RESPECTeD-IoT
Really Enforceable Solution to Protect End-users Consent Decisions in IoT

Soheil Human
soheil.human@wu.ac.at

Endbericht | Call 16 | Projekt ID 5937

1 Introduction

Privacy, and with it the protection of personal data, stands as a fundamental human right, integral to preserving individual dignity and autonomy. To uphold this right, individuals must not only understand the ways in which their personal data is collected but also have the ability to control its usage and sharing with third parties. While some progress has been made in empowering users to manage their data on the web, these efforts remain far from satisfactory. Even so, the web offers a comparatively more developed framework than the domain of Internet of Things (IoT) devices, where the lack of standardized mechanisms for human-compatible digital protection communication leaves significant concerns unresolved. The diverse technological architectures and frameworks defining IoT systems further compound these challenges.

This challenge is particularly pressing as IoT devices have become pervasive, encompassing technologies such as smart home systems, wearable devices, public surveillance networks, and Wi-Fi access points. These devices often gather and process personal data without offering users effective mechanisms to manage their consent or privacy preferences. This lack of consistency in implementing privacy controls creates significant hurdles for compliance with data protection regulations, particularly the European Union's General Data Protection Regulation (GDPR), which mandates that consent must be explicit, informed, specific, and freely provided.

The project aimed to tackle these issues by introducing a comprehensive framework based on the *Advanced Data Protection and Control (ADPC)* protocol, specifically designed to meet the demands of IoT ecosystems. The framework included a mobile application equipped with *Bluetooth Low Energy (BLE)* capabilities, enabling users to assert their digital rights by managing consent and privacy decisions, including receiving information and requests, and granting, withdrawing, or modifying permissions. To improve user accessibility and provide tailored guidance, the application incorporated a P*ersonal Digital Protection, Consenting and Controlling Assistant system (PDPCAS)* powered by Artificial Intelligence (AI). Additionally, a server-side implementation using *ESP32 hardware* facilitated seamless interaction between the mobile application and IoT devices, delivering a holistic approach to privacy and digital rights management.

Through the development and evaluation of a working prototype, the project sought to demonstrate the feasibility and effectiveness of a scalable, user-friendly solution for digital protection management within IoT environments. Comprehensive usability assessments and technical validation underpinned the effort to provide a robust model that aligned with regulatory requirements while addressing the practical challenges of IoT ecosystems, fostering a digital-rights-and-privacy-first approach in the digital age.

2 Project Description

The project was focused on addressing the complex and multifaceted challenges associated with digital protection and consent management in IoT environments. It integrated technical, legal, and human-compatible dimensions to propose a comprehensive solution. Conducted by the Sustainable Computing Lab, a group dedicated to advancing equitable digital rights through interdisciplinary research and development, the project aimed to empower users by enhancing their control and agency over personal data within the rapidly expanding ecosystem of IoT technologies.

The central achievement of the project was the development of the *ADPC-IoT (Advanced Data Protection and Control for IoT)*, a specialized technical specification designed to meet the unique demands of IoT systems. Building upon the existing ADPC framework, ADPC-IoT formalizes the processes involved in the communication of privacy-related data, information, requests, and decisions between IoT devices, such as sensors or other connected hardware, and a mobile application. This specification addresses the lack of standardized methods for privacy management in IoT environments by enabling streamlined, user-friendly interactions that support informed decision-making about data protection and consent.

The project delivered functional prototypes as a proof of concept, which included a mobile application developed for both iOS and Android platforms. This application utilized *Bluetooth Low Energy (BLE)* technology and web-based solutions to facilitate real-time data interactions between users, as data subjects, and data controllers responsible for managing IoT systems. To complement the mobile application, a server-side script for ESP32 hardware was implemented, enabling seamless communication between IoT devices and the application. This combination of technologies provided a holistic system for managing data protection and consent across diverse IoT environments, ensuring compatibility with various device architectures and operational contexts.

