Usable Implementation of Data Sovereignty in Digital Ecosystems

Denis Feth(✉)

Fraunhofer IESE, Fraunhofer-Platz 1, 67663 Kaiserslautern, Germany
denis.feth@iese.fraunhofer.de
https://www.iese.fraunhofer.de

Abstract. Products and services are increasingly being offered in so-called "digital ecosystems", where the processing of sensitive data plays a major role. In such ecosystems, the aim should always be to offer "data providers" (e.g., companies or consumers of goods and services) transparency and control over the processing of their data. This concept is called "data sovereignty." However, it is extremely challenging to present complex processes, data flows and protective measures to users in an understandable and comprehensible way. Furthermore, it is important to make users aware of the consequences of their choices when it comes to settings and consent—without influencing them inappropriately. However, users of digital ecosystems are very heterogeneous in their needs and abilities. For appropriate transparency (e.g., user-friendly privacy statements, uniform icons, traceable data flows) and self-determination measures (e.g., end-to-end consent management), these needs, abilities and some fundamental limitations must be considered. With this paper, we discuss how ecosystem providers and participants can implement data sovereignty in a user-friendly way. We extend the human-centred design process to include data sovereignty aspects and show how data usage control can help to technically implement user needs.

Keywords: Usable Security and Privacy · Data Sovereignty · Digital Ecosystems

1 Digital Ecosystems and Data Sovereignty

Products and services (so-called assets) are increasingly being exchanged and traded digitally. Providers and consumers are finding each other in so-called *digital ecosystems*. For example, consumers can book accommodation via Airbnb, commission craftsmen's services via MyHammer or buy products via the Amazon marketplace. Digital Ecosystems are defined as follows:

Definition 1 (Digital Ecosystem). *"A **digital ecosystem** is a socio-technical system connecting multiple, typically independent providers and consumers of assets for their mutual benefit. A digital ecosystem is based on the*

This work is funded by the German Federal Ministry of Education and Research (BMBF), grant number 16KIS1507.

A. Moallem (Ed.): HCII 2023, LNCS 14045, pp. 135–150, 2023.
https://doi.org/10.1007/978-3-031-35822-7_10

provision of digital ecosystem services via digital platforms that enable scaling and the exploitation of positive network effects. A ***digital ecosystem service*** *is characterized by a brokering activity that enables the exchange of assets between their providers and consumers. Typically, asset providers offer assets over a digital platform that brokers these assets to asset consumers. An* ***asset broker*** *aims to increase the transaction rate over the marketplace and thus facilitates the harmonized exchange of assets, carrying the responsibility of onboarding the participants, matching assets between them, and enabling physical or digital fulfillment. A* ***digital platform*** *is a software system that forms the technical core of a digital ecosystem, is directly used by providers and consumers via APIs or UIs—such as a digital marketplace—and facilitates the matching of a provider and a consumer in relation to an asset within a digital ecosystem service." [18]*

Digital ecosystems offer a wide range of opportunities for their participants. These include the development of new business areas, the acquisition of new customers, and the initiation of innovations in their own industry. Economies of scale and network effects are a central component of digital ecosystems and the platform economy.

In all of this, data plays a major role. For example, the asset providers and the platform provider generally process personal data in order to provide the asset. There are even various examples where the traded asset itself is data, e.g. Caruso[1], Advaneo[2], or GovData[3]. In this context, there is an increasing demand both by legislation (in the context of the GDPR) and by the users (i.e., primarily providers and consumers) themselves that users be granted certain information and co-determination rights regarding the use of "their" data. This kind of informed self-determination is also referred to as *data sovereignty*:

Definition 2 (Data Sovereignty). *"Data sovereignty means the greatest possible control, influence and transparency over the use of data by the data provider. The data provider should be entitled and empowered to exercise informational self-determination and be given transparency about the use of their data." [16] (translated from German)*

Data sovereignty is all the more important in view of the fact that digital ecosystems consist of a highly dynamic and hard to understand network of participants that have a commercial interest in the data.

1. Users must be able to *understand, interpret and verify* with reasonable effort how their data is used and shared.
2. Users must be given the opportunity to *influence the processing* of their data.
3. Users must understand the *impact* of certain decisions on them (e.g., giving consent).
4. Users must be *free and uninfluenced* in their decision.

[1] https://www.caruso-dataplace.com/.
[2] https://www.advaneo.de/.
[3] https://www.govdata.de/.

