Data Cart: A Privacy Pattern for Personal Data Management in Organizations

Jan Tolsdorf and Luigi Lo Iacono

1 Introduction

The entry into force of the General Data Protection Regulation (GDPR) [29] in the European Union (EU) in 2016 has had a lingering impact worldwide on how individuals' personal data are processed. Essentially, entities that determine the purpose and/or process personal data are held more accountable than before for protecting the privacy of individuals. For instance, these entities are obligated to implement individuals' rights to transparency and intervention (Art. 12–21 GDPR), as well as to take measures for upholding the GDPR's principles for the privacy preserving and secure processing of personal data (Art. 5 GDPR). To reduce the risks of privacy violations and data breaches, the GDPR obligates these entities to implement Technical and Organizational Measures (TOMs) *"to ensure and to be able to demonstrate that [personal data] processing is performed in accordance with"* the GDPR (Art. 24 GDPR). For example, TOMs can include, but are not limited to, organizational measures such as risk assessments, implementation of a privacy policy, and awareness training for employees, as well as technical measures such as encryption and pseudonymization or tools to enforce the data protection policy. Among other things, this has caused organizations to (1) reorganize their business processes, (2) implement data protection management, (3) redesign their privacy policies, and (4) train their employees involved in personal data processing [76]. Failure to comply with the GDPR, such as not implementing the rights of individuals or insufficient protection of personal data, has already resulted in heavy fines for organizations [67]. Similar to the GDPR, other data protection laws around the world now also impose sanctions for these types of breaches, including

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

N. Gerber et al. (eds.), *Human Factors in Privacy Research*,
https://doi.org/10.1007/978-3-031-28643-8_18

the CPPA in California [75] and the APPI in Japan [57]. This development has also influenced academic discourse in the disciplines of Computer Science, Information Systems, and Human–Computer Interaction (HCI) for quite some time. In this context, related work on human factors in privacy has focused almost exclusively on the needs of individuals whose personal data are being processed, i.e., on the needs of data subjects. Among other things, these works include (1) examining the effectiveness and behavioral impact of transparency enhancing tools with respect to legal requirements [43, 52, 69, 81], (2) studying tools that provide data subjects with the ability to intervene and consent as required by law [27, 48, 80], (3) examining the compliance of transparency and intervention mechanisms with the GDPR's demand to provide information on personal data processing to data subjects *"in a concise, transparent, intelligible and easily accessible form, using clear and plain language"* (Art. 12) [42, 54, 79], (4) studying individuals' perceptions of their (new) rights introduced by the GDPR [3, 61], and (5) designing (new) transparency and intervention tools that comply with both legal and individuals' privacy requirements [9, 27, 53, 68, 81].

However, the current focus of research on human factors under contemporary data protection laws neglects the fact that privacy protection remains highly dependent on the privacy-compliant processing of personal data within organizations through the "correct" application and use of TOMs by employees responsible for personal data processing [12]. Following the notion of Human-Centered Design (HCD), the design of an organizations' internal TOMs must therefore account for the needs and capabilities of data processing employees. TOMs that are simply implemented without considering these factors are likely to be ineffective and even harmful to the organization. For example, previous work has found that data processing employees are not fully familiar with the essential terminology, concepts, and basic rules of the GDPR, which increases the risk of non-compliance [78]. In addition, TOMs may impose a burden on established business routines and increase the workload of data processing employees [36]. In this regard, industry reports indicate that up to 90% of all data breaches are caused by some form of human error [37]. Particular problems are both the accidental processing of data without permission and the forwarding of data to the wrong recipients. For example, this is reportedly true for 39% of incidents in the USA in 2019 [60] and for two-thirds of incidents in the Netherlands in 2020 [62]. Reasons include negligence of employees [66], high stress levels at work, and overladen communication channels (e.g., email) [11]. Half of the incidents resulted in disciplinary or other professional consequences for the employees [30]. The GDPR in particular has therefore increased the pressure on organizations and their data processing employees to comply with the regulation's strict rules.

The obvious solution is to provide data processing employees with TOMs that fulfill usability [28] criteria when it comes to the privacy compliant handling of personal data. However, stakeholders involved in the design and development of TOMs, e.g., employers and IT engineers, often face the challenge of translating complex legal, technical, and human requirements into concrete design and architectural decisions. In particular, the development from scratch and going through a

complete HCD process can be extremely resource intensive [49]. To speed up the development process of TOMs and keep it cost-efficient, it may be advisable to use privacy design strategies and privacy patterns. These represent existing and proven concepts for the implementation of TOMs. In this chapter, we introduce a privacy pattern for the implementation of TOMs for data processing employees.

The remainder of this chapter is structured as follows: Sect. 2 provides some overall background information relevant for the implementation of TOMs using privacy patterns. Section 3 then provides a brief outline of the HCD development process of our own privacy pattern, including the requirements elicited. Next, our privacy pattern is presented in Sect. 4, followed by insights gained in our evaluation in Sect. 5. We then conclude this chapter in Sect. 6 by summarizing our approach.

2 Background

This section provides background information on the implementation of TOMs using privacy patterns under the GDPR. Section 2.1 provides a brief overview of the key principles set out in the GDPR that must be adhered to when processing personal data and that TOMs should help comply with. Section 2.2 outlines the principles of the design philosophy Privacy by Design (PbD) to be considered when implementing TOMs. At last, Sect. 2.3 describes how privacy patterns can be leveraged to implement TOMs that comply with these principles.

2.1 GDPR Principles

Generally speaking, the implementation of TOMs is supposed to help entities who process personal data to comply with the GDPR's foundational principles put forward in Art. 5 of the regulation. In the following, we provide an overview of the different principles and briefly explain their implications for the development of TOMs aimed at assisting data processing employees in the privacy-compliant handling of personal data.

- *Lawfulness, fairness, and transparency* denote (1) that personal data processing must be based on a valid legal basis prior to processing, (2) that personal data are not processed in a manner that is unjustifiably harmful, unlawfully discriminatory, unexpected, or deceptive to data subjects, and (3) that personal data processing is transparent, open, and clear to data subjects. The design of TOMs should generally help ensure that the processing of personal data by data processing employees complies with these principles. For example, depending on the situation, TOMs should help data processing employees understand whether the processing of personal data is based on an organization's legitimate interests

or must be based on the data subject's consent. TOMs should also help inform data subjects about the nature and scope of the processing.

- *Purpose limitation* denotes that personal data may only be obtained for specific, explicit, and legitimate purposes. The data must not be processed in a way that is incompatible with the purposes for which they were obtained. TOMs should therefore ensure that data processing employees process personal data only for specified purposes to perform a specific job task.
- *Data minimization* refers to only processing personal data that are adequate, relevant, and limited to what is necessary for a given purpose. Thus, TOMs should facilitate limiting data collection to personal data that are necessary for a purpose associated with the job tasks of data processing employees.
- *Accuracy* indicates that the personal data processed are accurate and up to date and that reasonable efforts are made to erase or rectify inaccurate data in relation to a specific purpose. TOMs should therefore help data processing employees ensure that the personal data they process meet these characteristics.
- *Storage limitation* denotes that the processing of personal data does not allow identifying data subjects for longer than is required for the original purpose or to comply with legal obligations. TOMs should therefore delete personal data or make personal data inaccessible to data processing employees after a job task has been completed, and no legal regulations prescribe longer storage.
- *Integrity and confidentiality* require the implementation of appropriate technical and organizational safeguards to ensure personal data security, including safeguards against unauthorized or unlawful processing, accidental loss, destruction, or damage. Accordingly, TOMs should only grant access to personal data if data processing employees are authorized and the job task requires the personal data processing. TOMs should further support data processing employees in storing and processing personal data in a suitably protected manner.
- *Accountability* means that controllers, i.e., entities who define the purposes for personal data processing, ensure and are able to demonstrate compliance with the aforementioned principles. This generally requires controllers to ensure and be able to demonstrate that their data processing employees' actions comply with these principles. This may include providing privacy policies based on an inventory of processing records, documenting and tracking processing activities, and creating data protection awareness among data processing employees.