The project identified two primary stakeholder groups as its beneficiaries: *data subjects*, who interact with IoT devices in various capacities, and *data controllers*, who are tasked with overseeing and ensuring compliance of IoT systems with data protection regulations. For *data subjects*, the ADPC-IoT framework offers an unprecedented level of transparency and control, enabling them to actively manage their digital rights by granting, modifying, or revoking consent (and other digital protection decisions) as needed. For *data controllers*, the framework provides a robust and practical tool to align their systems with contemporary data protection laws, including the General Data Protection Regulation (GDPR). This alignment not only enhances regulatory compliance but also helps maintain user trust by demonstrating a commitment to privacy-first practices, while simultaneously improving user experience through intuitive and transparent data management mechanisms.

Recognizing the broader impact of these developments, the project also aimed to provide developers and system architects with a foundational technical framework to facilitate the creation of privacy-respecting IoT applications. By offering standardized and human-compatible tools, ADPC-IoT lowers the barriers to innovation in the realm of digital protection while ensuring that such innovations remain aligned with human-centric and regulatory requirements.

A notable feature of the project was the integration of Artificial Intelligence (AI), with a particular emphasis on generative AI, to further support the dynamic and adaptive management of digital protection and consent. This effort culminated in the creation of a *Personal Digital Protection, Consenting and Controlling Assistant System (PDPCAS)*, an AI-powered module embedded within the mobile application. PDPCAS provided personalized, context-aware support to users, empowering them to navigate complex privacy decisions with ease. This system was particularly valuable for users with limited technical knowledge, ensuring accessibility and inclusivity in privacy management.

To evaluate the effectiveness of the proposed solutions, the project conducted a comprehensive user study. This study assessed the usability, functionality, and overall impact of the ADPC-IoT framework and its associated tools. The results validated the approach, demonstrating that the system effectively empowered users to exercise their digital rights while aiding data controllers in addressing the legal, technical, and ethical challenges of privacy management in IoT ecosystems.

By addressing the intersection of technology, law, and user experience, the project sets a new standard for privacy management in IoT environments. It highlights the critical importance of creating standardized, scalable, and human-compatible solutions that not only meet regulatory demands but also foster trust and transparency in an increasingly interconnected digital landscape. This work lays the foundation for future advancements in digital protection and emphasizes the need for ongoing innovation to address the evolving challenges of IoT ecosystems.

3 Workpackages

3.1 Workpackage 1 – Project Management

Work Package 1 focused on the comprehensive management of the project, encompassing both the initial formalities and the final documentation and reporting. This included the planning, monitoring, and administrative tasks required to ensure the smooth execution of the project and adherence to the funding requirements.

At the project start, the following tasks were undertaken: the project contract was reviewed, signed in duplicate, and submitted to the funding body via registered mail. A detailed project plan, based on a provided Excel template, was created and approved, outlining the tasks and deliverables for all work packages. Additionally, a detailed list of project deliverables, including their licensing

terms and locations for public availability, was prepared and approved. The project website was launched, with an initial blog post introducing the project.

At the project conclusion, significant emphasis was placed on ensuring the proper documentation and dissemination of results. All planned deliverables, as outlined in the project results worksheet, were finalized, functional, and accompanied by sufficient documentation. The project website was updated one final time, ensuring that all deliverables were made publicly available under the specified open-source or Creative Commons licenses. The final project report, including a summary and final financial statements, was submitted and approved. The process concluded with the submission of an application for the final funding installment and the publication of a closing blog post summarizing the project outcomes.

This work package ensured that the project adhered to all administrative and formal requirements while facilitating transparency and accessibility through detailed documentation and the public dissemination of results.

3.2 Workpackage 2 - Technical Specification Adaptation and Development

Work Package 2 focused on the development and refinement of the ADPC-IoT specification, adapting the existing ADPC framework to address the specific challenges and requirements of IoT environments. The goal was to create a standardized approach to facilitate privacy management and consent communication within the diverse and complex IoT ecosystem.

The first phase of this work package involved drafting a preliminary version of the specification. This initial draft was designed to integrate the foundational principles of the ADPC framework while accounting for the unique technical and operational constraints of IoT devices, such as limited computational resources, diverse communication protocols, and the need for user-friendly interfaces. The draft specification outlined the mechanisms for enabling seamless interaction between users, IoT devices, and data controllers, ensuring compliance with privacy regulations.

Following the development of the draft, the specification underwent a rigorous evaluation process, incorporating feedback from technical validation activities conducted within the project. These evaluations tested the practicality, efficiency, and scalability of the specification in real-world IoT scenarios.