These requirements relate directly to the user experience (UX) and in particular the usability of the data sovereignty measures. In very general terms, the interaction between data sovereignty and UX can be summarized as follows: On the one hand, lack of data sovereignty can have a negative impact on important UX aspects such as satisfaction or trust. Therefore, data sovereignty can be a prerequisite for good UX. On the other hand, data sovereignty can only be achieved if the measures are also implemented in a usable way. Otherwise, users will not use them (at least not correctly) and thus indirectly be deprived of their sovereignty. For example, incorrectly made settings can even have the exact opposite effect of what the user actually wants.

In this paper, we convey the importance of a usable implementation of data sovereignty measures, address the specific challenges in digital ecosystems and present solution approaches. To this end, we take a closer look at our target groups in Sect. 2 and their main goals and challenges in Sect. 3. We then elaborate on design practices and propose an approach based on human-centred design and introduce the concept of "data usage control," which is an essential building block for technically enforcing data sovereignty in Sect. 4. We conclude in Sect. 5 by summarizing our key take-aways.

2 Target Groups

Before we can think about how to implement data sovereignty in a user-friendly way, we must clarify who is responsible in the first place and who the addressed users are.

In order to understand responsibilities, we have to be aware that digital ecosystems consist of a large number of interdependent systems and components that build on one another. By their very nature, these are not designed, developed and distributed by a single provider, but by a provider chain, as Fig. 1 illustrates.

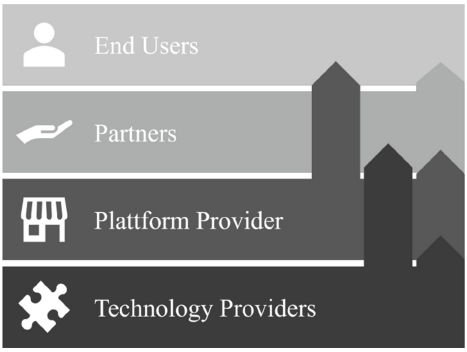

Fig. 1. Chain of providers and consumers

At the lowest level, technology providers provide generic software components, including data sovereignty components, for data flow tracking, access control or usage control. These solutions are used by the platform provider as well as by the ecosystem partners to develop their systems. These systems can ultimately be used by end users, directly or indirectly, to define and enforce their data sovereignty needs. Thus, each level is both a user of measures for the level(s) below and a provider of measures for the level(s) above. This makes the developers themselves to users when they integrate existing software libraries or system components—just on a different, more technical level than the end users. In contrast to the end-user level, however, poor usability or UX of the components to be integrated has a systemic impact on all ecosystem participants (e.g., through security vulnerabilities). A similar argument applies to system administrators, who must reliably configure and maintain security measures. Here, too, small errors can have serious consequences. In such cases, usability problems affect not only individual users, but all participants equally. Thus, one has to consider different characteristics of developers, as for example described by Clarke [5].

A general recommendation in the area of security is to develop as little functionality as possible yourself and instead to use established, possibly even certified components. At the same time, unfortunately, it must be noted that there are only a few established standard solutions, both for digital ecosystems and for data sovereignty. Looking at the research and development landscape, however, projects like GAIA-X[4], International Data Spaces[5] and solutions like MYDATA[6] illustrate a positive trend. In this respect, the background to this recommendation—namely, that security and data protection are highly complex areas and therefore errors or security gaps can easily creep in during in-house development—is of course nevertheless valid and relevant in our context.

End users are, of course, the primary stakeholder group when it comes to data sovereignty. When we talk about "the end user," we should first be aware of whether we are talking about a user whose sensitive data is being processed (i.e., the "data subject" in the area of data protection or in general the "data provider" when it comes to non-personal data) or about a user who, in turn, processes the sensitive data of others (the so-called "data user"). In addition, users differ greatly in their individual needs and capabilities with regard to data sovereignty. It is therefore worth taking a closer look at the classification of "Deutschland sicher im Netz" [Germany secure online] [6], which currently distinguishes five user types: fatalistic users (16.5 percent), outsiders (4.3 percent), gullible users (42.9 percent), thoughtful users (17 percent), and driving users (19.3 percent). DsiN also provides suggestions on how to counter the security deficits of the various user groups. Ultimately, however, general categorizations are only helpful up to a certain point, because digital ecosystems differ greatly. And even within a digital ecosystem, there can be strong cultural differences. For example, in a study by the European Union Agency for Fundamental Rights [8], 65 percent of

[4] https://www.gaia-x.eu/.
[5] https://www.internationaldataspaces.org/.
[6] https://www.mydata-control.de/.

participants from Cyprus said they would be willing to share their facial images with the government, compared to only nine percent of the German participants. Therefore, platform or service providers should always carefully examine their user base, classify it, and describe it using personas, for example. Corresponding methods and templates can be found in the relevant literature from the field of requirements engineering. This makes it possible to keep an eye on the specific characteristics of one's target groups during the (further) development of the digital ecosystem.