2.2 Privacy and Data Protection by Design

The GDPR requires that the implementation of TOMs takes into account the principles of *data protection by design and by default* (Art. 25 GDPR). These principles build upon the design philosophy of Privacy by Design (PbD) [16]. PbD advocates that *"privacy must be incorporated into networked data systems and technologies, by default. Privacy must become integral to organizational priorities,*

project objectives, design processes, and planning operations" [16]. PbD provides seven principles on how to integrate privacy [16]:

1. *Proactive not reactive; preventative not remedial*—all privacy policies and mechanisms must be in place prior to processing so that privacy issues can be resolved before they become real problems.
2. *Privacy as the default*—the default case guarantees integrity of privacy and provides fair processing of personal data. This includes, but is not limited to, purpose limitation, data minimization, transparency, and intervention capabilities.
3. *Privacy embedded into design*—privacy protection should not be considered an "add-on" but an integral part of information systems and business practices. It requires considering the broader context and all stakeholder views for finding the best solution.
4. *Full functionality*—PbD means promoting privacy as a complement, not a trade-off, and provides for innovative and creative solutions, which take into account all legitimate interests.
5. *End-to-end security*—privacy requires consideration of the entire processing chain, from collection to destruction of personal data ("cradle to grave").
6. *Visibility and transparency*—controllers should meet their accountability obligations by demonstrating compliance and providing truthful information about the processing.
7. *Respect for user privacy*—data protection should reflect the interests and needs of data subjects and requires user-oriented approaches in the design of tools, information systems, and business processes.

In 2010, the International Conference of Data Protection and Privacy Commissioners recognized PbD *"as an essential component of fundamental privacy protection"* and promoted its widespread adoption in legislation [63]. However, the translation of its principles into specific guidelines for action is a major practical problem [6, 24, 39, 73, 74]. PbD is frequently linked to Privacy Enhancing Technologies (PETs, see also the chapter "Acceptance Factors of Privacy-Enhancing Technologies on the Basis of Tor and JonDonym") because their development usually implicitly takes into account some PbD principles, in particular, *privacy by default* and *end-to-end security* [24]. However, PbD has always taken a holistic view and must be seen as a kind of lesson from the past, showing that implementing privacy by means of technology is only part of the answer toward more privacy, but not the answer itself [50]. That is, PETs should be understood as an integral part of PbD but must be accompanied by complementary measures that respect the privacy implications at the design stage of the technology.

Moreover, implementing PbD using a purely legally oriented process promotes the manifestation of one-size-fits-all solutions, which are detrimental to effective privacy protection because they disregard the nature of privacy, which is individualistic, contextual, diverse, and multifaceted [44, 51]. That said, PbD itself already takes this issue very much into account, promoting the principle of *respect for user privacy—keep it user-centric*. It essentially requires human factors of privacy to be incorporated in every IT system and business process [16, 17]. In

particular, it emphasizes on the need for privacy controls to be *"human-centered, user-centric, and user-friendly so that informed privacy decisions may be reliably exercised"* [16]. As such, there are increasing efforts to reinforce this principle in TOM development [32] and to expand the implementation of PbD to a human-centric process which accounts for this need [7, 31, 51, 71].

2.3 Privacy (Design) Patterns

Privacy patterns are design patterns used to translate the abstract principles of PbD and *data protection by design and by default* into practical advice for developing privacy-friendly systems and processes. In the following, we first briefly introduce the idea behind design patterns in general and then provide an overview of the use of privacy patterns in system design, business process design, and in HCI.

Design Patterns

Design patterns are proven solutions to known and recurring problems in a specific domain that are systematically recorded and documented [35]. The pattern approach was first developed and introduced in the field of urban and building architecture to document proven architectural designs in a standardized structure [2]. Later, the concept of design patterns became particularly popular in software engineering [35] and was eventually adapted to related fields, such as human–computer interaction [22] and cybersecurity [83]. Since the design of complex systems usually involves a wide range of recurring problems, engineers also usually need to draw on different design patterns to implement system requirements. To facilitate access to various design patterns, they are commonly organized in *pattern catalogs*. A pattern catalog represents a collection of design patterns that systematically classifies design patterns into different categories [14]. Its underlying systematization can be informal or based on formal pattern taxonomies. Pure pattern catalogs often consider patterns in isolation and ignore the fact that design patterns are frequently interdependent with other design patterns. For example, a design pattern may represent, among other things, an aggregation or specialization of other design patterns. Therefore, if a pattern catalog contains a sufficiently large number of design patterns, it may be useful to convert it into a *pattern system* capable of describing these dependencies [14]. Pattern systems, also known as *pattern languages*, describe dependencies between individual design patterns based on a predefined set of relationship types, as well as guidelines and rules for their implementation [15].

Privacy Pattern Collections

The concept of design patterns from software development was later extended to security [83] and privacy [65, 70]. Continuous efforts by the research community have resulted in a comprehensive collection of privacy patterns being available today, covering a multitude of topics including but not limited to anonymity [70] and pseudonymity [34], the development and application of privacy-enhancing technologies [40], as well as issues targeting human-computer interaction [25, 33, 38] with an emphasis on transparency [72]. The privacy patterns mainly support designers and developers in identifying privacy requirements for their system or process, provide suggestions for a suitable system architecture, or provide concrete design and implementation guidelines [47]. To this end, the pattern descriptions are often accompanied by conceptual representations, UML diagrams, sequence diagrams, and screenshots. Many of the privacy patterns available have further been documented in a repository that is maintained by a collaboration of international researchers.[1] The patterns have also been organized into catalogs targeting specific domains, such as the online context [4, 65] and the Internet of Things [55]. In addition, some catalogs categorized patterns according to the principles of the privacy framework in ISO/IEC 29100 with the aim of further simplifying the application of privacy patterns to comply with international standards and privacy laws [4, 26]. Meanwhile, there are first proposals for privacy pattern systems [19, 20, 40], as well as proposals for a suitable modeling language to concisely describe dependencies between privacy patterns [15].

Privacy Design Strategies and Tactics

Privacy design strategies allow a mapping between legal requirements and system requirements and are suitable for specifying clear objectives related to PbD in order to achieve a certain level of privacy protection [21]. For better distinction and labeling, privacy patterns are often classified according to eight privacy design strategies [41]: (1) *Minimize* the amount of personal data that are processed (2) *Hide* personal data and their interrelationships from plain view (3) *Separate* the processing of personal data into compartments (4) *Aggregate* personal data to the highest level and with the least possible detail (5) *Inform* data subjects about personal data processing (6) *Control* over personal data processing by data subjects (7) *Enforce* privacy policies compatible with legal requirements (8) *Demonstrate* compliance with privacy policies and legal requirements

A recent literature survey revealed that about half of the privacy patterns published in peer-reviewed articles focus on the strategies *hide* and *separate*, which are usually strongly characterized by the use of TOMs [47]. In addition, various tactics are available for implementing each data protection strategy. A tactic

[1] https://privacypatterns.org/

represents a homogeneous set of privacy patterns and summarizes their underlying main concept [21]. Tactics provide a useful intermediate level of abstraction for modeling systems and processes because they are more fine-grained than privacy strategies, but more abstract than privacy patterns.

Patterns for Business Processes and Workflows

Akin to design patterns for system design and architecture, there also exist patterns for modeling business processes to include obligations imposed by privacy laws [1, 5, 8, 13, 18, 64]. Patterns in this category support organizations in modeling their high-level architecture and business processes while incorporating PbD. Some approaches employ enterprise architecture model description languages to make the interdependence of systems and the associated data flows transparent and understandable [18]. This also allows determining which components must be added or implemented in order to comply with privacy principles or regulatory requirements [10]. Other approaches employ description languages for business process models to incorporate privacy principles and regulatory-mandated organizational measures into business processes by default [1, 5, 8, 13, 64].

However, the scope covered by the approaches varies; some works focus on patterns covering the standard cases of data protection law, in particular those of the GDPR. Cases covered include controllers' obligations and data subjects' rights [1, 18, 64]. They may be used as templates by organizations and architects to avoid having to model standard processes themselves. Second, there are methodologies available for modeling legal requirements and creating patterns using standard modeling languages [8, 13, 64]. They support organizations and architects in documenting their own patterns and processes in a comprehensible and consistent manner. Third, some works present more specific patterns for business processes in certain contexts that help to reduce the level of abstraction of the former two approaches [5].

