

# What are your intentions with my data? A tool to enhance consumer data sovereignty in digital ecosystems

Aaron Witzki <sup>1</sup>, K. Valerie Carl <sup>2</sup>, Léon Dankert <sup>3</sup>, Oliver Thomas <sup>4</sup>, and  
Oliver Hinz <sup>5</sup>

**Abstract:** As data collection enhances, consumer data sovereignty becomes increasingly important. Despite initiatives like the GDPR, information asymmetries persist, and privacy policies remain complex or lengthy, often preventing consumers from giving truly informed consent for data sharing. Building on established concepts for more informed consent, we propose a tool—the consent registry—to enable informed consent and strengthen consumer data sovereignty while being easy to implement in a variety of digital ecosystems and applications. Our concept takes three different stakeholder groups into consideration, the consumer, the inquiring institution and the application provider, since often times the consumer is not directly connected to inquiring institutions and instead relies on third-party applications in digital ecosystems. Our tool employs case-to-case consent, describing that consent is valid only for a singular request. This empowers consumers to exercise informed control over data collection and usage while enhancing data availability across institutional borders in digital ecosystems.


**Keywords:** Data Sharing, Consumer Sovereignty, Privacy Policies, Informed Consent, Privacy Tool, Digital Ecosystem

## 1 Introduction


As companies today collect an ever-increasing amount of data of their customers, they can create even more detailed personal profiles, enabling them to, e.g., tailor advertisements

---


<sup>1</sup> Goethe University Frankfurt/Main, Chair of Information Systems and Information Management, Theodor W.-Adorno-Platz 4, 60323 Frankfurt/Main, witzki@wiwi.uni-frankfurt.de,

 <https://orcid.org/0009-0009-7150-6627>


<sup>2</sup> Goethe University Frankfurt/Main, Chair of Information Systems and Information Management, Theodor W.-Adorno-Platz 4, 60323 Frankfurt/Main, kcarl@wiwi.uni-frankfurt.de,

 <https://orcid.org/0000-0003-4655-1046>


<sup>3</sup> German Research Centre for Artificial Intelligence, Smart Enterprise Engineering, Parkstraße 40, 49080 Osnabrück, leon.dankert@dfki.de,

 <https://orcid.org/0009-0008-7989-8058>

<sup>4</sup> German Research Centre for Artificial Intelligence, Smart Enterprise Engineering, Parkstraße 40, 49080 Osnabrück, oliver.thomas@dfki.de,

 <https://orcid.org/0009-0007-3326-4175>

<sup>5</sup> Goethe University Frankfurt/Main, Chair of Information Systems and Information Management, Theodor W.-Adorno-Platz 4, 60323 Frankfurt/Main, ohinz@wiwi.uni-frankfurt.de,

 <https://orcid.org/0000-0003-4757-0599>

and services [VT21]. However, this also leads to growing information asymmetries, as consumers provide increasingly more data, while companies disclose little in an understandable way, particularly regarding how they handle data [Wa20]. Especially in digital ecosystems, consumers often share data with the whole ecosystem without being actually aware of it. For this reason, legislation such as the General Data Protection Declaration (GDPR) represents a significant step in the direction of more data sovereignty. However, it remains far from comprehensive. For example, it often results in lengthy privacy policies that consumers in many cases do not understand or even read at all, leading to uninformed consent [Ba22]. This lack of awareness can diminish consumer data sovereignty despite being an important value, especially in a more digitalized world. In addition, access to data presents a significant challenge, particularly for smaller companies, as there are currently few alternatives available for obtaining data, other than through consumers' acceptance of privacy policies when using the product and collaborating with other firms [JB24]. Consumers can profit from more transparent methods supporting their data sovereignty in the digital world and reducing information asymmetries, while responsibly granting deliberate access to collected data for a wider audience. These measures should empower consumers with a clear understanding of how institutions handle their data [Mi22, Tr23] and give consumers the ability to make informed decisions about data usage, eventually even on a case-to-case-basis. Previous research shows that users might be willing to disclose data in exchange for desired services [Ko17]. However, such cases might not enhance consumer empowerment, as they do not provide sufficient information about data usage, thus not supporting informed disclosure.

We present a novel tool specifically designed for digital ecosystems which we term as the *consent registry*, to enhance the empowerment of consumers. This registry has the ability to enhance consumer data sovereignty by enabling use-case-specific, active and informed consent to data requests. The acceptance of one request is only valid for a single case for one institution. In this way, our tool inherently increases transparency, yet the main focus remains in strengthening consumer data sovereignty. Privacy policies and legislation such as the GDPR lay the groundwork for our solution, yet we aim to enhance them by increasing consumer friendliness and easing the way they can exercise power over data collection and usage. Often times, inquiring institutions present privacy policies unintuitively to consumers today [Ef19], potentially leading to uninformed consent. Previous works investigated possible solutions and more comprehensible representations of privacy policy, e.g., privacy icons [RP20] and one-pager solutions [RS18]. Drawing from such concepts, we present a compact, yet concise, representation of privacy policies to consumers in a dedicated tool to control their data in digital ecosystems, to ultimately enhance consumer data sovereignty in the digital age. In contrast to previously established concepts, such as ID wallets [e.g., PAZ22], our tool only focuses on the user data that is generated in the application, in our use case (energy) consumption data and does not include further identifying information. The goal of our concept is to strengthen consumer data sovereignty by granting the consumers granular decisions regarding their data sharing. We structure the remainder of the paper as follows. Section 2 introduces the concepts of data privacy and sovereignty. Following, section 3 provides the architecture

of the data management tool: the consent registry. Finally, in section 4, we present an outlook of our work and the contribution to consumer data sovereignty in theory.