The final phase of Work Package 2 was the completion of the specification, which integrated insights and improvements derived from the evaluation process. The finalized specification was documented. By adapting and refining the ADPC framework for IoT, this work package delivered a robust and standardized technical specification, forming the backbone of the project's broader efforts to enhance privacy management in the IoT domain.

3.3 Workpackage 3 – Implementation

Work Package 3 focused on the software engineering and implementation tasks necessary to realize the proposed ADPC-IoT specification in a tangible and functional form. The objective was to develop proof-of-concept (PoC) software for both the client-side and IoT device-side components, showcasing the feasibility and practicality of the ADPC-IoT framework.

The first deliverable of this work package was the development of a client-side application. This software was designed to operate in alignment with the ADPC-IoT specification, enabling users to interact with IoT devices and manage their privacy seamlessly. The client application served as the interface through which users could view and modify their consent and privacy preferences, receive requests for data access, and exercise their rights over personal data. Built as a proof-of-concept, this application demonstrated the core functionalities required for human-compatible privacy management in IoT ecosystems.

The second deliverable involved the development of a server-side software module for IoT devices. This software was created to integrate directly with IoT hardware, facilitating the communication and implementation of the ADPC-IoT specification. The module ensured that IoT devices could interpret and respond to user commands, process consent-related interactions, and maintain compliance with privacy requirements. The server-side software also provided the technical backbone for secure and efficient data communication between devices and the client application.

Both software components were designed and implemented as proofs of concept to validate the ADPC-IoT framework's applicability in real-world scenarios. Together, they demonstrated the end-to-end functionality of the specification, from user interaction to device-level execution.

This work package provided the foundational software artifacts necessary for evaluating and refining the ADPC-IoT specification, advancing the project's aim of delivering practical and scalable solutions for privacy management in IoT environments.

3.4 Workpackage 4 – Evaluation

Work Package 4 focused on the systematic evaluation of the outputs from the preceding work packages to ensure the effectiveness, reliability, and applicability of the developed solutions. The objective was to assess the developed ADPC-IoT specification as well as the client-side and server-side software components through comprehensive testing and expert/user feedback.

The evaluation process began with a detailed analysis of the ADPC-IoT specification. This involved examining the specification's ability to address the unique challenges of IoT environments, such as technical heterogeneity, limited device capabilities, and compliance with privacy regulations. The evaluation aimed to validate the specification's scalability, interoperability, and alignment with user-centric privacy management principles. Feedback gathered from these assessments informed recommendations for further improvements.

The next phase involved the evaluation of the client-side application and the server-side module. The client-side software was tested for usability, functionality, and its effectiveness in enabling users to exercise control over their data and manage consent preferences. The server-side module was evaluated for its compatibility with IoT hardware, its ability to process and implement consent requests, and its overall performance within the IoT ecosystem. Together, these assessments demonstrated how the software components worked cohesively to operationalize the ADPC-IoT framework.

This work package was instrumental in validating the project outcomes, providing a solid foundation for future developments and ensuring the project's contributions are both practical and impactful.

3.5 Workpackage 5 – Dissemination

Work Package 5 focused on the dissemination activities of the project, ensuring that the results and insights reached both technical and academic audiences while promoting transparency and accessibility. This work package involved maintaining a strong online presence, producing project documentation, and contributing to academic discourse.

A significant activity within this work package was the maintenance of the project website and weblogs. The website served as the central hub for disseminating project updates, deliverables, and findings to the public. Regular weblog posts were created to share progress, key milestones, and final results, ensuring continuous engagement with the broader community. This online platform also provided a repository for all publicly available project outputs, including open-source code and documentation, in accordance with the licensing terms defined in the project plan.

Another key task was the development of project documentation tailored to different stakeholder groups. These documents included technical manuals for developers, user guides for end-users, and detailed descriptions for data controllers to facilitate the implementation and integration of the ADPC-IoT framework. Each document was designed to address the specific needs of its audience, ensuring clarity and usability across diverse contexts.

Additionally, academic writing was a core component of this work package. The project's findings and innovations were prepared for submission to peer-reviewed journals and conferences, contributing to the academic dialogue on privacy management in IoT environments. These publications aimed to share the technical advancements, evaluation outcomes, and theoretical underpinnings of the project, further extending its impact within the scientific community.