Usable Privacy and Interaction Patterns

Privacy patterns focus not only on technical and architectural aspects but also on usability aspects, i.e., designing privacy protection in a human-centered manner to make it efficient, effective, and satisfying for the respective user group. To this end, numerous so-called *HCI (privacy) patterns* have been proposed to provide usable interfaces for PETs [33, 38]. In particular, several patterns have been proposed under the design strategy *inform*, which are commonly referred to as privacy transparency patterns and are suitable for implementing data subjects' information rights [33, 72].

Independent of the topic of privacy, design patterns that define problems and solutions targeting the perceived interaction behavior are generally referred to as *interaction design patterns* [22]. The term emerged in the HCI community to clearly distinguish design patterns with a focus on interaction behavior from design patterns

for the realization of interfaces in software engineering. Interaction design patterns are usually the result of a HCD process in which the pattern was developed and evaluated together with the affected stakeholders [33, 56].

3 Privacy Pattern Development

In this section, we outline the development process of our privacy pattern *Data Cart*. Generally speaking, stakeholders involved in the design and development process of tools that adhere to PbD need a deep understanding of (1) the situation and context *in which* the tools will be used, as well as (2) the personal data processing activities *for which* the tools will be used [58]. To incorporate these aspects early in the design process for a privacy pattern for data processing employees that supports them in the data protection compliant handling of personal data, we applied a User-Centered Design (UCD) approach (see the chapter "Achieving Usable Security and Privacy Through Human-Centered Design") with data processing employees from two public institutions in Germany. In the following, we first provide a brief overview of the UCD study in Sect. 3.1. Then, in Sect. 3.2, we outline the main requirements identified for tools to support our stakeholders in managing personal data in a privacy-compliant manner. The detailed study procedure, elicited requirements, and development process are available elsewhere [77].

3.1 User-Centered Design Study

A total of 19 data processing employees participated in our UCD study. A summary of their demographics is available in Table 1. Overall, our sample was highly educated, as all participants held a university degree. At the time of participation, they had been in their job and with the organization for between 1 and 19 years (median = 3 years and mean = 5.4 years). In most cases, our participants held multiple job roles, including research officer, third-party funding officer, legal officer, team assistant, network manager, and innovation manager. Their tasks included consulting and coaching activities, guiding and supporting grant applications or patent approvals, and monitoring ongoing projects or start-ups. In these activities, they primarily processed personal data of employees of the organization. The data typically included personnel data, contact data, and demographic data. In addition, our participants often processed classified information (e.g., patents). Other tasks include public relations and marketing as well as networking, which includes the regular planning and hosting of events. These activities require extensive processing of private and professional contact data, as well as image recordings. In all of these activities, participants regularly cooperated and communicated with their colleagues and other departments or with external organizations such as project sponsors and funding agencies. Particularly often, our participants were in contact with the HR

Table 1 Participant demographics

ID	Sex[S]	Age (years)	Education (highest)	Job description (primary)	Job tenure (years)
P01	f	35–44	PhD	Research Funding Officer	6–10
P02	f	35–44	PhD	Research Promotion Officer	1–5
P03	m	25–34	PhD	Research Officer	1–5
P04	f	45–55	Master's degree	Research Officer	1–5
P05	f	45–55	Master's degree	Research Officer	1–5
P06	f	45–55	Master's degree	Research Officer	6–10
P07	f	35–44	Master's degree	Research Officer	1–5
P08	f	35–44	Master's degree	Network Manager	16–20
P09	m	25–34	Master's degree	Innovation Manager	1–5
P10	f	55–65	State exam	Research Officer	16–20
P11	f	35–44	State exam	Legal Officer	1–5
P12	f	25–34	Master's degree	Third-Party Funding Coordinator	1–5
P13	f	35–44	Master's degree	Research Officer	6–10
P14	f	35–44	PhD	Research Officer	1–5
P15	f	35–44	State exam	Third-party Funding Coordinator	1–5
P16	f	45–55	Master's degree	Research Officer	1–5
P17	f	45–55	Master's degree	Research Officer	6–10
P18	f	35–44	PhD	Research Officer	6–10
P19	f	45–55	Bachelor's degree	Team Assistant	6–10

Note. [S]Options were diverse, female, male, prefer not to say

Department to request personal data instead of obtaining them directly from the data subjects. In most cases, their tasks require sharing (personal) data with others or using the data to generate statistics and reports. Thirteen participants self-reported processing personal data very frequently or regularly, while six participants reported processing such data occasionally.

The UCD study consisted of a series of eight workshops to investigate the data processing employees' needs for assistance in handling personal data and to evaluate potential solutions. An overview of the full development process is given in Fig. 1. In the first workshop, we adopted a concept of Polst et al. [59] in order to familiarize ourselves with the stakeholder group and their everyday work. In the subsequent workshops, we elicited common problems that our participants encountered when processing personal data. We explicitly addressed data protection concerns and asked as to how they envision a redesign of the processes to improve privacy. Based on the obtained feedback, we developed a concept and refined it in several sessions with UX designers and usable privacy and security experts. We then evaluated the concept using pen and paper mockups to conduct a pluralistic walkthrough [82] with our participants. From the results, we compiled a list of final requirements and drafted a prototype. The prototype was implemented as a web application. It included several scenarios of our participants' everyday work. We ran formative usability tests to evaluate the prototype's usability and privacy-enhancing properties.

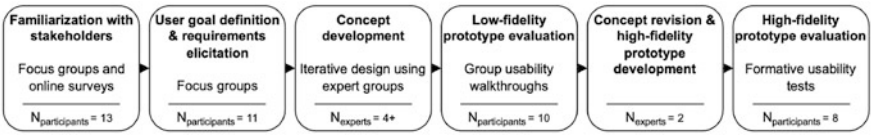

Fig. 1 Summary of the development process of *Data Cart*. Note that due to busy schedules of our participants and staff turnover in the departments, not all participants participated in all steps of the UCD study ($N_{\text{participants total}} = 19$)

We also discussed the extent to which the tool would change established work processes and the handling of personal data with our participants.

For the most part, we relied on focus groups because we expected our participants to enrich each other [45], but we also used interviews because both methods are well suited for both requirements elicitation and evaluation [46]. We either adapted existing workshop concepts to our needs or created our own study protocol in accordance with established guidelines. All study protocols were designed and reviewed by two subject-matter experts, as well as researchers from a larger research project team, and researchers with experience conducting user studies. Depending on the type of study, we piloted studies with members of our own institutions or other organizations.

3.2 Data Processing Employee Requirements

Participants identified numerous problems and opportunities to improve workflows and strengthen data protection within them. Major concerns were the inconsistent processes and decentralized infrastructure across different departments. This greatly affects the gathering of personal data and the handling of outdated data. Participants complained that much of their time was spent communicating with other departments, such as HR, or with the data subjects themselves when they needed data. Employees rated clearly identifiable responsibilities and fast, as well as complete, responses to their inquiries as essential factors for their job tasks, as they are often subject to tight deadlines.

Moreover, participants were well aware of their responsibility in dealing with personal and classified data. They assured that they strived to act to the best of their knowledge but expressed their uncertainties in practice. In particular, they felt insecure due to a lack of knowledge about data protection rules that apply to certain situations and data. They desired tools to keep them from committing unlawful actions and demanded clear instructions without any room for interpretation. Besides, participants showed concern about the lack of transparency of their processing activities to data subjects and were also unaware whether and how data subjects would have consented. Consequently, they asked to make the extent of processing and data flow transparent to data subjects.

