg and International Marketing and Media Management at the Rheinische Fachhochschule Cologne. After four years as a digital marketing manager and digital consultant, he returned to academia in September 2019.

Maximilian Schnebbe is author of several Books, papers and legal commentaries about data protection law. He was a researcher at the Institute of Information-, Health- and Medicine Law (IGMR) at the University of Bremen, Germany, where he finished his doctoral thesis. He is CEO and founder of the DataRight GmbH (info@dataright.de), where he advises on data protection and cybersecurity.

Jens Poeppelbuss is Full Professor of Industrial Sales and Service Engineering in the Mechanical Engineering Department at the Ruhr University Bochum, Germany. His main research interest is digital service innovation in manufacturing, especially smart service systems. His work has been published in peer-reviewed academic journals such as *Electronic Markets*, *Communications of the Association for Information Systems*, and *Business & Information Systems Engineering*. He has served regularly as associate editor and track chair for the service tracks at the *European Conference on Information Systems* and *International Conference on Information Systems*, amongst others.

Maik Eisenbeiss is a Professor of Marketing and director of the markstones Institute of Marketing, Branding & Technology of the University of Bremen, Germany. His research interests are in the areas of digital marketing, retailing, channel management, and customer relationship management. He has published in various international journals, such as Marketing Science, *Journal of Marketing, International Journal of Research in Marketing, Journal of the Academy of Marketing Science, Journal of Retailing, Journal of Service Research, and Journal of Interactive Marketing.*

Copyright © 2022 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712 Attn: Reprints or via e-mail from publications@aisnet.org.

Transactions on Human – Computer Interaction

Editor-in-Chief

https://aisel.aisnet.org/thci/

Fiona Nah, City University of Hong Kong, Hong Kong SAR

Advisory Board

Izak Benbasat, University of British Columbia, Canada
John M. Carroll, Penn State University, USA
Dennis F. Galletta, University of Pittsburgh, USA
Shirley Gregor, National Australian University, Australia
Elena Karahanna, University of Georgia, USA
Paul Benjamin Lowry, Virginia Tech, USA
Jenny Preece, University of Maryland, USA
Gavriel Salvendy, University of Central Florida, USA
Suprateek Sarker, University of Virginia, USA
Ben Shneiderman, University of Maryland, USA
Joe Valacich, University of Arizona, USA
Jane Webster, Queen's University, Canada
K.K. Wei, Singapore Institute of Management, Singapore
Ping Zhang, Syracuse University, USA

Senior Editor Board

Torkil Clemmensen, Copenhagen Business School, Denmark
Fred Davis, Texas Tech University, USA
Gert-Jan de Vreede, University of South Florida, USA
Soussan Djamasbi, Worcester Polytechnic Institute, USA
Traci Hess, University of Massachusetts Amherst, USA
Shuk Ying (Susanna) Ho, Australian National University, Australia
Matthew Jensen, University of Oklahoma, USA
Richard Johnson, Washington State University, USA
Atreyi Kankanhalli, National University of Singapore, Singapore
Jinwoo Kim, Yonsei University, Korea
Eleanor Loiacono, College of William & Mary, USA
Anne Massey, University of Massachusetts Amherst, USA
Gregory D. Moody, University of Nevada Las Vegas, USA
Stacie Petter, Wake Forest University, USA
Lionel Robert, University of Michigan, USA
Choon Ling Sia, City University of Hong Kong, Hong Kong SAR
Heshan Sun, University of Oklahoma, USA
Kar Yan Tam, Hong Kong U. of Science & Technology, Hong Kong SAR
Chee-Wee Tan, Copenhagen Business School, Denmark
Dov Te'eni, Tel-Aviv University, Israel
Jason Thatcher, Temple University, USA
Noam Tractinsky, Ben-Gurion University of the Negev, Israel
Viswanath Venkatesh, University of Arkansas, USA
Mun Yi, Korea Advanced Institute of Science & Technology, Korea
Dongsong Zhang, University of North Carolina Charlotte, USA

Editorial Board

Miguel Aguirre-Urreta, Florida International University, USA
Michel Avital, Copenhagen Business School, Denmark
Gaurav Bansal, University of Wisconsin-Green Bay, USA
Ricardo Buettner, Aalen University, Germany
Langtao Chen, Missouri University of Science and Technology, USA
Christy M.K. Cheung, Hong Kong Baptist University, Hong Kong SAR
Tsai-Hsin Chu, National Chiayi University, Taiwan
Cecil Chua, Missouri University of Science and Technology, USA
Constantinos Coursaris, HEC Montreal, Canada
Michael Davern, University of Melbourne, Australia
Carina de Villiers, University of Pretoria, South Africa
Gurpreet Dhillon, University of North Texas, USA
Alexandra Durcikova, University of Oklahoma, USA
Andreas Eckhardt, University of Innsbruck, Austria
Brenda Eschenbrenner, University of Nebraska at Kearney, USA
Xiaowen Fang, DePaul University, USA
James Gaskin, Brigham Young University, USA
Matt Germonprez, University of Nebraska at Omaha, USA
Jennifer Gerow, Virginia Military Institute, USA
Suparna Goswami, Technische U.München, Germany
Camille Grange, HEC Montreal, Canada
Juho Harami, Tampere University, Finland
Khaled Hassanein, McMaster University, Canada
Milena Head, McMaster University, Canada
Netta Iivari, Oulu University, Finland
Zhenhui Jack Jiang, University of Hong Kong, Hong Kong SAR
Weiling Ke, Southern University of Science and Technology, China
Sherrie Komiak, Memorial U. of Newfoundland, Canada
Yi-Cheng Ku, Fu Chen Catholic University, Taiwan
Na Li, Baker College, USA
Yuan Li, University of Tennessee, USA
Ji-Ye Mao, Renmin University, China
Scott McCoy, College of William and Mary, USA
Tom Meservy, Brigham Young University, USA
Stefan Morana, Saarland University, Germany
Robert F. Otondo, Mississippi State University, USA
Lingyun Qiu, Peking University, China
Sheizaf Rafaeli, University of Haifa, Israel
Rene Riedl, Johannes Kepler University Linz, Austria
Khawaja Saeed, Kennesaw State University, USA
Shu Schiller, Wright State University, USA
Christoph Schneider, IESE Business School, Spain
Theresa Shaft, University of Oklahoma, USA
Stefan Smolnik, University of Hagen, Germany
Jeff Stanton, Syracuse University, USA
Chee-Wee Tan, Copenhagen Business School, Denmark
Horst Treiblmaier, Modul University Vienna, Austria
Ozgur Turetken, Toronto Metropolitan University, Canada
Wietske van Osch, HEC Montreal, Canada
Weiquan Wang, Chinese University of Hong Kong, Hong Kong SAR
Dezhi Wu, University of South Carolina, USA
Fahri Yetim, FOM U. of Appl. Sci., Germany
Cheng Zhang, Fudan University, China
Meiyun Zuo, Renmin University, China

Managing Editor

Gregory D. Moody, University of Nevada Las Vegas, USA

SIG HCI