3 Goals and Challenges

From Definition 1 (see page 2), we can directly derive two main goals of data sovereignty: transparency and self-determination. In this chapter, we take a closer look on what that means and what typical challenges are in the digital ecosystem context. Furthermore, we discuss fundamental limitations of data sovereignty.

3.1 Transparency

First, let's take a look at the definition of transparency:

Definition 3 (Transparency). *Transparency means that the collection and processing of data in procedures and their use can be planned, traced, reviewed and evaluated with reasonable effort. (based on [24])*

Transparency in the processing of sensitive data is increasingly demanded by data providers (e.g., companies or consumers of goods and services) and, in the case of personal data, also by legislators. It is also a precondition for self-determination, because data subjects cannot decide about something they do not understand. In practice, complex facts have to be presented in such a way that users can understand and interpret them. Since sensitive data is processed on a large scale in digital ecosystems and a large number of companies are involved, this is no easy task. At this point, we will look at three transparency measures for digital ecosystems: user-friendly privacy policies, uniform icons and data flow tracking.

User-Friendly Privacy Policies. In practice, privacy policies are currently the only means of providing users with information about the processing of their data. However, it is well documented that the acceptance of privacy statements is already very low on "traditional" websites. Surveys (e.g., [21,29,30]) show that about three quarters of users do not read privacy statements at all, and the remaining users at most skim them. Approaches to improve the readability [7,20], comprehensibility [23], design [31], or basic structure [9,10,22] of privacy notices have so far borne little fruit in practice. In the case of digital ecosystems, this problem is exacerbated by the fact that this is a network that is difficult for

users to survey and is not transparent, with each participating company having its own data protection declaration. Users are thus inundated with information, and inconsistent interaction patterns, designs, and wording make it extremely difficult for users to understand and compare.

But with all these challenges, the centrality of digital ecosystems plays into our hands. Although the individual participants are independent in the ecosystem, their role often falls into one of a few categories (e.g., service providers, service consumer). The platform provider has the power to address the aforementioned issues by imposing binding requirements on all participants regarding the structure, expected information, and design of privacy policies. In addition, the platform itself can serve as a central entry point for users, making sense of the information provided by various privacy statements.

Uniform Icons. According to Art. 12 GDPR, information must be provided "in a precise, transparent, comprehensible and easily accessible form, using clear and simple language". As already described, in practice this usually results in textual data protection statements. The possibility of using uniform icons for the communication of data protection information is explicitly provided for (cf. GDPR Article 12, paragraphs 7 and 8). These icons could, for example, help to make the privacy notices, which are so vehemently ignored by users, more user-friendly in the future. Various initiatives have tried to develop good icons, e.g. the "Privacy Icons Forum"[7], Bitkom[8] or the State Commissioner for Data Protection and Freedom of Information of Baden-Württemberg[9]. Unfortunately, none of these proposals has yet gained widespread acceptance in practice. Until this is the case, individual solutions will continue to be in demand. As with the topic of privacy policies, the platform provider has the power to establish a uniform language and icons that support the user and increases transparency.

Data Flow Tracking. Another problem with data privacy policies is that they are static and rather abstract. For example, they merely explain that certain categories of data (e.g., address data) may be passed on to certain partners (e.g., shipping service providers) under certain circumstances (e.g., when an order is placed). However, it is seldom possible to trace which specific data was actually passed on to which partner for which order. In digital ecosystems in particular, where a high degree of dynamics and a large number of participants are a core characteristic, this is precisely where added value for users would arise. Again, the centrality of digital ecosystems plays into our hands here, since it is often comparatively easy from a technical point of view to log data flows on the platform. The greater challenge here is to make the available data comprehensible and user-friendly, for example as presented by Bier et al. [1].

[7] https://privacyiconsforum.eu/.
[8] https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Privacy-Icons.
[9] https://www.baden-wuerttemberg.datenschutz.de/datenschutz-icons/.

3.2 Self-determination

The goal of high transparency was not only to inform those affected, but also to lay the groundwork for them to take control of their own data while understanding the consequences. To make this possible, two additional steps are required:

1. the data subject must be given the opportunity to define his needs and requirements with regard to processing.
2. the defined rules must be implemented by all ecosystem participants.

Both aspects are very challenging. We will deal with the first aspect directly below by looking at the challenges of consent management and setting options in general. We will return to the second aspect in Sect. 4.2.