## 2 Data privacy and consumer data sovereignty

Data privacy describes a broad concept with the goal to ensure the responsible usage of data [CH24]. It encompasses various aspects [Ca21b] regarding, e.g., data protection (e.g., protection against unauthorized access) [He25] and the ethical use of data [Mi22]. Laws set minimum requirements for data privacy [Ca22a] in various regions around the world: e.g., the Personal Information Protection Law in China [Ca22a] and the GDPR in the European Union [LYH19]. The GDPR, for instance, describes data privacy as a “fundamental right” in recital 1. These frameworks have been established to safeguard fundamental citizen rights in the digital realm [CM22]. Apart from aspects of data protection and compliance with laws, the concept of data privacy also includes more consumer-focused aspects, e.g., transparent communication to the consumer that exceed regulatory minimum requirements [JLL21, Ca22b, CH24].

Data sovereignty, as a concept, centers on the consumer, their personal data and their ownership of their data [Hu21]. The focus of data sovereignty is the empowerment of the consumer in the digital sphere with the goal to ensure the ownership of the personal data [Ca21a], thereby often exceeding regulatory minimum requirements. Data sovereignty includes multiple aspects, like data ownership and control of the data [Hu21]. To ensure data sovereignty, consumers should have control over their data, including who can access it and how different actors utilize it [BC11]. The GDPR defines various aspects of data control in Articles 15-22, for instance the right of access by the data subject (Art. 15 GDPR). To ensure this, transparency practices [Lo24] and informed consent [AKR22] are potential measures. Transparency hereby includes all relevant information regarding the further processing of the data for the consumer, to control the compliance with the stated usage [Lo24], therefore being a crucial prerequisite for an informed consent.

The informed consent is a necessity, since a general acceptance of privacy policies might not be sufficient [Ef19]. Consumers tend to underestimate the consequences of the general acceptance of privacy policies [Ba22]. This could potentially lead to unforeseen and undesirable consequences (e.g., loss of privacy or unknowingly relinquishing rights) for the consumer and may permanently damage their trust [MF16]. Often times, institutions present the privacy policies in a way that does not focus on easy understanding, e.g., through policies that are hard to comprehend for the consumer [CC15] or not of an appropriate length for the service or product used. Another aspect is that, despite lengthy privacy policies, information asymmetries remain [Wa20]. Consumers often lack information about already collected data and to what extent inquiring institutions will actually use the data [Mi22]. This further complicates the informed consent [Ef19] due to an inadequate level of transparency. Despite the right to access and alter collected data (i.e., granted by the GDPR), consumers do not exercise their power often.

Through this lens, it is apparent that regulations alone, e.g., the GDPR, might not be sufficient to ensure consumer data sovereignty in practice. While the regulations include sufficient formal requirements, their implementation often falls short in usability and effectiveness for consumers, hindering consumers from performing their legal rights. For this reason, previous research has proposed various consumer-centered concepts [SE24]. Concepts such as privacy icons [Wi22] or one-pager privacy policies [RS18] arose (partly indicated by the GDPR but not mandatory), to further enhance consumer data sovereignty and enable the informed consent [Ca22b]. However, these concepts face challenges as well. For instance, privacy icons alone might not be sufficient to convey the complexity of certain cases and may vary in effectiveness depending on the context [Gr24]. One-pager solutions for the general consent face the risk of oversimplifying circumstances and may lead to misinterpretations of the consumers [KKS20]. Still, those approaches are valuable measures to strengthen consumer sovereignty beyond legal requirements.

We build upon these concepts to present a tool that supports the informed consent in digital ecosystems. As of now, digital ecosystems mainly employ complicated, lengthy privacy policies and often only require one consent per check mark to share collected data with the whole institution or even ecosystem. Therefore, we aim to develop an easy to implement tool that fosters data sovereignty by easing control over collected data, enhancing data control in digital ecosystems on a case-to-case basis. We consider three distinct stakeholder groups in digital ecosystems: consumers generating data, institutions requesting data, and application providers. Consumers often lack a direct connection with the inquiring institutions and instead rely on third-party applications in digital ecosystems.