4 The *Data Cart* Privacy Pattern

A key requirement of data processing employees is the timely and effective access to personal data that are usually not under their control. Therefore, a primary task is to assemble a set of different and varying personal data and data subjects from external sources that are needed for a particular business process. This may require initiating multiple data queries, keeping track of them, and processing the responses. Similar complexity in the compilation and tracking of different items and attributes is a well-known problem in online shopping. This is why we adapted the shopping cart[2] interaction pattern to our context and created the metaphor of a "data cart." The metaphor builds on data processing employees' existing knowledge of interaction concepts for complex processes where one first defines an output based on metadata, considers different statuses (e.g., availability), and only gains access after completing different tasks (e.g., payment, delivery). For this purpose, the steps necessary to model the processing of personal data in administrative tasks have been roughly mapped to an online shopping cart. The data cart metaphor serves two purposes. First, we used the metaphor in the context of our internal design and development cycle, as well as in internal communication within the research team. This allowed for a common understanding of the interaction concept among all researchers. Second, we also used the metaphor to break down the complexity of data protection for our participants and integrate privacy requirements into meaningful workflows that align with their needs.

Based on the data cart metaphor and taking into account legal concerns and stakeholder requirements, we developed an employee-centric solution that provides sufficient flexibility to meet various use cases of our stakeholders related to the processing of personal data. The solution basically provides for synchronizing the recurring tasks of retrieving and managing personal data with privacy obligations. The result is a harmonized combination of process flow and interaction concept, which we have documented as a privacy pattern. In the remainder of this section, we provide a basic description of the pattern following established templates [19].

Name Data Cart

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

Context This pattern applies to data processing employees working in organizations that elicit personal data as a part of an overarching business process and must share the personal data with other entities or departments as part of this business process. Elicitation is usually done in structured surveys through forms or by requesting the personal data from other departments within the organization. The pattern has been evaluated with data processing employees from public institutions who mainly process employee personal data for purposes such as academic services,

[2] https://web.archive.org/web/20211124013206/http://welie.com/patterns/showPattern.php?patternID=shopping-cart

consulting, and patent registration and exploitation. The personal data processed generally included information on contact, education, finances, professional activity, as well as pictures and personal identifiers.

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

Solution Provide a privacy enhancing personal data management interface to personal data that (1) streamlines data collection processes in organizations and aligns them with data protection requirements, (2) standardizes access to personal data for data processing employees, (3) simplifies access to privacy policies for data processing employees, and (4) supports both controllers and data processing employees in demonstrating transparency and compliance by documenting processing activities.

GDPR Principles *Lawfulness*, *fairness*, and *purpose limitation* are addressed by reducing human error due to ignorance, since information about the legal basis and purpose become an integral part of any request for personal data; *data minimization* and *accuracy* are achieved through (1) centrally controlled access to personal data, (2) provision of meta-information about data, and (3) triggering of updates, and *storage limitation* and *integrity and confidentiality* are supported by incorporating *privacy by default* (e.g., encryption of exports) and data handling information. *Fairness*, *transparency*, and *accountability* are supported by the implicit documenting of requests. *Accountability* is further addressed by making data processing employees aware of personal data processing obligations through clear and uniform privacy notices.

Privacy Design Strategies [41]
Primary:

- *Enforce* privacy policies compatible with legal requirements
- *Demonstrate* compliance with privacy policies and legal requirements

Supports:

- *Minimize* the amount of personal data that are processed
- *Inform* data subjects about personal data processing
- *Control* over personal data processing by data subjects

4.1 Process Flow Model

In this section, we describe the process flow associated with the *Data Cart* solution outlined above. It shall serve IT architects, developers, and process managers as a means to understand and integrate the *Data Cart* pattern into their own systems and processes, respectively. The process flow divides into tasks to define a personal data processing activity, process personal data, and demonstrate compliance. The basic flow is outlined in Fig. 2 and divides into eight tasks. A detailed process flow diagram is shown in Fig. 3. The process flow starts by assuming that a data processing employee has a demand to process personal data and opens the *Data Cart* interface. The process flow is as follows:

1. The first process step requires data processing employees to model a data processing activity to be performed. For this purpose, they must choose a processing activity from the organization's records of processing activities for which they are authorized. According to Art. 30 GDPR, this directory must be maintained by all data controllers with regular processing activities and contains a list of all legitimate personal data processing activities. Each entry comprises a purpose, categories of personal data, categories of data subjects, categories of recipients, legal basis, and, if applicable, further information on technical and organizational measures. Upon selection, employees are provided with a summary of the processing record. This requires employees to become aware of the legal basis before processing begins. In the event that the personal data have already been collected via form, this can also be imported instead. In such a case, the appropriate processing record entry can be selected automatically.
2. In the second process step, data processing employees define tuples of required categories of personal data and data subjects. They may also add additional details, such as specific recipients, the version of personal data they require, or a personal message to the data source (e.g., data subject, department). Once

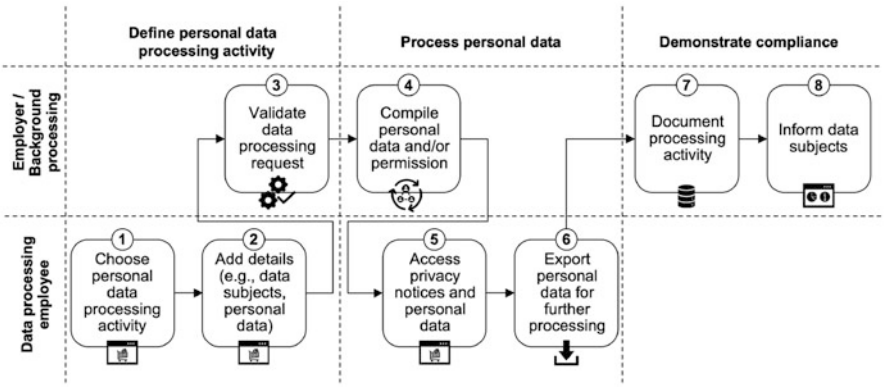

Fig. 2 Flow of the concept developed using the metaphor of a data cart

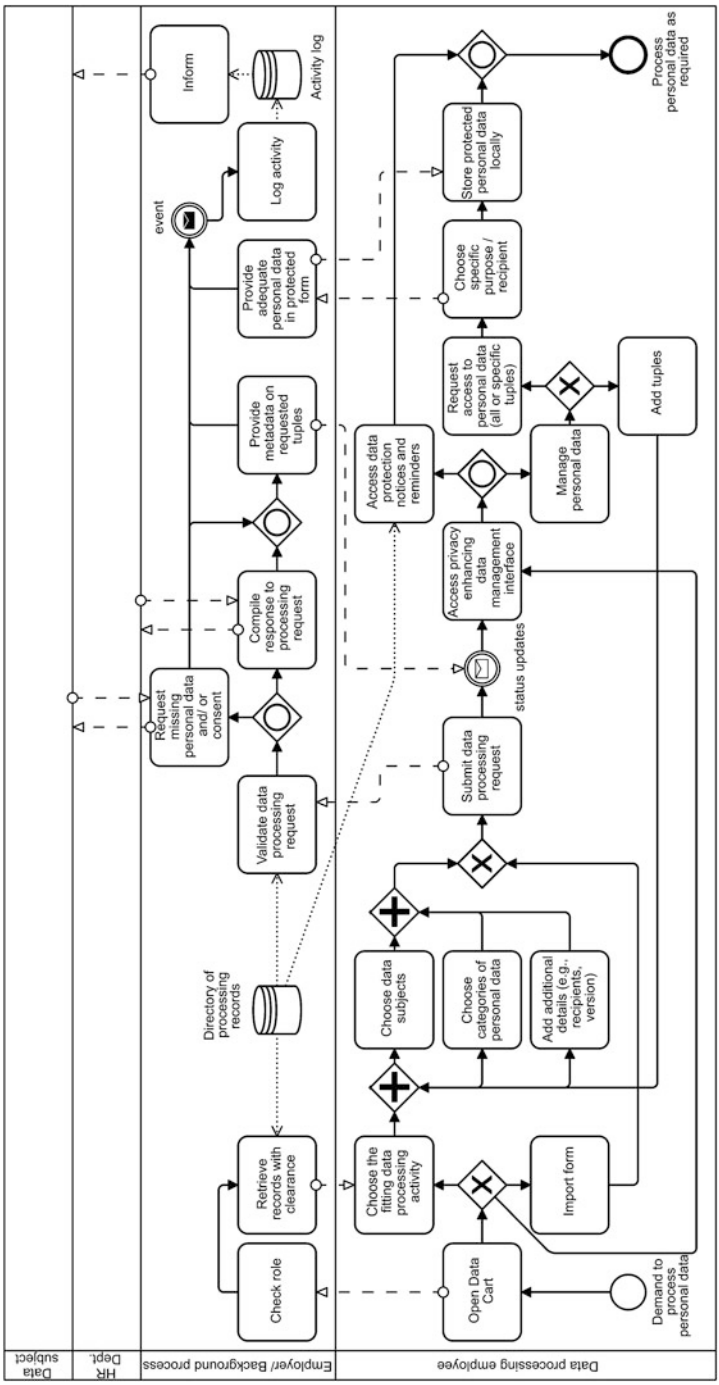

Fig. 3 Process flow diagram of the concept developed using the metaphor of a data cart