Consent Management. In the area of data protection, the GDPR stipulates that companies may only process personal data if at least one of six prerequisites is met. One of these prerequisites is that the data subject has given consent. In principle, there are no such restrictions for non-personal data, even though they are quite plausibly transferable and benefit the self-determination of data providers. In the case of data protection, however, the downsides also come to light at this point: due to the uncertainties created by the GDPR, users are often confronted with consent forms, even though it is not necessary. Furthermore, consent is only legally valid if it is given voluntarily and uninfluenced. "Nudging", as often occurs with cookie consent, is therefore not permissible. Even small design decisions (so-called "dark patterns") can tempt a person to select an option that does not correspond to his or her actual wishes [3]. In this case, consent is not legal.

In a study by Kettner et al. [17], consumers were presented with various designs for consent management. Based on this study, a best practice model for innovative consent management was developed using various practical examples. In the case of digital ecosystems, the question should also be asked as to whether it makes sense and is feasible to offer centralized consent management via the platform. Ultimately, this would save work and provide security for all ecosystem participants.

User-Friendly Privacy Settings. Many large platforms already offer users data protection settings. Many of these settings require the user to make tradeoffs between privacy and other features or resources. For example, restrictive privacy settings (i.e., a higher level of privacy) in Google search are accompanied by less personalized suggestions (i.e., a lower level of effectiveness). Nevertheless, the default settings should be privacy-friendly in any case, in line with the principle of "privacy by default". Regardless of this general challenge, settings options differ according to the degrees of freedom and support they provide to the user, as well as their general interaction paradigm [25]. Here, there is a wide spectrum - starting with very coarse security levels, over templates and wizards, up to special "policy languages" (e.g. XACML, ODRL or proprietary languages) to

express needs and constraints. Which paradigm is most appropriate depends on a variety of factors and the target group (cf. Sect. 2). Policy languages, for example, are reserved for experts on the intermediate layers because they require detailed knowledge of the language and the system being controlled. At the same time, coarse security levels do not provide experts with the desired flexibility. At most, they can serve them to make basic settings. The choice and implementation of the interaction paradigm must therefore always be precisely tailored to the respective characteristics and needs of the user groups.

3.3 Limitations of Data Sovereignty in Digital Ecosystems

The centrality of the platform plays into our hands in many places, as we have just seen. However, there are also a number of characteristics of digital ecosystems and some fundamental trade-offs that complicate the situation:

- *Temptations:* Digital ecosystems offer great advantages to providers and consumers, especially when services can be customized based on the user's data. At the same time, the barrier to entry and the perceived risks are fairly low. This makes it tempting for users to give consent and disclose data.
- *Achieving overall trust:* Trust is essential for data being shared and used. However, it is challenging to establish trust in an entire ecosystem that potentially comprises thousands of (legally independent) participants. Since all participants are legally independent entities, it often is unclear for the user who is the data controller for a concrete use case or transaction. It is therefore important that the platform operator does everything to ensure that customers have an extremely high level of trust in him and support the user in the best possible way.
- *Volatility:* Digital ecosystems, like all ecosystems, are subject to constant change: providers come and go; services are revised; terms and conditions or privacy statements are updated; the ecosystem adapts to changing laws, etc. This means that the user would continuously need to be concerned with the protection of their data-which is, of course, completely illusory.
- *Transparency vs. monitoring:* The more data flows and data processing are made transparent, the higher the risk that sensitive information about the persons processing the data will be disclosed. For example, if the exact time and person of a data use is disclosed, the data subject can draw conclusions about the work behavior of the data user. Anonymization can at least partially resolve this trade-off.
- *Trust vs. distrust:* With a high level of transparency, there is a risk that users will not be able to correctly classify the information shown and will draw erroneous conclusions. In addition, they may become aware of facts that seem surprising to them. The reasons and objectives for new measures (such as increasing transparency) should also be made clear. Data subjects might otherwise wonder, for example, whether there was a data protection incident that led to this introduction.

– *Data sovereignty vs. social pressure:* If data providers and data users know each other, e.g., if they have a direct business relationship, data providers may face social pressure to provide their data. This, of course, then directly threatens their sovereignty.

These described examples illustrate that there is not or cannot be a "perfect" solution. Even if the implementation of data sovereignty initially appears to be ideally implemented from the user's perspective, many factors must be taken into account and weighed against each other. With regard to the data protection paradox, the question arises as to whether it is even possible to solve the described problems in a meaningful way. After all, regardless of whether users exercise their data sovereignty or not, someone else's privacy may be at risk. The maxim of granting users as much transparency and participation as possible is therefore untenable. Instead, a case-by-case approach and the balancing of interests are essential.

Finally, it should be clear to all involved that data sovereignty does not, of course, mean that users have unrestricted freedom with regard to the processing of their data. There are, of course, various situations (e.g., law enforcement) or laws (e.g., retention obligations) that have a higher priority than the self-determination of the individual. This is also regulated accordingly in the GDPR (e.g., in Article 2, paragraph 2d or Article 6, paragraph 1e). Ultimately, the following principle applies to data protection as well as data sovereignty: "The freedom of the individual ends where the freedom of others begins."