### **3 The consent registry tool to enhance consumer data sovereignty**

To facilitate the practical applicability, we present our tool within the context of a digital ecosystem for smart living, since data from personal households is sensitive and requires informed consent for sharing. The tool will be implemented in an already used application to track consumption data, so that the consumers will only face the choice of sharing their data without any further needed configurations. When designing the tool, we tried to ensure self-explainability and ease of use. This application is not independent of requiring institutions, rather the application is part of the same digital ecosystem like requiring institutions, despite the app users not being an active participant of the digital ecosystem yet before introducing our tool. Our consent registry is situated within the context of emerging data ecosystems that prioritize consumer data sovereignty, such as SmartLivingNEXT [Sm25]. We developed the tool based on prior research and stakeholder requirements through dedicated focus groups and discussed the consent registry during several workshops with academics, practitioners and interested persons. We display the general process of the proposed consent registry tool in Figure 1.

To issue such requests, institutions need to fill out predefined request forms, which serve to inform the consumer about, e.g., not only the intended purpose of the data, but also how

long they intend to use the data. Often times consumers are not in direct contact with requesting stakeholders in a digital ecosystem, but use third-party applications and services to record and manage their data in such ecosystems and are therefore part of such ecosystems. Therefore, at first, the requests will pass these third-party application providers. The application providers have the ability to block requests that they deem inappropriate for their user community. If the application providers allow requests, they will be sent to consumers and be presented in a comprehensible format. Only if the consumer decides to accept the request, the data will be sent to the institution.

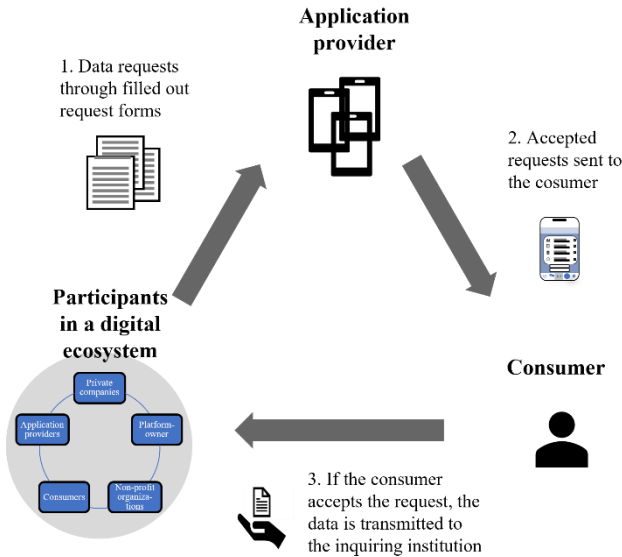


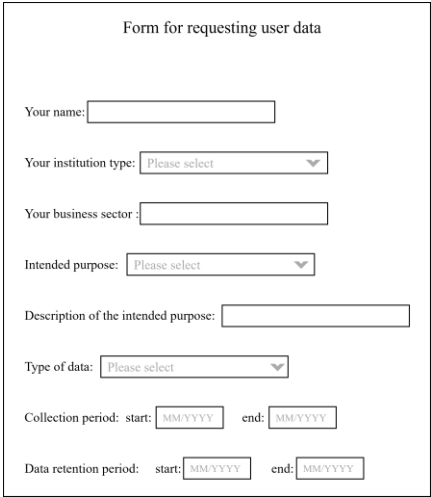
Fig. 1: Process of the consent registry

The consumers need to be aware of the exact goals that institutions follow with their data to give informed consent. Such active consent does not necessarily hinder data collection and usage. Rather, giving informed consent can enhance trust in digital ecosystems and particular participants. Further, entities collecting consumer data are sometimes afraid of legal and security risks when sharing data with external partners. However, employing such an active-consent-approach can allow more external institutions access to collected consumer data and therefore benefit particularly small and medium-sized enterprises as well as start-ups in their initial data access. In this way, all involved stakeholder groups can potentially benefit from such a consent tool: Consumers can easily exercise their power over collected data and deliberately choose with whom to share data for which reasons. Corporate entities in a digital ecosystem can request data from consumers without a direct business relationship and can therefore benefit from a vast amount of data available in such digital ecosystems. And finally, the application provider benefits from a more trusting relationship to their users since they allow them to decide about data sharing

rather than obtaining general consent. Overall, the whole digital ecosystem can benefit from consumer trust on the one side and an enhanced data availability on the other side.

### 3.1 Request from the inquiring institution

A lack of transparency in privacy policies, e.g., through non-consumer-centered designs [CC15], is a fundamental barrier to achieving informed consent today [Ba22]. Consumers need to have a holistic view of the data activities to be able to give an informed consent. The first part of the consent registry is a standardized form that the inquiring institutions need to completely fill out to ensure a comprehensive request that can be displayed to the consumer (see Fig. 2). We carefully considered the trade-off between comprehensibility and exhaustiveness. For this reason, the form includes formalized, predetermined answers to increase the consumers’ comprehensibility and open-text fields for detailed information.