finished, the modeled processing activity is to be submitted as a new data processing request.
3. The submitted processing request must then be validated by verifying for lawfulness of processing against the processing policies extracted from the record of processing activities and by checking the availability and timeliness of the personal data requested.
4. The next process step comprises obtaining missing personal data and permissions. Depending on the processing activity, this may require initiating requests to the respective data subjects or departments to provide the missing data and approvals. It is critical from our stakeholders' point of view that the request be structured and that input validation is performed. Requests must also include detailed information about the requester and their legitimacy, as well as procedural and legal aspects of the underlying processing. Our own pattern does not specify how such a request should be designed, but privacy patterns similar to *informed consent* may be used here [33].
5. After all tasks have been completed, data processing employees get access to a privacy enhancing personal data management interface. It provides access to metadata of the data processing request, including status information and details about the tuples requested. In addition, it provides access to contextual privacy policies and reminders extracted from the organizations' directory of processing records. Furthermore, the interface provides the ability to request additional combinations of personal data and data subjects and to request access to the personal data (e.g., exports).
6. To access raw personal data, data processing employees must choose a specific purpose for which they require the data. Based on this, they should be provided with an export of the personal data, which contains only the data authorized for the purpose and recipients. The export should be adequately protected by default, as our stakeholders do not have the necessary knowledge to do this themselves. All exports should further contain a copy of the data protection information provided in the data management interface, as well as an ID to ensure traceability of the exported file to the original request. The exported personal data then shall be further processed by data processing employees as required. Based on stakeholder feedback, we recommend using common data exchange formats (e.g., MS Excel).
7. All actions, including requests for data and data exports, are logged to document all personal data processing activities. After completing a processing activity, requests can be archived and serve as evidence for later audits and traceability. In addition, the activity log may be used to create a usage history for data processing employees.
8. Furthermore, the here described concept advocates transparency and conceptually provides that data subjects are informed about the processing carried out on the basis of the activity log. This is not covered by our own pattern. Instead, depending on the needs, existing tools and components optimized for employees in their role as data subjects may be used for this purpose [23, 68].

4.2 Interaction Concept

Based on the process flow outlined above, we developed a corresponding user interaction concept that reflects our stakeholders' point of view. The interaction concept including a mapping to the requirements elicited is shown in Fig. 4. The interaction concept is divided into five parts.

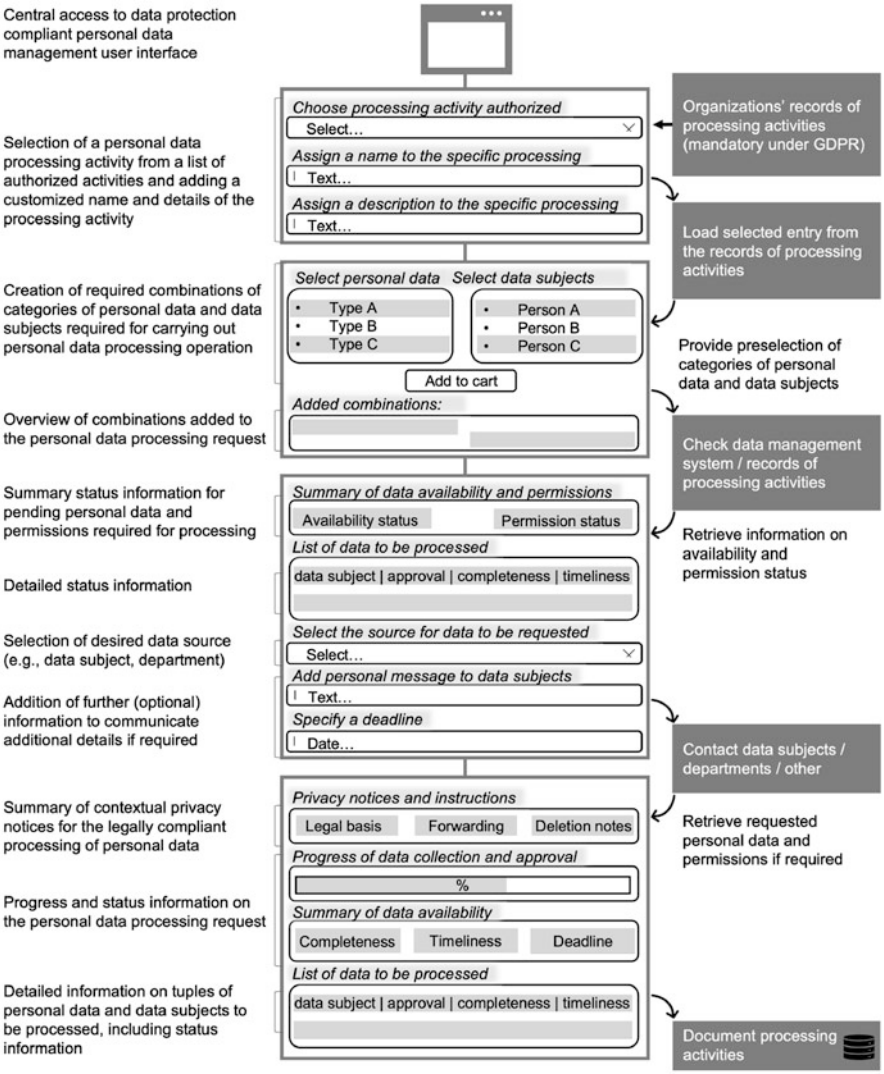

Fig. 4 Basic interaction concept designed following the data cart metaphor

1. First, data processing employees should be offered a personal data management tool that provides for centralized access to personal data and enforces consistency of the full data management process.
2. To model a data processing request, data processing employees should be provided with a preloaded list of processing activities for which they are authorized. Upon selection, employees should be provided with a summary of the processing record. In addition, the planned processing must be given a name and a description. These steps require employees to become aware of the legal basis before processing begins. At the same time, the interaction concept provides for contextual support, such as providing templates and contextual information. Templates may be based on previous requests, too.
3. To define tuples of personal data and data subjects, data processing employees should be provided with predefined lists. For personal data, these lists may be derived from the selected processing record entry and should be offered as a pre-selection. Likewise, data subjects should be accessible from a list of employees in the organization. The interface should further support the iterative adding of multiple different combinations.
4. When submitting the request for validation, the results should be provided for review in an overview. It should include status information on whether the processing activity can start immediately after submission of the processing request or whether additional actions are required, such as collecting personal data or obtaining consent. Detailed status information should be accessible as needed.

   At this point, further information may be added to the request. Employees may choose whether to request the data directly from the data subjects, via an administrative department, or in a customized manner. They may also compose individual messages to the data subjects and set a deadline for responding to the request.
5. The privacy enhancing data management interface should provide detailed information on the status of pending requests. In addition, it provides frequently needed or important information on data protection tailored to its users' needs. This includes information on allowed processing operations, whether processing has been approved, to whom data may be disclosed, deletion periods, data sensitivity, and how data must be safeguarded. In general, the interface aims to provide such notices at a glance, with details accessible when necessary. Additional visualizations and a help section for questions accompany detail views.

5 *Data Cart* Evaluation Results

In this section, we report on results obtained in the UCD study by evaluating our *Data Cart* mock-ups. We report on our participants' perceptions and understanding of the "data cart" metaphor in Sect. 5.1. We then present our participants' feedback

on *Data Cart*'s properties for data protection in Sect. 5.2, followed by limitations and open issues in Sect. 5.3.