4 Methods and Tools

Having gained an overview of the different stakeholders, their goals and challenges, as well as some solution approaches for digital ecosystems, the question naturally arises how to methodically approach the user-friendly implementation of data sovereignty. In this chapter, we approach this question from an organisational and a technical side.

4.1 Organisational Implementation

In the past decades, a number of product development models and methods have been proposed to support the development of secure products (e.g., Microsoft's Security Development Lifecycle (SDL) [14]). Unfortunately, all these methods hardly consider the usability and UX of security measures. Conversely, for many application domains there are still no best practices on how to adequately consider security and privacy in a user-centric design.

Therefore, in this chapter we would like to present our approach to integrating "Usable Security & Privacy" (USP) concepts into the human-centred design (HCD) process (cf. ISO 9241). HCD is understood as an interactive and iterative design process with users, where designers use prototyping and feedback loops to understand users and their requirements. To each step of HCD, we added aspects related to the user-friendly implementation of data sovereignty.

Understand the Context of Use. The first step of HCD is to understand the context of use. According to ISO 9241, context of use includes users, tasks, equipment (hardware, software, and materials), and the physical and social environment in which a product is used. We propose to consider three more aspects:

1. *Understanding Data in the Digital Ecosystem.* First, one has to be clear about data categories processed in the digital ecosystem and who can access them under which circumstances. This can be done by analyzing the ecosystem service, the business processes, the platform architecture and interfaces.
2. *Understand Privacy Regulations.* Second, one has to know and consider data protection regulations, company policies and the Terms and Conditions and contracts in the digital ecosystem to be able to narrow down the solution space. Particular attention should also be paid to the issues of commissioned data processing and cross-border data transfer. If data leaves the GDPR's scope of jurisdiction, for example, this must of course first be clarified in legal terms.
3. *Understand User Characteristics.* Users have different needs and characteristics related to data sovereignty. For example, regardless of the legal assessment one should also check how users feel about cross-border data transfer. Are they okay with it or will they reject it because they feel their privacy is at risk? End users can be distinguished based on the characteristics shown in Fig. 2, among others. All these characteristics can have an impact on the design. For example, if a person has a strong need for privacy, appropriate privacy features could be placed prominently so that the user understands that the system cares about privacy. If a user knows little about data sovereignty, the system could educate the user about the threats and opportunities. If the user's skills are low, a tutorial could help them apply the measures. If the user is not used to being able to act sovereignly, reminders could help to establish such habits.

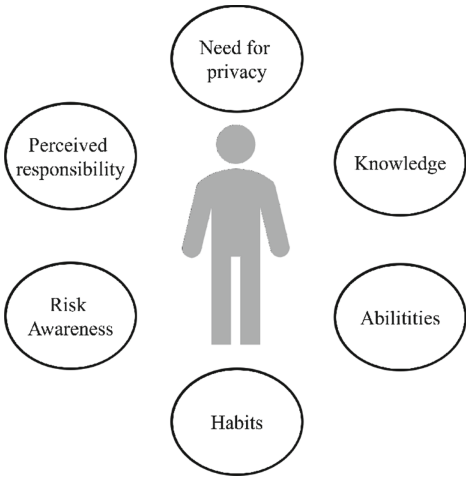

Fig. 2. Characteristics of end users in terms of Data Sovereignty

Elicit User Needs. The second step in HCD is to identify user needs, based on the identified user types. In our case, there are two important types of users—data providers and data users. It is important to distinguish them because they have different needs that may conflict with each other.

Data providers (data subjects in the sense of data protection) have the following types of needs:

- *Data protection needs:* the desire to protect certain types of data or certain data elements.
- *Transparency needs:* the need or desire for information about how their data is used.
- *Self-determination needs:* the need or desire for control over how their data is used.

Data users (the people who process someone else's data) have the following types of needs:

- *Data processing needs:* the need to process a data category or data item to accomplish a task.
- *Information needs for processing:* a person's need for information about the rules governing the processing of data, e.g., information about the purposes for which the specific data may be used.

Of course, it must be specifically determined which particular needs they have in the respective categories.

It is also to be noted that, data processing needs and data protection needs can be conflicting. The conflict can be resolved or mitigated by providing information about the need for and benefits of the data processing as well as the measures to protect the data.

Develop Solutions. The third HCD step is the development of solutions. Best practices from the area of USP should be known and observed here. The USecureD project[10] has collected such best practices and distinguished between three levels: principles, guidelines and patterns.