The form is titled "Form for requesting user data". It contains the following fields:

- Your name:
- Your institution type:
- Your business sector:
- Intended purpose:
- Description of the intended purpose:
- Type of data:
- Collection period: start:  end:
- Data retention period: start:  end:

Fig. 2: Inquiring institution’s view of the form for requesting consumer data

First, the inquiring institutions need to identify themselves. This is necessary, since only the exact entity that requested the data can use the data. Institutions should not place a request for a whole conglomerate but rather for the particular entity requiring this data. Prior studies show that the requester influences the consumers’ willingness to share data [Li17, WGW19]. This might, e.g., be due to familiarity and prior experiences with the inquiring institution, through which the consumers were able to build trust [Ro15, Wi16].

Further, consumers might have particular preferences for sharing data with different institution types. For example, consumers showed a higher willingness to share data for medical research compared to private companies [Mc16]. The inquiring institution needs to specify their type of institution, selecting from a set of predetermined options: (i) (private) research institute; (ii) university; (iii) private company; (iv) non-profit

organization; (v) governmental institution; and (vi) other [...]. The indication of different institution types gives consumers, that might not be familiar with specific business sectors, the possibility to gain a more general insight towards the organization.

To further ease the evaluation for consumers, the requester needs to specify their business sector. The institution's name alone might not be sufficient, since consumers might not be familiar with all actors in a digital ecosystem but may have specific preferences based on the business sector. Prior work highlights the importance of the business sector of the inquiring institution for consumers' willingness to share data [Ac21].

Further, the inquiring institution needs to specify the intended use of the requested data in a standardized form. The intended use of the data is crucial, since it significantly affects the consumers' willingness to share data [Ro15]. For instance, prior works have shown, that consumers might be more willing to share data for research purposes than for commercial usage [TLS17]. To facilitate the consumers' understanding, the inquiring institution needs to specify their intended use among predefined options for a first evaluation: (i) research; (ii) product development; (iii) artificial intelligence (AI) training; (iv) personalized marketing; (v) market research; and (vi) other [...]. In this way, consumers can form a general opinion towards specific purposes and can potentially easily understand the actual purpose compared to free text fields only.

To further enhance the consumers' understanding of the intended use of data, we added a particular field that details the intended use expanding the overall category of usage and describes in an easy-to-understand way how the inquiring institution will use the data. This additional information should enhance consumers' understanding of the general purpose behind the proposed use of their data.

The type of data is another relevant information for the consumers [Ha17]. For instance, the works of Marxen et al. [MFF24] have shown the importance and influence of the type of requested data on the willingness to share it. For this reason, the inquiring institution needs to define the type of the requested data. The type of data is deeply connected to the use case of the implementation of the consent registry and describes the type of data that is requested by the inquiring institution. For this reason, we deviate from the GDPR definition of categories of (personal) data (Art. 9 GDPR). To facilitate the comprehensibility for the consumers, the inquiring institution can only choose between predetermined options available in the particular digital ecosystem. In our case in the smart living domain (i) electricity consumption, (ii) water consumption and (iii) gas consumption data is available through the intermediary application that will implement the consent registry tool first within an initial case study before it is rolled out across the entire ecosystem, leading to more variety in available data types.

In addition, the inquiring institution needs to determine the collection period of the desired data: They need to state start and end dates of the targeted data. It enables the consumer to gain a clearer understanding of the volume of the requested data, thereby enabling a more informed consent, as the consumer is aware of the exact time period and extent of their data that they will share with the inquiring institution.

Further, the inquiring institution needs to specify the intended retention period of the desired data. The retention period is another crucial information, addressed, e.g., in the GDPR's right to be forgotten [Ko15]. Consumers need to be aware of the period during which the inquiring institution will handle the data, after they give the consent. This constitutes another critical piece of information that allows consumers to better assess the potential consequences of their consent.

### **3.2 Application provider as intermediary**

Within digital ecosystems, individuals frequently do not interact directly with institutions seeking their data, relying instead on third-party platforms and services for data storage and management. For this reason, the consent registry will not immediately forward a request to the consumers. In our concept, the application providers take the role of intermediaries. Previous research has underlined the focal role of application and service providers and their public role. For instance, service providers inherently have a gatekeeping function, to protect their users [TF17]. For this reason, our concept registry enables application providers to accept or decline every request before sending them to their users, thereby preserving their gatekeeping role. The application providers thereby keep the control over which institutions might gain access to user data of their platform, enabling them to protect their users from actors who may not align with core values of the application or actors which the users might perceive negatively, thereby potentially undermining trust between the users and the application providers. Additionally, the application providers are also able to protect their users from overwhelming amounts of requests by restricting too many requests from one inquiring institution. Furthermore, in the current state of our concept, application providers also act as arbitrators, e.g., by verifying whether the description of the intended purpose aligns with the selected intended purpose. A different institution in the ecosystem could potentially perform this function, depending on the implementation of the ecosystem, like a trust anchor that at least sporadically checks whether intended general purposes matches the free text description.