5.1 Metaphor and Concept Understanding

Overall, we found that the data cart metaphor was helpful in outlining the basic assumptions and processes of the *Data Cart* concept to data processing employees. In particular, we found that the data cart metaphor supports data processing employees in understanding that a personal data processing operation always requires the definition of a tuple consisting of one or multiple purposes, data subjects, and data categories, but without the need to understand the details of the GDPR. In this context, the data cart metaphor was useful to explain the basics of a directory of processing activities, since we found that data processing employees in our UCD study were generally unfamiliar with this concept and its meaning. Only one participant indicated that they knew their organization maintained such a directory.

5.2 *Data Protection Properties of* Data Cart

In total, we identified five themes on data protection in our participants' feedback on *Data Cart*. The themes are summarized in Table 2.

Desire for Systematic Data Protection by Design In general, the *Data Cart* concept encouraged our participants to discuss their need for systematic data protection that integrates with work processes, rather than always being added as an additional expense and interfering with work. Participants pointed out that the correct handling of personal data *"is too often overlooked in everyday life, and the use of a such a tool would, on the one hand, simplify this and, on the other hand, somehow make you aware of the relevance of data protection and data"* (P06). Furthermore, our participants praised the PbD approach taken by *Data Cart*, because *"[personal data] would be handled in a more sensitive way without making it [(data protection)] too much of an issue"* (P04). In addition, the approach to systematic data protection in the form of *Data Cart "creates legal certainty and can somehow take away uncertainty"* (P05) when dealing with personal data: *"Well, basically, because everything is already predefined [. . .] I think you feel a bit safer, because you can make fewer mistakes yourself, because it is automated or because hints are given"* (P03) and *"because I don't have to worry at all about whether the person consents or not, because it is all there"* (P03).

Central Source of Information for Data Protection Our participants positioned *Data Cart* as a central information platform for data protection topics, which *"compiles the information quite well, so you don't have to go through the hassle of*

Table 2 Summary of participant feedback related to data protection properties of *Data Cart*

Theme	Description
Desire for systematic data protection	▹ Establishing data protection by design ▹ Enabling efficient, effortless, and secure handling of personal data
Central source of information for data protection	▹ Eliminating non-uniform handling of data protection rules by providing clear and understandable instructions on data protection ▹ Keeping data privacy information available and allowing quick access to "important" information
Raising awareness of data protection	▹ Sensitizing data processing employees for data protection ▹ Allowing sensitization of data subjects ▹ Correcting and aligning interindividual understanding of "sensitive data"
Integration limits as a barrier for data protection	▹ Transitions between processes and systems are critical for data protection compliance ▹ Processing of data remains unaffected without adaptation of processes
Consequences of systematic data protection as an obstacle to work	▹ Conflicting with established work practices and procedures

finding out how to proceed with it [(personal data)]" (P03). Particularly important was quick access to important information, i.e., that one can *"immediately see which data I'm allowed to pass on externally or internally, I think that's pretty good"* (P05) *"because you're simply dealing with sensitive data, and you don't always know whether you're allowed to [process data] or not"* (P01).

Raising Awareness of Data Protection *Data Cart* is seen as a driver of awareness for both data processing employees and data subjects. Our participants particularly welcomed the sensitization for legally compliant data processing: *"Otherwise, you are just less aware of it, so I think it makes you more aware that these are all very important data and that they must also be specially protected"* (P04). Here, too, PbD played a role: *"Because otherwise it's like this in the everyday handling of data: I don't even think about what people have approved, what they haven't approved"* (P08), but *"just by having this tool at your disposal, you're more likely to even think about 'do I need to pay attention to anything right now?'."* At the same time, documentation and communication through *Data Cart* allows data processing employees to fulfill their desire to inform data subjects: *"I find this tool quite good for that. That I can then write to [those] whose data I process [. . .] and make them aware that their data are being processed and whether they agree to it at all"* (P06).

Integration Limits as a Barrier for Data Protection Our participants noted that tools like *Data Cart* cannot solve all privacy issues. Especially if tools are introduced as a supplement to existing processes or current workflows, *"because*

then the data are accessible again: I have to archive them for later auditing [...] and then, of course, these sensitive data are stored there. That's a place where everyone has access" (P04). Further problems arise from the lack of digitalization, since requests for project proposals are often made via traditional means of communication not under control of *Data Cart*, yet they may already contain critical data: *"But I wonder what happens when you simply receive data. So just in everyday work, one simply gets some kind of data by email"* (P15).

Consequences of Systematic Data Protection as an Obstacle to Work It becomes clear that the handling of personal data enforced by *Data Cart* creates new obstacles: *"Because if we use this here, we make the request, it gets approved, so the data have to be checked first [...] At that moment, we can't continue at that point. And that delays some workflows"* (P01). In particular, lack of or denial of approval is perceived as the biggest obstacle: *"If someone's data are not approved, then I can't continue processing. Of course, we don't have this situation now because no one knows that the data are being used"* (P06).

5.3 Limitations and Open Issues

Based on our analysis of *Data Cart*, we identified several further topics and issues related to TOMs like *Data Cart* from the perspective of data processing employees [77]. For example, there are possible integration barriers, especially if tools are introduced as a supplement to existing processes or current workflows. Further problems may arise from a lack of digitalization in organizations, which could cause a significant overhead in both the integration and operation. Further issues may result from the consequences of systematic data protection, as it enforces a specific way of working that might need additional change management efforts. These potential issues should definitely be considered when implementing tools based on *Data Cart* and will require further investigation in the future.

6 Conclusion

Data processing employees have always played an important role in putting privacy goals into practice. To assist them in the privacy-compliant handling of personal data, TOMs must be designed to align with their needs and capabilities. To this end, this chapter introduced and presented the privacy pattern *Data Cart*, consisting of a process flow model and interaction concept. *Data Cart* offers a practical solution to stakeholders involved in privacy research or engineering for the human-centered design of TOMs under the GDPR. It (1) streamlines data management processes and brings them in line with data protection requirements, (2) standardizes access to personal data, (3) facilitates employee access to privacy policies, and (4) enables

documentation of personal data processing. In general, we found that *Data Cart* addresses data processing employees' desire for systematic data protection, i.e., data protection that integrates with work processes, rather than always being added as an additional expense and interfering with work. In this context, a PbD approach seems to be valued for implicitly enforcing data protection in the handling of personal data by designing the entire process from the perspective of data processing employees. By mapping the organization's requirements directly into the process and interface design, data processing employees benefit by focusing more on the essential process and being less exposed to uncertainty when processing personal data. In our UCD study, data processing employees perceived *Data Cart* as a relief because it reduces the manual compliance effort on their end. *Data Cart* may be adapted in the future to meet participants' demands for more comprehensive solutions and become an integral part of standard software or its own class of standard software for privacy management used in organizations.

Acknowledgments This chapter is derived in part from an article published in Behaviour & Technology 2022 ©Taylor & Francis, available online: https://www.tandfonline.com/10.1080/0144929X.2022.2069596. This research was supported by the German Federal Ministry of Education and Research (BMBF) under the contract numbers 16KIS0899 and 16KIS1508.