Principles: Principles are general rules for designing systems. They are based on experience, are relatively short, and are well suited for gaining a basic understanding of USP. USecureD provides a collection of 23 principles online, such as the following:

- Good security now [12]: Don't wait for the perfect.
- Path of least resistance [32]: The easiest path should be the safest.
- Conditioning [4]: Use positive reinforcement to encourage a desired behavior.

[10] https://www.usecured.de/.

Guidelines: Guidelines describe how to implement the principles. They are important to eliminate as many potential problems as possible early in the process [2]. They also help to ensure a high quality standard and reduce the complexity of development projects. USecureD provides a collection of guidelines online, such as guidelines for usable crypto APIs [13], for error prevention [27], and for standardized procedures [26,28].

Patterns: Patterns are proven solutions to recurring problems encountered during system development. Today, following patterns is an integral strategy in the software industry. This is reflected in a large number of collections, which contain patterns for many phases of the software engineering, e.g. architecture, documentation, organization of user interfaces or even security. In the last years also increasingly patterns for USP developed. They deal with aspects such as authentication, authorization, key management, digital signatures, encryption, secure data deletion, creation of backups, user-friendly APIs, and the design of hints, warnings, and system states [19]. USecureD provides an extensive collection online here as well.

Evaluate Against the Requirements. In the final HCD step, the developed solution is evaluated against the requirements. User tests are usually very time-consuming and cost-intensive, since users usually receive at least an expense allowance for their participation. It is therefore advisable to have a heuristic evaluation performed by experts before starting user tests. This method is less expensive, faster, and can already uncover many design flaws before getting to the users with it. To this end, we provided a list of 45 heuristics for evaluating the usability of security and privacy measures and described their application in HCD (cf. Fig. 3) in an earlier publication [11].

These heuristics cover usable transparency (e.g., it is clearly stated for which purposes data is used), authentication (e.g., password policies are directly displayed when passwords are issued), user control and freedom (e.g., users can update or delete incorrect data on their own), error detection, diagnosis and correction (e.g. error messages inform about the severity of the problem), user support and documentation (e.g., help and documentation follow process steps), and accessibility (e.g., the system supports the use of text passwords for visually impaired users).

4.2 Technical Enforcement

In the previous chapters, we have seen the challenges that need to be addressed in order to implement data sovereignty in a user-friendly way. The problem is that the complexity of many requirements and privacy settings goes beyond what can be directly implemented with standard Identity and Access Management solutions. In particular, data filtering (e.g., “Only records from the last 30 days”), data masking (e.g., “Blacken fields with purchased items”), data anonymization, and data usage requirements (e.g., “Delete data after 14 days”) are gaining

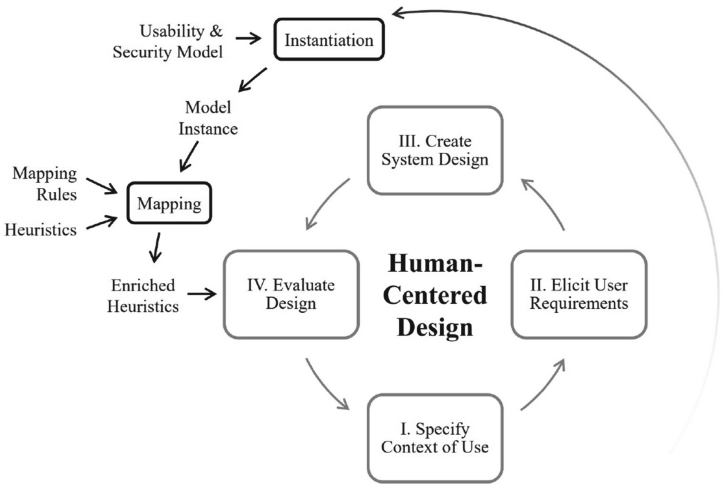

Fig. 3. Heuristic evaluation in the human-centred design [11]

importance. Especially data usage requirements, which regulate usage of data, not the access to it, are challenging. However, platform and service providers need to find ways to technically enforce such requirements in a digital ecosystem.

To this end, the following features must be implemented:

1. data usage and data flows must be controlled at relevant points in the ecosystem, e.g., in the platform.
2. desired data uses must be balanced against a variety of complex rules, which may include propositional, cardinal, and temporal aspects. Contextual factors may also need to be considered.
3. Preventive (e.g., blocking or filtering the data flow) or reactive (e.g., notifying the user or administrator) actions must be able to be performed according to the evaluation of the constraints.
4. if data is passed on, usage obligations ("delete data after 14 days") must be passed on to the target system and implemented there accordingly.