This work package ensured that the project results were effectively communicated and made accessible to all relevant audiences. By engaging both technical and academic communities, it maximized the reach and applicability of the project's outcomes, fostering continued research, collaboration, and innovation in the field of IoT privacy management.

4 List of Project Results

1	Project Interim Report	*NA*	*NA*
2	Project summary	*CC-BY-Sharelike*	*https://www.netidee.at/respected-iot*
3	*Documentations for developers*	*MPL-2.0 license*	*https://github.com/Data-Protection-Control*
4	*Documentations for users*	*MPL-2.0 license*	*https://github.com/Data-Protection-Control*
5	*Project Summary*	*CC-BY-Sharelike*	*https://www.netidee.at/respected-iot*
6	*Documentation of external communication to achieve visibility/sustainability*	*CC-BY-Sharelike*	*A section of final report, https://www.netidee.at/respected-iot*
7	*ADPC IoT Mobile App*	*MPL-2.0 license*	*https://github.com/Data-Protection-Control*
8	*ADPC-IoT-Server-side*	*MPL-2.0 license*	*https://github.com/Data-Protection-Control*
9	*ADPC-IoT Technical Specification*	*MPL-2.0 license*	*https://github.com/Data-Protection-Control*

5 Application of Project Results in Practice

The results of this project address the pressing need for effective privacy management in the increasingly pervasive ecosystem of IoT systems. As IoT devices become integral to daily life—spanning applications in smart homes, wearable technology, public infrastructure, and industrial settings—the importance of robust data protection mechanisms cannot be overstated. The ADPC-IoT specification and associated tools developed in this project provide a scalable, standardized solution to meet these challenges.

The ADPC-IoT framework equips organizations with the means to align their IoT systems with data protection regulations, such as the GDPR, by embedding privacy-aware features into their operations. Data controllers can leverage this framework to ensure transparent, user-friendly consent management, enabling end-users to exercise greater control over their personal data. This capability is particularly significant in addressing the trust deficit often associated with the widespread deployment of IoT technologies.

The client-side application serves as a model for empowering users to manage their digital rights in IoT ecosystems. By enabling seamless interaction with IoT devices, the application offers a practical tool for real-world scenarios, allowing users to grant, withdraw, or modify consent and

privacy decisions dynamically. This capability fosters a sense of agency and trust in environments where data collection is often ubiquitous and non-transparent.

On the IoT device side, the server-side module provides manufacturers and operators with a practical solution to embed privacy-compliant functionalities directly into their devices. This ensures that IoT systems are not only capable of processing user preferences but also of integrating with larger, privacy-respecting ecosystems.

Moreover, the open-source nature of the deliverables and accompanying documentation ensures that these solutions are accessible to developers, innovators, and organizations of varying scales. By providing a blueprint for implementing human-compatible digital protection, the project outcomes promote broader adoption of privacy-aware practices across the diverse IoT landscape.

As IoT systems continue to proliferate, the implementation of the ADPC-IoT framework and tools will play a pivotal role in safeguarding individual rights while enabling technological progress. These outcomes are not only timely but also essential for creating a future where IoT technologies coexist with robust privacy protections.

6 Dissemination

The project placed significant emphasis on public outreach and networking to maximize the impact and visibility of its outcomes while fostering collaboration across various sectors. Several activities have already been carried out, and additional efforts are planned to ensure continuous engagement with key stakeholders and the wider community.

Completed Outreach and Networking Activities:

- **Project Website and Weblogs**: The project website was established as a central platform for disseminating information about the project. Regular weblog entries were published to provide updates on milestones, deliverables, and key findings, ensuring transparency and public accessibility.
- **Presentations and Events**: The project team actively participated in conferences, workshops, and seminars to present the ADPC-IoT framework and its applications. These events provided an opportunity to engage with both academic and industry audiences, fostering dialogue and generating interest in the project's contributions.
- **Collaboration with Stakeholders**: Connections were established with key stakeholders in the IoT and data privacy sectors, including industry leaders, academic researchers, and policymakers. These interactions facilitated the exchange of insights and feedback, which were instrumental in refining the project outcomes.
- **Open-Source Contributions**: To support the open dissemination of results, all project deliverables, including the technical specifications, code, and documentation, were made

available under open-source licenses. This approach encourages adoption and further development by external developers and organizations.