Administering each individual request separately might become an overwhelming and time-consuming task for the application providers, potentially resulting in imprecise management of requests or rejecting them and the consent registry in general. For this reason, the application provider has the option to determine rules about incoming requests when initially implementing the consent registry, thereby mitigating inappropriate requests (e.g., declining requests from private companies or particular intended purposes).

For instance, the application provider is able to predefine the general types of institutions that are allowed to send requests. They might deem certain types of institution inappropriate for requesting data from their users, e.g., permitting research institutions to submit requests while considering private companies unsuitable, as leveraging data for profit could conflict with their fundamental values. Application providers have the ability to prevent institutions they consider inappropriate from requesting data from their users.



Similar to the institution type, application providers have the ability to predetermine specific purposes. For instance, application providers might be opposed to data requests for marketing purposes, since this might affect the user's perception of the (own) application and could ultimately negatively influence trust in the application provider.

Further, application providers can predetermine which types of data institutions could request from their users. Our use case involves three types of usage data, whose confidentiality may be perceived similarly. However, the consent registry is supposed to be adapted to various different use cases with different types of data. For instance, in use cases that include wearable devices, the requested data might include movement profiles or health data. For this reason, the option to exclude requests for specific types of data might be particularly useful for use cases with data of varying sensitivity.

Application providers can determine different rules connected with Boolean operators to specify the use cases for data requests they would generally approve. This aspect of the consent registry limits the number of potentially unnecessary requests for application providers, since too many requests might burden them and ultimately lead to rejecting consent at all for any requests and the consent registry in general. Requests, that the application providers did not exclude still require their explicit approval to be sent to users, if desired, as the application provider may still consider certain requests inappropriate.

### 3.3 Request for the consumer

Finally, consumers receive data requests that the application providers deemed appropriate and can decide on a case-to-case basis which request they want to accept. To enable an informed consent, we follow two key goals: First, the consumer must receive complete information of the processing of their data. Second, the information needs to be presented to the consumer in a comprehensible format. To achieve the comprehensible format, we utilize the concept of progressive disclosure. Progressive disclosure describes the initial presentation of condensed information to the consumer to enable a quick overview of a certain topic [SW19]. The consumer only receives detailed information upon request. Researchers have applied the concept of progressive disclosure in various fields, including algorithmic transparency [SW19], explainable AI [Mu24] and education [HG18].

Drawing from the concept of progressive disclosure, we opted for the design displayed in Figure 3. We utilize the concept of privacy icons to facilitate the understanding of the key aspects of the request, expanding the icons with an additional description for enhanced clarity. The presented form contains four fields, extracting the data submitted by the inquiring institution via the request form and displaying it in a concise, streamlined format.

At first, the consumer will see four key information patterns of the request: (i) inquiring institution; (ii) intended purpose; (iii) type of data; and (iv) retention period. However, the consumer is able to expand the respective fields and receive additional information on demand, indicated by the plus next to each field (i.e., a progressive disclosure).

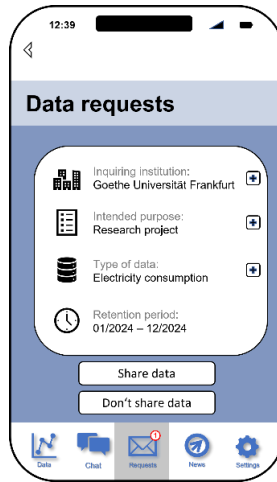


Fig. 3: Consumer's initial view of the request form

In its default state, the request form displays only the name of the institution to the consumer. This information on its own is sufficient to unambiguously identify the inquiring institution. However, if consumers are interested in additional information, they can expand this field and receive further information regarding the inquiring institution like the business sector and institution type (see Fig. 4a). This approach prevents consumers from being overwhelmed with unnecessary information if they are already familiar with the inquiring institution. If consumers are not familiar with the institution, they are able to easily access additional information to form an opinion. This could support and facilitate the decision process if consumers are not familiar with a particular institution but are generally willing to share data with organizations in this sector.

Initially, the consumer will only view the intended usage category of the data in the default form. This information is necessary for the consumers to be aware of the general intended use of the inquiring institution. Since the inquiring institution chooses among predetermined options, the consent registry offers a quick overview of the intended purpose to the consumer. This might facilitate an informed decision-making. However, the consumer is able to extend this field as well, receiving the detailed description of the intended purpose given by the inquiring institution in the request form (see Fig. 4b).

Since the type of the requested data is crucial information to the consumer, the consent registry immediately presents this information, along with the other three fields. The tool further displays information on the collection period of the requested data when the consumer expands this field. This information is crucial and should remain accessible to the consumer. However, to balance comprehensibility and exhaustiveness, we decided to present only the information on the type of data initially.