While it is still possible to implement the first three requirements oneself in traditional systems with reasonable effort, this is no longer practicable in the case of cross-company data exchange in an inherently volatile, digital ecosystem with regard to the fourth requirement. Special usage control frameworks and solutions that combine the specification, management and enforcement of data usage rules, have to be used here [15].

5 Summary and Conclusion

For digital ecosystems, the processing of sensitive data is fundamental. In particular, incentives to share sensitive data in a digital ecosystem quickly outweigh

actual intentions or concerns. In this paper, we thus addressed how to implement usable data sovereignty—which essentially consists of the areas of transparency and self-determination—in digital ecosystems. Data sovereignty is not limited to personal data, but to all kinds of sensitive data that is processed in a digital ecosystem. It therefore has a broader scope than data protection, but makes use of many of its aspects.

To create transparency, it must be possible for the data provider to trace, check and evaluate the use of data with a reasonable amount of effort. Privacy policies are mandatory, but are not well received in their current form. Therefore, use different levels of detail and speak the language of the user—briefly, precisely, and oriented to the use case. Ideally, the platform provider provides binding design specifications here. Concepts like contextual privacy policies and data flow tracking allow becoming more concrete than static, abstract privacy policies.

With respect to self-determination, it has to be considered that users can only express their needs effectively, efficiently and satisfactorily if the consent and setting tools offered are tailored to them. Consents are only valid if they are given voluntarily and without manipulation of the user.

When planning and implementing data sovereignty measures, it needs to be considered that users are not homogeneous, and that there is certainly no "one-size-fits-all" solution when it comes to data sovereignty and digital ecosystems. User classification and personas help to keep track of the specific characteristics of target groups. However, one needs to be aware that data sovereignty can also have negative effects. Ultimately, the interests of all ecosystem participants must be weighed against each other.

Usability and UX are often neglected in security processes and vice versa. A user-centric approach along the HCD process we have presented can help to better understand user needs and implement data sovereignty in a user-friendly way. This process should be seen more as an inspiration, but not as something to which one must always adhere. Also, the area of "Usable Security & Privacy" covers a broad spectrum of cross-cutting and interdisciplinary topics between the areas of security, privacy, and UX. We recommend that these topics should always be considered holistically and from the outset, taking into account their mutual interactions.

Finally, with all the discussions about the user's needs, one must of course not lose sight of the technical feasibility. Usage obligations in particular are often difficult to technically implement in practice, because traditional security solutions often end at the "access gate". Data usage control [15] offers a suitable extension here.

References

1. Bier, C., Kühne, K., Beyerer, J.: PrivacyInsight: the next generation privacy dashboard. In: Schiffner, S., Serna, J., Ikonomou, D., Rannenberg, K. (eds.) APF 2016. LNCS, vol. 9857, pp. 135–152. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-44760-5_9

2. Birolini, A.: Zuverlässigkeit von Geräten und Systemen. Springer, Heidelberg (2013)
3. Caraban, A., Karapanos, E., Gonçalves, D., Campos, P.: 23 ways to nudge: a review of technology-mediated nudging in human-computer interaction. In: Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems, CHI 2019, pp. 1–15. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3290605.3300733
4. Chiasson, S., van Oorschot, P., Biddle, R.: Even experts deserve usable security: design guidelines for security management systems. In: SOUPS Workshop on Usable IT Security Management (USM), pp. 1–4 (2007)
5. Clarke, S.: What is an end user software engineer? In: Burnett, M.H., Engels, G., Myers, B.A., Rothermel, G. (eds.) End-User Software Engineering. Dagstuhl Seminar Proceedings (DagSemProc), vol. 7081, p. 1. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, Dagstuhl, Germany (2007). https://doi.org/10.4230/DagSemProc.07081.26. https://drops.dagstuhl.de/opus/volltexte/2007/1080
6. Deutschland sicher im Netz e.V.: DsiN-Sicherheitsindex 2021 (2021). https://www.sicher-im-netz.de/dsin-sicherheitsindex-2021
7. Ermakova, T., Fabian, B., Babina, E.: Readability of privacy policies of healthcare websites (2015)
8. European Union Agency for Fundamental Rights: Your rights matter: data protection and privacy: fundamental rights survey. Publications Office (2020). https://doi.org/10.2811/292617
9. Feth, D.: Transparency through contextual privacy statements. In: Burghardt, M., Wimmer, R., Wolff, C., Womser-Hacker, C. (eds.) Mensch und Computer 2017 - Workshopband. Gesellschaft für Informatik e.V., Regensburg (2017). https://doi.org/10.18420/muc2017-ws05-0406
10. Feth, D.: Modelling and presentation of privacy-relevant information for internet users. In: Moallem, A. (ed.) HCII 2020. LNCS, vol. 12210, pp. 354–366. Springer, Cham (2020). https://doi.org/10.1007/978-3-030-50309-3_23
11. Feth, D., Polst, S.: Heuristics and models for evaluating the usability of security measures. In: Proceedings of Mensch Und Computer 2019, MuC 2019, pp. 275–285. Association for Computing Machinery, New York (2019). https://doi.org/10.1145/3340764.3340789
12. Garfinkel, S.: Design principles and patterns for computer systems that are simultaneously secure and usable. Ph.D. thesis, Massachusetts Institute of Technology (2005)
13. Green, M., Smith, M.: Developers are not the enemy!: the need for usable security APIs. IEEE Secur. Priv. **14**(5), 40–46 (2016)
14. Howard, M., Lipner, S.: The Security Development Lifecycle, vol. 8. Microsoft Press, Redmond (2006)
15. Jung, C., Dörr, J.: Data usage control. In: Otto, B., ten Hompel, M., Wrobel, S. (eds.) Designing Data Spaces, pp. 129–146. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-93975-5_8
16. Jung, C., Eitel, A., Feth, D.: Datensouveränität in Digitalen Ökosystemen: Daten nutzbar machen, Kontrolle behalten. In: Rohde, M., Bürger, M., Peneva, K., Mock, J. (eds.) Datenwirtschaft und Datentechnologie, pp. 203–220. Springer, Heidelberg (2022). https://doi.org/10.1007/978-3-662-65232-9_15
17. Kettner, S., Thorun, C., Spindler, G.: Innovatives datenschutz-einwilligungsmanagement. Forschungsvorhaben gefördert durch das BMJV, Berlin (2020)