References

1. Agostinelli, S., Maggi, F. M., Marrella, A., & Sapio, F. (2019). Achieving GDPR compliance of BPMN process models. In *Proceedings of the CAiSE Forum as part of the 31st International Conference on Advanced Information Systems Engineering (CAiSE Forum)* (pp. 10–22).
2. Alexander, C., Ishikawa, S., Silverstein, M., Jacobson, M., Fiksdahl-King, I., & Shlomo, A. (1977). *A pattern language: Towns, buildings, construction*. OUP.
3. Alizadeh, F., Jakobi, T., Boden, A., Stevens, G., & Boldt, J. (2020). GDPR reality check—claiming and investigating personally identifiable data from companies. In *Proceedings of the IEEE European Symposium on Security and Privacy Workshops (EuroSPW)* (pp. 120–129).
4. Aljohani, M., Blustein, J., & Hawkey, K. (2018). Toward applying online privacy patterns based on the design problem: A systematic review. In *Proceedings of the 7th International Conference on Design, User Experience, and Usability (DUXU)* (pp. 608–627).
5. Aljohani, M., Hawkey, K., & Blustein, J. (2016). Proposed privacy patterns for privacy preserving healthcare systems in Accord with Nova Scotia's personal health information act. In *Proceedings of the 4th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)* (pp. 91–102).
6. Alshammari, M., & Simpson, A. (2017). Towards a principled approach for engineering privacy by design. In *Proceedings of the 5th Annual Privacy Forum (APF)* (pp. 161–177).
7. Ayalon, O., & Toch, E. (2021). User-centered privacy-by-design: Evaluating the appropriateness of design prototypes. *International Journal of Human-Computer Studies, 154*, 102641.
8. Barati, M., & Rana, O. (2021). Design and verification of privacy patterns for business process models. In S. Patnaik, T.-S. Wang, T. Shen, & S. K. Panigrahi (Eds.), *Blockchain technology and innovations in business processes* (pp. 125–139). Springer.
9. Bier, C., Kühne, K., & Beyerer, J. (2016). PrivacyInsight: The next generation privacy dashboard. In *Proceedings of the 4th Annual Privacy Forum (APF)* (pp. 135–152).
10. Blanco-Lainé, G., Sottet, J.-S., & Dupuy-Chessa, S. (2019). Using an enterprise architecture model for GDPR compliance principles. In *Proceedings of the 12th IFIP Working Conference on the Practice of Enterprise Modeling (PoEM)* (pp. 199–214).

11. Brackenbury, J., & Bailey, R. (2020). 2020 Outbound Email Security Report | Egress. https://www.egress.com/newsroom/2020-outbound-email-security-report
12. Brodie, C., Karat, C.-M., Karat, J., & Feng, J. (2005). Usable security and privacy: A case study of developing privacy management tools. In *Proceedings of the 1st Symposium on Usable Privacy and Security (SOUPS)* (pp. 35–43).
13. Buchmann, E., & Anke, J. (2017). Privacy patterns in business processes. In *Proceedings of the 47th Jahrestagung der Gesellschaft für Informatik (INFORMATIK)* (pp. 793–798).
14. Buschmann, F., Meunier, R., Rohnert, H., Sommerlad, P., & Stal, M. (1996). *Pattern-oriented software architecture—a system of patterns* (Vol. 1). Wiley.
15. Caiza, J. C., Martín, Y.-S., Del Alamo, J. M., & Guamán, D. S. (2017). Organizing design patterns for privacy: A taxonomy of types of relationships. In *Proceedings of the 22nd European Conference on Pattern Languages of Programs (EuroPLoP)* (pp. 1–11).
16. Cavoukian, A. (2011). *Privacy by design the 7 foundational principles implementation and mapping of fair information practices*. Brochure, Information and Privacy Commissioner of Ontario Canada.
17. Cavoukian, A., Shapiro, S., & Cronk, R. J. (2014). Privacy engineering: Proactively embedding privacy by design. White paper, Information and Privacy Commissioner of Ontario Canada.
18. Coelho, M. D., Vasconcelos, A., & Sousa, P. (2021). Privacy by design enterprise architecture patterns. In *Proceedings of the 23rd International Conference on Enterprise Information Systems (ICEIS)* (pp. 743–750).
19. Colesky, M., & Caiza, J. C. (2018). A system of privacy patterns for informing users: Creating a pattern system. In *Proceedings of the 23rd European Conference on Pattern Languages of Programs (EuroPLoP)* (pp. 1–11).
20. Colesky, M., Caiza, J. C., Del Álamo, J. M., Hoepman, J.-H., & Martín, Y.-S. (2018). A system of privacy patterns for user control. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing (SAC)* (pp. 1150–1156).
21. Colesky, M., Hoepman, J.-H., & Hillen, C. (2016). A critical analysis of privacy design strategies. In *Proceedings of the IEEE Security and Privacy Workshops (SPW)* (pp. 33–40).
22. Dearden, A., & Finlay, J. (2006). Pattern languages in HCI: A critical review. *Human–Computer Interaction, 21*(1), 49–102.
23. Dehling, F., Feth, D., Polst, S., Steffes, B., & Tolsdorf, J. (2021). Components and architecture for the implementation of technology-driven employee data protection. In *Proceedings of the 18th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)* (Vol. 12927, pp. 99–111).
24. Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Métayer, D., Tirtea, R., Schiffner, S., Danezis, G., European Union, & European Network and Information Security Agency. (2014). Privacy and Data Protection by Design - from Policy to Engineering. Report, European Union Agency for Cybersecurity (ENISA).
25. Doty, N., & Gupta, M. (2013). privacy design patterns and anti-patterns—patterns misapplied and unintended consequences. In *Proceedings of the 1st Trustbusters for User Interfaces Workshop* (pp. 1–5).
26. Drozd, O. (2016). Privacy pattern catalogue: A tool for integrating privacy principles of ISO/IEC 29100 into the software development process. In *Proceedings of the 10th IFIP International Summer School on Privacy and Identity Management* (pp. 129–140).
27. Drozd, O., & Kirrane, S. (2020). Privacy CURE: Consent comprehension made easy. In *Proceedings of the 35th IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)*.
28. EN ISO 9241-11:2018. Ergonomics of Human-System Interaction Part 11: Usability: Definitions and Concepts. International Standards. International Organization for Standardization.
29. European Union. (2016). General Data Protection Regulation. Regulation (EU) 2016/679.
30. Evdokimov, A., Reva, A., & Maris, K. (2020). Taking care of corporate security and employee privacy. Survey, AO Kaspersky Lab.
31. Feth, D., Maier, A., & Polst, S. (2017). A user-centered model for usable security and privacy. In *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)* (pp. 74–89).

32. Fischer-Hübner, S., & Berthold, S. (2017). Privacy-enhancing technologies. In *Computer and Information Security Handbook* (pp. 759–778). Elsevier.
33. Fischer-Hübner, S., Köffel, C., Pettersson, J. S., Wolkerstorfer, P., Graf, C., Holtz, L. E., König, U., Hedbom, H., & Kellermann, B. (2010). HCI pattern collection—version 2. Deliverable D4.1.3, PrimeLife.
34. Gabel, A., & Schiering, I. (2019). Privacy patterns for pseudonymity. In *Proceedings of the 13th IFIP International Summer School on Privacy and Identity Management* (pp. 155–172).
35. Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1995). *Design patterns: Elements of reusable object-oriented software*. Addison-Wesley.
36. Gan, M. F., Chua, H. N., & Wong, S. F. (2019). Privacy enhancing technologies implementation: An Investigation of its impact on work processes and employee perception. *Telematics and Informatics, 38*, 13–29.
37. Goodman, S. (2020). Human Error to Blame for 9 in 10 UK Cyber Data Breaches in 2019. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/
38. Graf, C., Wolkerstorfer, P., Geven, A., & Tscheligi, M. (2010). A pattern collection for privacy enhancing technology. In *Proceedings of the 2nd International Conferences on Pervasive Patterns and Applications (PATTERNS)* (pp. 21–16).
39. Gürses, S., Troncoso, C., & Diaz, C. (2011). Engineering privacy by design. In *Proceedings of the 4th Conference on Computers, Privacy & Data Protection (CPDP)* (pp. 1–25).
40. Hafiz, M. (2013). A pattern language for developing privacy enhancing technologies. *Software: Practice and Experience, 43*(7), 769–787.
41. Hoepman, J.-H. (2014). Privacy design strategies. In *Proceedings of the 29th IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)* (pp. 446–459).
42. Johansen, J., & Fischer-Hübner, S. (2020). Making GDPR usable: A model to support usability evaluations of privacy. In *Proceedings of the 14th IFIP International Summer School on Privacy and Identity Management* (pp. 275–291).
43. Karegar, F., Pulls, T., & Fischer-Hübner, S. (2016). Visualizing exports of personal data by exercising the right of data portability in the data track—are people ready for this? In *Proceedings of the 11th IFIP International Summer School on Privacy and Identity Management* (pp. 164–181).
44. Knijnenburg, B. P., Page, X., Wisniewski, P., Lipford, H. R., Proferes, N., & Romano, J. (2022). Introduction and overview. In B. P. Knijnenburg, X. Page, P. Wisniewski, H. R. Lipford, N. Proferes, & J. Romano (Eds.), *Modern Socio-Technical Perspectives on Privacy* (pp. 1–11). Springer.
45. Krueger, R. A., & Casey, M. A. (2015). *Focus groups: A practical guide for applied research* (5th ed.). Sage.
46. Lazar, J., Feng, J. H., & Hochheiser, H. (2017). *Research methods in human computer interaction* (2nd ed.). Elsevier.
47. Lenhard, J., Fritsch, L., & Herold, S. (2017). A literature study on privacy patterns research. In *Proceedings of the 43rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA)* (pp. 194–201).
48. Machuletz, D., & Böhme, R. (2020). Multiple purposes, multiple problems: A user study of consent dialogs after GDPR. *Proceedings on Privacy Enhancing Technologies, 2020*(2), 481–498.
49. Mathis, F., Vaniea, K., & Khamis, M. (2021). Prototyping usable privacy and security systems: Insights from experts. *International Journal of Human–Computer Interaction. 38*(5), 468–490.
50. Morton, A., & Sasse, M. A. (2012). Privacy is a process, not a PET: A theory for effective privacy practice. In *Proceedings of the Workshop on New Security Paradigms (NSPW)* (pp. 87–104).
51. Mulligan, D. K., & King, J. (2012). Bridging the gap between privacy and design. *University of Pennsylvania Journal of Constitutional Law, 14*(4), 1–46.
52. Murmann, P., & Fischer-Hübner, S. (2017). Tools for achieving usable ex post transparency: A survey. *IEEE Access, 5*, 22965–22991.