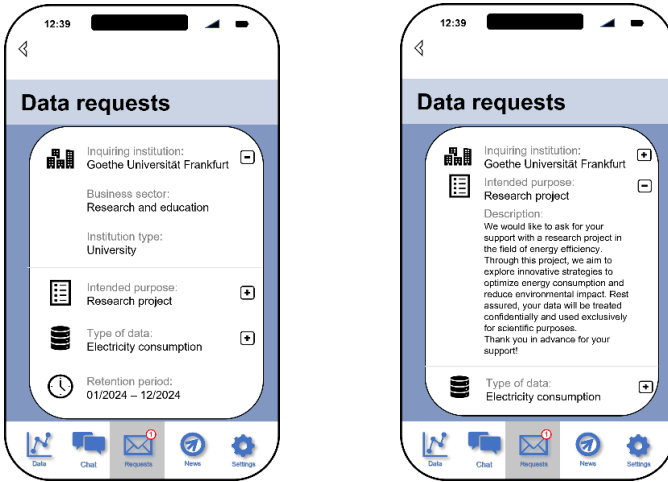


Fig. 4a and Fig. 4b: Expanded fields inquiring institution (4a, left) and intended purpose (4b, right)

The last information that the consent registry initially presents to the consumer is the retention period of the data. This information is another key aspect consumers need to be aware of to enable a comprehensive understanding of the implications of sharing data, thereby supporting the informed consent. It contains implications about the long-term effects of data sharing and should therefore be immediately visible to the consumer. This field, in the current form of the concept registry, does not include additional information and therefore the consumer is not able to expand this field.

Above all, this concept is supposed to enable an informed consent for consumers. On the one hand, it reduces and structures the given information to minimize the cognitive load and facilitate the understanding of the consequences of the consent to share data by employing a standardized form. On the other hand, consumers are able to access additional information, e.g., a comprehensive description of the intended use, in addition to a general classification, therefore allowing a comprehensively informed consent.

However, receiving individual requests could potentially burden consumers. Through the application providers' function as intermediaries, consumers will probably only receive a reduced amount of requests, thereby decreasing the cognitive load again. Future research could explore further approaches to limit the burden of requests for consumers even more, through, for instance, only presenting requests on a daily or weekly basis.

## 4 Conclusion and Outlook

The goal of our work is to sketch a tool to enhance consumer data sovereignty. Our concept encompasses three stakeholder groups involved in a data request: consumers producing

data, inquiring institutions desiring data access and application providers in a digital ecosystem as intermediaries with a certain responsibility toward their users. Our tool addresses the prevalent information asymmetries. While lawmakers have already addressed this issue with legislative measures, prior investigations indicate that they might not be sufficient to enable an informed consent for consumers [Ef19, Ba22]. While concepts such as privacy icons and one-page solutions aim to empower consumers, they also have notable shortcomings. We address this issue by building on these concepts and combining them with progressive disclosure, offering consumers an initially simplified request while providing the option to access additional information on demand. Our tool facilitates the consumers' exercise of power proposed by legislative measures like the GDPR and thereby helps strengthen consumer data sovereignty. The presented concept is applicable to various different use cases, encompassing various data types across different industries. The developed tool could potentially enhance data handling transparency by presenting the individual requests to the consumer in a more comprehensible format. We specifically positioned our exemplary use case within the context of a digital ecosystem, as such environments in particular may lead to consumers not being aware of who might have access to their data and the potential consequences of such data sharing. Yet, the consent registry can not only be applied in digital ecosystems, but also in single applications as well. The consent registry therefore represents another step towards enabling informed consent and enhancing consumer data sovereignty while also promoting (responsible) data sharing and addressing data silos. Its applicability to different digital ecosystems and use cases should support widespread adoption in practice.

Future research could consider the validation of the consent registry with consumers in real-world scenarios to test its effectiveness and consumer acceptance. We will contribute to this initial evaluation by implementing our proposed concept in a case study and testing the concept with consumers in a digital ecosystem in the context of smart living appliances. In real-world application, we will further develop the tool and implement changes as needed. For instance, if the consumers prefer it, we might implement the possibility to disclose data in bulks, rather than limiting the disclosure to individual datasets. Additionally, we might limit the retention period by only allowing requests with a retention period that does not exceed a certain time. However, the priority of consumer data sovereignty will remain in our tool and thus changes must not compromise this objective. Another important avenue for future research is ensuring that companies adhere to their stated purpose of data usage. The current consent registry does not guarantee this, but addressing it is crucial for fostering user trust.

## **Acknowledgement**

The project COMET is funded by the Federal Ministry for Economic Affairs and Climate Action (BMWK) as part of the technology program "SmartLivingNEXT – Artificial Intelligence for Sustainable Living Environments." SmartLivingNEXT is creating a universal, AI-based ecosystem for the simple and cost-effective development of intelligent and sustainability-oriented smart living services and applications.