- **Academic Dissemination**: Scholarly articles based on the project outcomes have been prepared for submission to peer-reviewed journals and conferences. These contributions aim to advance academic discussions on privacy management and IoT technologies while showcasing the innovative aspects of the ADPC-IoT framework.

Planned Outreach and Networking Activities:

- **Workshops and Expert Panels**: The organization of workshops and expert panels is planned to facilitate in-depth discussions about the ADPC-IoT framework and its potential applications. These sessions will target developers, policymakers, and privacy advocates, promoting broader adoption and collaboration.
- **Partnership Building**: Efforts are ongoing to establish long-term partnerships with industry players, academic institutions, and regulatory bodies. These partnerships aim to ensure the continued development and application of the ADPC framework across different sectors.
- **Public Awareness Campaigns**: Outreach campaigns are planned to raise public awareness about the importance of privacy management in IoT environments. These campaigns will utilize social media, blogs, and other digital channels to communicate the practical benefits of the ADPC-IoT framework.
- **Continued Academic Contributions**: Additional academic publications are in preparation to share further insights and advancements from the project. These will focus on emerging applications of the framework, such as in sustainable buildings and immersive technologies.

By combining these completed and planned activities, the project aims to ensure the sustained impact and relevance of its outcomes while fostering a collaborative ecosystem that supports innovation in privacy management and IoT systems.

7 Project Websites

- https://www.netidee.at/respected-iot
- https://www.dataprotectioncontrol.org
- https://github.com/Data-Protection-Control
- https://www.sustainablecomputing.eu

8 Planned Activities After the End of the Netidee Project

The sustainability and ongoing development of the ADPC framework remain a core focus beyond the conclusion of the *netidee RESPECTeD-IoT project*. Efforts are currently underway to extend the ADPC framework to address emerging digital ecosystems, with particular attention to mixed and augmented reality (MR/AR) environments. As these immersive technologies gain prominence in both consumer and industrial applications, the adaptation of the ADPC framework to such contexts ensures its relevance and capability in tackling the unique privacy and data protection challenges posed by MR/AR platforms. This expansion aims to establish robust mechanisms for user control and transparency in increasingly interactive and immersive digital spaces.

In parallel, significant attention is being directed toward applying ADPC-IoT within the domain of sustainable and smart buildings. These infrastructures, often equipped with interconnected IoT devices for energy management, security, and user comfort, present substantial challenges for data privacy. By integrating the ADPC-IoT framework into sustainable infrastructure, the project seeks to enhance privacy management and data protection in smart environments, ensuring compliance with regulatory standards while fostering trust among users. This application represents a critical step in demonstrating the framework's adaptability and value in large-scale, real-world deployments.

To support these initiatives, extensive efforts are being made to engage a wide array of stakeholders, including industry leaders, academic institutions, and policy-making entities. The aim is to foster a collaborative community around the ADPC framework, facilitating its growth and implementation across diverse sectors. By establishing strategic partnerships, the project team seeks to drive innovation, ensure the framework's scalability, and enable its adoption in various domains, ranging from IoT and smart infrastructure to extended reality environments.

Furthermore, to contribute to academic and professional discourse, several scholarly publications detailing the ADPC framework and its applications are currently being prepared and reviewed. These publications aim to disseminate the findings from the project, highlight the framework's potential in addressing privacy challenges, and stimulate further research in the fields of digital protection, IoT, and immersive technologies.

Beyond these immediate goals, the continuous evolution of the ADPC framework is guided by the need to respond proactively to emerging technological trends and societal demands for greater digital privacy and user empowerment. By fostering innovation, collaboration, and knowledge exchange, these efforts ensure that the ADPC framework remains a cutting-edge tool for privacy management, adaptable to the ever-changing digital landscape and aligned with the needs of diverse stakeholders.

9 Suggestions for Further Developments by Third Parties

The ADPC framework provides extensive opportunities for third-party utilization and further innovation, making it a versatile foundation for advancing privacy and data protection across diverse domains. Its flexible and modular architecture allows adaptation and extension into a wide range of industries and technological contexts.