18. Koch, M., Krohmer, D., Naab, M., Rost, D., Trapp, M.: A matter of definition: criteria for digital ecosystems. Digit. Bus. **2**(2), 100027 (2022). https://doi.org/10.1016/j.digbus.2022.100027. https://www.sciencedirect.com/science/article/pii/S2666954422000072
19. Lo Iacono, L., Schmitt, H., Feth, D., et al.: Arbeitskreis usable security & privacy: nutzerzentrierter schutz sensibler daten (2018)
20. Milne, G.R., Culnan, M.J., Greene, H.: A longitudinal assessment of online privacy notice readability. J. Public Policy Mark. **25**(2), 238–249 (2006)
21. Obar, J.A., Oeldorf-Hirsch, A.: The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services. Inf. Commun. Soc. **23**(1), 128–147 (2020)
22. Ortloff, A.M., Güntner, L., Windl, M., Feth, D., Polst, S.: Evaluation kontextueller datenschutzerklärungen. In: Dachselt, R., Weber, G. (eds.) Mensch und Computer 2018 - Workshopband. Gesellschaft für Informatik e.V., Bonn (2018). https://doi.org/10.18420/muc2018-ws08-0541
23. Reidenberg, J.R., et al.: Disagreeable privacy policies: Mismatches between meaning and users' understanding. Berkeley Tech. LJ **30**, 39 (2015)
24. Rost, M., Bock, K.: Privacy by design und die neuen schutzziele. Datenschutz und Datensicherheit-DuD **35**(1), 30–35 (2011)
25. Rudolph, M., Polst, S., Doerr, J.: Enabling users to specify correct privacy requirements. In: Knauss, E., Goedicke, M. (eds.) REFSQ 2019. LNCS, vol. 11412, pp. 39–54. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-15538-4_3
26. Shneiderman, B., Leavitt, M., et al.: Research-Based Web Design & Usability Guidelines. Department of Health and Human Services, Washington DC (2006)
27. Shneiderman, B., Plaisant, C., Cohen, M.S., Jacobs, S., Elmqvist, N., Diakopoulos, N.: Designing the User Interface: Strategies for Effective Human-Computer Interaction. Pearson (2016)
28. Smith, S.L., Mosier, J.N.: Guidelines for Designing User Interface Software. Citeseer (1986)
29. Symantec: State of Privacy Report 2015 (2015)
30. Tsai, J.Y., Egelman, S., Cranor, L., Acquisti, A.: The effect of online privacy information on purchasing behavior: an experimental study. Inf. Syst. Res. **22**(2), 254–268 (2011)
31. Waldman, A.E.: Privacy, notice, and design. Stan. Tech. L. Rev. **21**, 74 (2018)
32. Yee, K.-P.: User interaction design for secure systems. In: Deng, R., Bao, F., Zhou, J., Qing, S. (eds.) ICICS 2002. LNCS, vol. 2513, pp. 278–290. Springer, Heidelberg (2002). https://doi.org/10.1007/3-540-36159-6_24