## Bibliography

- [Ac21] Ackermann, K.; Miesler, L.; Mildenerger, T.; Frey, M.; Bearth, A.: Willingness to share data: Contextual determinants of consumers' decisions to share private data with companies. In: *Journal of Consumer Behaviour* 21, pp. 375–386, 2021
- [AKR22] Andreotta, A. J.; Kirkham, N.; Rizzi, M.: AI, big data, and the future of consent. In: *AI & SOCIETY* 37, pp. 1715–1728
- [Ba22] Bahrini, M.; Zargham, N.; Wolff, A.; Kipker, D.K.; Sohr, K.; Malaka, R.: It's Long and Complicated! Enhancing One-Pager Privacy Policies in Smart Home Applications. In: *Nordic Human-Computer Interaction Conference '22.*, pp. 1–13, 2022
- [BC11] Bélanger, F.; Crossler, R. E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. In: *MIS Quarterly* 35, pp. 1017–1041, 2011
- [Ca21a] Calzada, I.: Data Co-Operatives through Data Sovereignty. In: *Smart Cities* 4, 1158–1172, 2021[Ca21b] Carl, K. V.: Corporate Digital Responsibility: Evaluating Privacy and Data Security Activities on Company-level. In: *INFORMATIK* 2021, pp. 757–771, 2021
- [Ca22a] Calzada, I.: Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). In: *Smart Cities* 5, 1129–1150, 2022
- [Ca22b] Carl, K. V.: The status-quo of companies' data privacy and security communication: An ethical evaluation and future paths. In: *INFORMATIK* 22, pp. 195–206, 2022
- [CC15] Capistrano, E. P. S.; Chen, J. V.: Information privacy policies: The effects of policy characteristics and online experience. In: *Computer Standards & Interfaces* 42, pp. 24–31, 2015
- [CH24] Carl, K. V.; Hinz, O.: What we already know about corporate digital responsibility in IS research: A review and conceptualization of potential CDR activities. In: *Electronic Markets* 34, pp. 1–30, 2024
- [CM22] Custers, B.; Malgieri, G.: Priceless data: why the EU fundamental right to data protection is at odds with trade in personal data. In: *Computer Law & Security Review* 45, 2022
- [Ef19] Efroni, Z.; Metzger, J.; Mischau, L.; Schirmbeck, M.: Privacy Icons: A Risk-Based Approach to Visualisation of Data Processing. In: *European Data Protection Law Review* 5, pp. 352–366, 2019
- [Gr24] Grafenstein, M.; Kiefaber, I.; Heumüller, J.; Rupp, V.; Graßl, P.; Kolless, O.; Puzst, Z.: Privacy icons as a component of effective transparency and controls under the

- GDPR: effective data protection by design based on art. 25 GDPR. In: *Computer Law & Security Review* 52, 2024
- [Ha17] Haeusermann, T.; Greshake, B.; Blasimme, A.; Irdam, D.; Richards, M.; Vayena, E.: Open sharing of genomic data: Who does it and why? In: *PLOS ONE* 12, 2017
- [He25] Hering, F.; Hinz, O.; Pfeiffer, J.; Aalst, W. van der: The Damocles Sword of Cyber Attacks - A Call for Information Systems Security. In: *Business & Information Systems Engineering* 67, forthcoming, 2025
- [HG18] Howard, M. L.; Gaviola, M. L.: Progressive disclosure cases: The design and evaluation of use in multiple therapeutics courses. In: *Currents in Pharmacy Teaching and Learning* 10, pp. 723–729, 2018
- [Hu21] Hummel, P.; Braun, M.; Tretter, M.; Dabrock, P.: Data sovereignty: A review. In: *Big Data & Society* 8, pp. 1–17, 2021
- [JB24] Jøranli, I.; Breunig, K. J.: Unlocking data’s potential: navigating the challenges of data-driven innovation for start-ups. In: *Measuring Business Excellence* 28, pp. 334–346, 2024
- [JLL21] Jelovac, D.; Ljubojević, Č.; Ljubojević, L.: HPC in business: the impact of corporate digital responsibility on building digital trust and responsible corporate digital governance. In: *Digital Policy, Regulation and Governance* 24, pp. 485–497, 2021
- [KKS20] Korunovska, J.; Kamleitner, B.; Spiekermann-Hoff, S.: The challenges and impact of privacy policy comprehension. In: *Twenty-Eighth European Conference on Information Systems 2020*, pp. 1–17, 2020
- [Ko17] Kokolais, S.: Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. In: *Computers & Security*, 64, pp. 122–134, 2017
- [Ko15] Korenhof, P.; Ausloos, J.; Szekely, I.; Ambrose, M.; Sartor, G.; Leenes, R.: Timing the Right to Be Forgotten: A Study into “Time” as a Factor in Deciding About Retention or Erasure of Data. In: (Gutwirth, S., Leenes, R., de Hert, P. eds.) *Reforming European Data Protection Law*, pp.171–201, 2015
- [Li17] Li, Y.; Kobsa, A.; Knijnenburg, B.; Nguyen, C.: Cross-Cultural Privacy Prediction. In: *Proceedings on Privacy Enhancing Technologies* 2017, pp. 113–132, 2017
- [Lo24] Long, Y.; Luo, X.; Zhu, Y.; Lee, K. P.; Wang, S. J.: Data Transparency Design in Internet of Things: A Systematic Review. In: *International Journal of Human–Computer Interaction* 40, pp. 5003–5025, 2024
- [LYH19] Li, H.; Yu, L.; He, W.: The Impact of GDPR on Global Technology Development. In: *Journal of Global Information Technology Management* 22, pp. 1–6, 2019