Third parties are encouraged to explore integrating ADPC into additional IoT environments, particularly in sectors such as healthcare, smart cities, and autonomous systems, where the protection of sensitive data and ensuring user control are of paramount importance. In healthcare, ADPC can strengthen the privacy of patient records and consent management for data sharing. For smart cities, it can enable privacy-preserving services in public infrastructure, transportation systems, and urban planning. In autonomous systems, including robotics and vehicles, ADPC can enhance user trust by ensuring secure and transparent data interactions.

The extension of ADPC into mixed and augmented reality (MR/AR) also represents a significant opportunity for developers and innovators working in immersive digital technologies. These environments pose unique challenges to privacy, given their highly interactive and data-rich nature. By embedding ADPC into MR/AR platforms, third parties can improve digital protection standards, bolster user trust, and meet evolving regulatory requirements in these cutting-edge fields.

Another promising avenue lies in the application of ADPC to sustainable and smart infrastructure, including building management systems, energy-efficient solutions, and green technologies. The integration of ADPC into these systems can ensure that privacy is an inherent part of the design, addressing data security concerns in smart environments and supporting broader sustainability goals. By embedding robust privacy mechanisms, ADPC can contribute to a future where technological advancement aligns seamlessly with user rights and ethical considerations.

Beyond technological applications, third parties have the opportunity to advance the standardization and regulatory alignment of ADPC. Collaboration with policymakers, regulatory authorities, and standards organizations to formalize ADPC as an established framework for digital protection could significantly increase its adoption and influence. This formalization would also provide a unified approach to privacy management across industries, streamlining compliance and enhancing interoperability.

Academic researchers are similarly encouraged to build upon the ADPC framework, exploring new theoretical paradigms and practical use cases that align with the evolving landscape of digital protection. Areas such as ethical AI, data sovereignty, and user-centric design in IoT and immersive environments present rich opportunities for academic inquiry and development.

In summary, the ADPC framework offers a robust and adaptable foundation for third-party initiatives across technology, regulation, and research. Whether through advancing privacy in critical sectors, enabling compliance in new digital environments, contributing to standardization, or expanding theoretical understanding, ADPC provides a pathway for innovation that prioritizes user empowerment and data protection.

10 External Communication to achieve Visibility/Sustainability

Future external communication efforts will focus on enhancing the visibility and ensuring the long-term sustainability of the ADPC framework across diverse sectors. Plans include expanding the project's digital presence through the project website and social media platforms, with a continued emphasis on sharing insights, technical updates, and success stories from implementations. The organization of targeted workshops, participation in international conferences, and collaboration with industry events will further elevate the ADPC framework's profile, showcasing its applicability in IoT, MR/AR, and sustainable infrastructure. Open-source dissemination will remain central to these efforts, ensuring that developers, organizations, and stakeholders can access and utilize the framework, thereby fostering innovation and broader adoption.

Sustainability will be reinforced through building long-term partnerships with industry leaders, academic institutions, and policymakers. These collaborations will focus on integrating the ADPC framework into real-world applications and aligning it with emerging regulatory standards. Planned expert consultations and multi-stakeholder forums will create opportunities to refine and expand the framework, ensuring its relevance in evolving digital landscapes. Efforts will also be directed toward formalizing ADPC as a recognized privacy management standard, advocating its adoption in legislative and policy frameworks. Concurrently, ongoing academic contributions, including publications and collaborative research projects, will ensure the framework remains a cornerstone of discussions on privacy and data protection, securing its role in addressing future challenges.

Over the past several years, our team has been dedicated to advancing research and development in the field of privacy and digital protection, with a strong emphasis on creating solutions that prioritize human compatibility. This work reflects our commitment to designing digital protection mechanisms that align with user needs, rights, and expectations in an increasingly complex digital landscape. The following bibliography provides an overview of the foundational research that underpins the ADPC framework, illustrating its evolution and our perspective on fostering human-compatible digital protection.

11 Bibliography

Alt, Rainer, Soheil Human, and Gustaf Neumann. 2020. "End-User Empowerment in the Digital Age." Edited by null Tung Bui. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 4099–4101.