53. Murmann, P., Reinhardt, D., & Fischer-Hübner, S. (2019). To be, or not to be notified: Eliciting privacy notification preferences for online mhealth services. In *Proceedings of the 34th IFIP International Conference on ICT Systems Security and Privacy Protection (IFIP SEC)* (pp. 99–114).
54. Nouwens, M., Liccardi, I., Veale, M., Karger, D., & Kagal, L. (2020). Dark patterns after the GDPR: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the CHI Conference on Human Factors in Computing Systems* (pp. 1–13).
55. Papoutsakis, M., Fysarakis, K., Spanoudakis, G., Ioannidis, S., & Koloutsou, K. (2021). Towards a collection of security and privacy patterns. *Applied Sciences, 11*(4), 1396.
56. Pauwels, S. L., Hübscher, C., Bargas-Avila, J. A., & Opwis, K. (2010). Building an interaction design pattern language: A case study. *Computers in Human Behavior, 26*(3), 452–463.
57. Personal Information Protection Commission Japan. (2020). Amended act on the protection of personal information.
58. Piras, L., Al-Obeidallah, M. G., Pavlidis, M., Mouratidis, H., Tsohou, A., Magkos, E., Praitano, A., Iodice, A., & Crespo, B. G.-N. (2020). DEFeND DSM: A data scope management service for model-based privacy by design GDPR compliance. In *Proceedings of the 17th International Conference on Trust, Privacy and Security in Digital Business (TrustBus)* (pp. 186–201).
59. Polst, S., Kelbert, P., & Feth, D. (2019). Company privacy dashboards: Employee needs and requirements. In *Proceedings of the 1st International Conference on Human-Computer Interaction for Cybersecurity, Privacy and Trust (HCI-CPT)* (pp. 429–440).
60. Privacy Rights Clearinghouse (PRC). (2020). PRC Data Breach Chronology. Database 1.13.20, Privacy Rights Clearinghouse.
61. Presthus, W., & Sørum, H. (2019). Consumer perspectives on information privacy following the implementation of the GDPR. *International Journal of Information Systems and Project Management, 7*(3), 19–34.
62. Rapportage Datalekken 2020. (2020). Technical report, Autoriteit Persoonsgegevens.
63. Resolution on Privacy by Design. (2010). Technical report, *32nd International Conference of Data Protection and Privacy Commissioners*.
64. Robak, M., & Buchmann, E. (2020). How to extract workflow privacy patterns from legal documents. In E. Ziemba (Ed.), *Information Technology for Management: Current Research and Future Directions* (pp. 214–234). Springer.
65. Romanosky, S., Acquisti, A., Hong, J., Cranor, L. F., & Friedman, B. (2006). Privacy patterns for online interactions. In *Proceedings of the 13th Conference on Pattern Languages of Programs (PLoP)* (pp. 1–9).
66. Rosen, E. (2015). Human error biggest cause of data breach: Survey. *Bloomberg Law*.
67. Runte, C., & Kamps, M. (2021). *GDPR enforcement tracker report: Executive summary* (2nd ed.). CMS Law-Now.
68. Sahqani, W., & Turchet, L. (2021). Co-designing employees' data privacy: A technology consultancy company use case. In *Proceedings of the 28th Conference of Open Innovations Association (FRUCT)* (pp. 398–406).
69. Schufrin, M., Reynolds, S. L., Kuijper, A., & Kohlhammer, J. (2021). A visualization interface to improve the transparency of collected personal data on the internet. *IEEE Transactions on Visualization and Computer Graphics, 27*(2), 1840–1849.
70. Schumacher, M. (2003). Patterns and security standards—with selected security patterns for anonymity and privacy. In *Proceedings of the 8th European Conference on Pattern Languages of Programms (EuroPLoP)* (pp. 1–11).
71. Senarath, A., Arachchilage, N. A. G., & Slay, J. (2017). Designing privacy for you: A practical approach for user-centric privacy. In *Proceedings of the 5th International Conference on Human Aspects of Information Security, Privacy and Trust (HAS)* (pp. 739–752).
72. Siljee, J. (2015). Privacy transparency patterns. In *Proceedings of the 20th European Conference on Pattern Languages of Programs (EuroPLoP)* (pp. 1–11).
73. Spiekermann, S., & Cranor, L. F. (2009). Engineering privacy. *IEEE Transactions on Software Engineering, 35*(1), 67–82.

74. Stark, L., King, J., Page, X., Lampinen, A., Vitak, J., Wisniewski, P., Whalen, T., & Good, N. (2016). Bridging the gap between privacy by design and privacy in practice. In *Extended Abstracts of the CHI Conference on Human Factors in Computing Systems (CHI EA)* (pp. 3415–3422).
75. State of California. (2018). California Consumer Privacy Act. Assembly Bill No. 375.
76. Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU general data protection regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review, 34*(1), 134–153.
77. Tolsdorf, J., Dehling, F., & Lo Iacono, L. (2022). Data cart—designing a tool for the GDPR-compliant handling of personal data by employees. *Behaviour & Information Technology, 41*(10), 2070–2105.
78. Tolsdorf, J., Dehling, F., Reinhardt, D., & Lo Iacono, L. (2021). Exploring mental models of the right to informational self-determination of office workers in Germany. *Proceedings on Privacy Enhancing Technologies, 2021*(3), 5–27.
79. Tolsdorf, J., Fischer, M., & Lo Iacono, L. (2021). A case study on the implementation of the right of access in privacy dashboards. In *Proceedings of the 9th Annual Privacy Forum (APF)* (pp. 23–46).
80. Utz, C., Degeling, M., Fahl, S., Schaub, F., & Holz, T. (2019). (Un)informed consent: Studying GDPR consent notices in the field. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)* (pp. 973–990).
81. Veys, S., Serrano, D., Stamos, M., Herman, M., Reitinger, N., Mazurek, M. L., & Ur, B. (2021). Pursuing usable and useful data downloads under GDPR/CCPA access rights via co-design. In *Proceedings of the 17th Symposium on Usable Privacy and Security (SOUPS)* (pp. 217–242).
82. Wilson, C. (2014). Pluralistic usability walkthrough. In *User interface inspection methods* (pp. 81–97). Elsevier.
83. Yoder, J., & Barcalow, J. (1997). Architectural patterns for enabling application security. In *Proceedings of the 4th Conference on Patterns Language of Programming (PLoP)* (pp. 1–31).