- [Mc16] McCormack, P.; Kole, A.; Gainotti, S.; Mascalzoni, D.; Molster, C.; Lochmuller, H.; Woods, S.: „You should at least ask“. The expectations, hopes and fears of rare disease patients on large-scale data and biomaterial sharing for genomics research. In: *European Journal of Human Genetics* 24, pp. 1–6, 2016
- [MF16] Mittelstadt, B.D., Floridi, L.: The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. In: *Science and Engineering Ethics* 22, pp. 303–341, 2016
- [MFF24] Marxen, H.; Frank, M.; Fridgen, G.: The Role of Gender in Data Sharing for Smart Charging of Electric Vehicles. In: *AMCIS 2024 Proceedings*, 2024
- [Mi22] Mihale-Wilson, C.; Hinz, O.; Aalst, W. van der; Weinhardt, C.: Corporate Digital Responsibility. In: *Business & Information Systems Engineering* 64, pp. 127–132, 2022
- [Mu24] Muralidhar, D.: The Effect of Progressive Disclosure in the Transparency of Explainable Artificial Intelligence Systems. In: *2024 IEEE Symposium on Visual Languages and Human-Centric Computing*, pp. 382–383, 2024
- [PAZ22] Podgorelec, B.; Alber, L.; Zefferer, T.: What is a (digital) identity wallet? A systematic literature review. In: *IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC) 2022*, pp. 809–818, 2022.
- [Ro15] Roeber, B.; Rehse, O.; Knorrek, R.; Thomsen, B.: Personal data: how context shapes consumers’ data sharing with organizations from various sectors. In: *Electronic Markets* 25, pp. 95–108, 2015
- [RP20] Rossi, A.; Palmirani, M.: Can Visual Design Provide Legal Transparency? The Challenges for Successful Implementation of Icons for Data Protection. In: *Design Issues* 36, pp. 82–96, 2020
- [RS18] Renaud, K.; Shepherd, L. A.: How to Make Privacy Policies both GDPR-Compliant and Usable. In: *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment*, pp. 1–8, 2018
- [SE24] Schramm, J.; Eichinger, T.: Towards Building GDPR-Friendly Consent Management Systems on Top of Self-Sovereign Identity Ecosystems. In: (Roßnagel, H.; Schunck, C. H.; Sousa, F. eds.) *Open Identity Summit 2024*, pp. 93–102, 2024
- [Sm25] SmartLivingNEXT, <https://smartlivingnext.de/en/>, accessed:14/04/2025
- [SW19] Springer, A.; Whittaker, S.: Progressive disclosure: empirically motivated approaches to designing effective transparency. In: *Proceedings of the 24th International Conference on Intelligent User Interfaces*, pp. 107–120, 2019
- [TF17] Taddeo, M., Floridi, L.: The Moral Responsibilities of Online Service Providers. In: (Taddeo, M., Floridi, L. eds.) *The Responsibilities of Online Service Providers*. Law,

Governance and Technology Series, 31, pp. 13-42, 2017.

- [TLS17] Thiebes, S.; Lyytinen, K.; Sunyaev, A.: Sharing is About Caring? Motivating and Discouraging Factors in Sharing Individual Genomic Data. In: ICIS 2017 Proceedings, pp. 15, 2017
- [Tr23] Trier, M.; Kundisch, D.; Beverungen, D.; Müller, O.; Schryen, G.; Mirbabaie, M.; Trang, S.: Digital Responsibility. In: Business & Information Systems Engineering 65, pp. 463-474, 2023
- [VT21] Viktoratos, I.; Tsadiras, A.: Personalized Advertising Computational Techniques: A Systematic Literature Review, Findings, and a Design Framework. In: Information 12, 2021
- [Wa20] Waerdt, P. J. van de: Information asymmetries: recognizing the limits of the GDPR on the data-driven market. In: Computer Law & Security Review 38, 2020
- [WGW19] Wessels, N.; Gerlach, J.; Wagner, A.: To Sell or not to Sell – Antecedents of Individuals' Willingness-to-Sell Personal Information on Data-Selling Platforms. In: ICIS 2019 Proceedings, 2019
- [Wi16] Wieneke, A.; Lehrer, C.; Zeder, R.; Jung, R.: PRIVACY-RELATED DECISION-MAKING IN THE CONTEXT OF WEARABLE USE. In: PACIS 2016 Proceedings, 2016
- [Wi22] Windl, M.; Ortloff, A.-M.; Henze, N.; Schwind, V.: Privacy at a Glance: A Process to Learn Modular Privacy Icons During Web Browsing. In: Proceedings of the 2022 Conference on Human Information Interaction and Retrieval '22, pp. 102–112, 2022