Human, Soheil. 2022a. "Advanced Data Protection Control (ADPC): An Interdisciplinary Overview." arXiv. https://doi.org/10.48550/arXiv.2209.09724.

Human, Soheil. 2022b. *Really Enforceable Solution to Protect End-Users Consent & Tracking Decisions*. Sustainable Computing Reports and Specifications. https://doi.org/10.57938/fefe9b84-b00f-42d9-bd7e-0f6ea391e88c.

Human, Soheil. 2024a. "Human-Compatible Digital Protection, Consenting and Controlling." PhD Thesis, Vienna, Austria: Vienna University of Economics and Business.

Human, Soheil. 2024b. "Humans [Plural] in The Loop: The Forgotten Collective Aspects of Privacy, Consenting, Controlling and Digital Protection." *Frontiers in Political Science* 6 (September). https://doi.org/10.3389/fpos.2024.1391755.

Human, Soheil, Rainer Alt, Hooman Habibnia, and Gustaf Neumann. 2022. "Human-Centric Personal Data Protection and Consenting Assistant Systems: Towards a Sustainable Digital Economy." In *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Human, Soheil, and Florian Cech. 2020. "A Human-Centric Perspective on Digital Consenting: The Case of GAFAM." In *Human Centred Intelligent Systems: Proceedings of KES-HCIS 2020 Conference*. https://doi.org/10.1007/978-981-15-5784-2_12.

Human, Soheil, Rita Gsenger, and Gustaf Neumann. 2020. "End-User Empowerment: An Interdisciplinary Perspective." Edited by null Tung Bui. *Proceedings of the 53rd Hawaii International Conference on System Sciences*, 4102–11.

Human, Soheil, and Mandan Kazzazi. 2021. "Contextuality and Intersectionality of E-Consent: A Human-Centric Reflection on Digital Consenting in the Emerging Genetic Data Markets." In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*.

Human, Soheil, Gustaf Neumann, and Rainer Alt. 2021. “Human-Centricity in a Sustainable Digital Economy.” In *Proceedings of the 54th Hawaii International Conference on System Sciences*.

Human, Soheil, Gustaf Neumann, and Rainer Alt. 2022. “A Call for Interdisciplinary Research on Applied Human-Centricity in a Sustainable Digital Economy.” Edited by Tung X. Bui. *Proceedings of the 55th Hawaii International Conference on System Sciences*.

Human, Soheil, Gustaf Neumann, and Rainer Alt. 2023. “Human-Centricity of Digital Economies: From Concepts to Assessment Methodologies, Case-Based Studies, Solutions and Beyond.” *Proceedings of the 56th Hawaii International Conference on System Sciences*.

Human, Soheil, Gustaf Neumann, and Rainer Alt. 2025. “Co-Production of Human-Centricity and Digital Sustainability in Information Systems.” In *Proceedings of the 58th Hawaii International Conference on System Sciences*.

Human, Soheil, Gustaf Neumann, and Markus F. Peschl. 2019. “[How] Can Pluralist Approaches to Computational Cognitive Modeling of Human Needs and Values Save Our Democracies?” *Intellectica* 70:165–80.

Human, Soheil, Harshvardhan J. Pandit, Victor Morel, Cristiana Santos, Martin Degeling, Arianna Rossi, Wilhelmina Botes, Vitor Jesus, and Irene Kamara. 2022. “Data Protection and Consenting Communication Mechanisms: Current Open Proposals and Challenges.” In *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. https://ieeexplore.ieee.org/abstract/document/9799369/.

Human, Soheil, Max Schrems, Alan Toner, null Gerben, and Ben Wagner. 2021. “Advanced Data Protection Control (ADPC).” *Advanced Data Protection Control (ADPC)*, Sustainable Computing Reports and Specifications. https://doi.org/10.57938/149a03c3-2f39-4ca0-8ff7-be7f8ded61b8.

Morel, Victor, Cristiana Santos, Yvonne Lintao, and Soheil Human. 2022. “Your Consent Is Worth 75 Euros A Year - Measurement and Lawfulness of Cookie Paywalls.” In *Proceedings of the 21st Workshop on Privacy in the Electronic Society*, 213–18. Los Angeles CA USA: ACM. https://doi.org/10.1145/3559613.3563205.