## 1. Project Goal

The project was centered around addressing the multifaceted challenges of data protection and consenting in IoT environments, encompassing technical, legal, and human-compatibility dimensions. Conducted by the Sustainable Computing Lab, a collective of interdisciplinary researchers and practitioners committed to advancing equitable digital rights, and led by Asst. Prof. Dr. Soheil Human, the project aimed to develop solutions that reinforce user agency and control over personal data within IoT environments.

The key outcome was the development of the "ADPC-IoT" (Advanced Data Protection and Control for IoT), a technical specification tailored specifically for IoT environments and built upon the foundational ADPC framework. This specification formalizes the communication of privacy-related data, information, requests and decisions between IoT devices, such as sensors, and a mobile application, enabling users to manage their digital protection and consenting. Functional prototypes, including a mobile app for iOS and Android, were developed, using Bluetooth Low Energy and web technologies to enable data management between users and data controllers. The system also incorporated a server-side script for ESP32 devices to support seamless device-to-device communication.

The project targeted two primary beneficiary groups: data subjects interacting with IoT systems and data controllers tasked with managing these systems. Users were empowered with enhanced control over their digital rights, allowing them to actively engage in the ongoing process of digital protection and consenting. For data controllers, the ADPC specification serves as a tool to better align their systems with contemporary digital protection requirements. Furthermore, the project provides developers and innovators with a foundational technical framework for implementing human-compatible digital protection solutions in IoT environments.

Additionally, the project explored the integration of AI, with a particular focus on generative AI, to support users in dynamically managing their digital protection and consenting processes. This effort culminated in the development of a simple Personal Digital Protection, Consenting and Controlling Assistant System (PDPCAS). A user study was conducted to validate the system's usability, confirming its effectiveness in empowering users and aiding data controllers in navigating the complex socio-cognitive and legal landscape of digital protection within IoT ecosystems.

## 2. Project Results

| | | | |
|---|---|---|---|
| *1* | Project Interimreport | *NA* | *NA* |
| *2* | Project final report | *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* |

## 3. Planned subsequent activities after the conclusion of the netidee project

The sustainability and continuous development of the ADPC framework remain a key priority following the conclusion of the netidee project. We are currently expanding the ADPC framework to new environments, particularly focusing on mixed and augmented reality (MR/AR) applications. This extension will ensure the ADPC is adaptable to the evolving digital landscape and capable of addressing privacy and data protection challenges in immersive environments. Additionally, the application of ADPC-IoT in the context of sustainable and smart buildings is a significant next step. We are actively shaping new proposals and projects aimed at integrating ADPC-IoT into these domains to enhance data protection mechanisms in sustainable infrastructure. To support these efforts, we are engaging with various stakeholders from industry, academia, and policy sectors to build a broader community around the ADPC framework. This includes fostering partnerships that can contribute to its growth and implementation across diverse fields. Moreover, several academic publications related to the ADPC and its applications are currently in preparation and under review, with the aim of disseminating our findings and advancing the academic discourse on digital protection in IoT and extended reality environments. These activities are intended to ensure that the ADPC framework continues to evolve in response to emerging technological and societal needs while fostering collaboration and knowledge exchange among relevant stakeholders.

## 4. Suggestions for further developments by third parties

The ADPC framework offers numerous opportunities for third-party utilization and further development. Given its flexible architecture, it can be adapted and extended across various sectors and technological environments. We recommend that third parties explore the integration of ADPC into additional IoT contexts, particularly in industries such as healthcare, smart cities, and autonomous systems, where robust data protection and user control are critical. Moreover, the extension of ADPC into mixed and augmented reality presents significant potential for developers and innovators working in immersive technologies. By incorporating ADPC, third parties can enhance privacy and digital protection standards in these emerging digital environments, fostering user trust and compliance with evolving regulations. The application of ADPC in sustainable and smart infrastructure is another promising avenue for development. We encourage third parties to explore its use in building management systems, energy efficiency projects, and other sustainable technologies to ensure data privacy is embedded in future smart environments.

Additionally, there are opportunities for third parties to contribute to the standardization and regulatory alignment of ADPC. Collaborating with policymakers and regulatory bodies to formalize ADPC as a recognized standard for digital protection could further enhance its adoption and impact across sectors. We also recommend academic researchers to build upon the existing framework to explore new theoretical models and applied use cases that align with the evolving demands of digital protection and user empowerment. In summary, the ADPC framework serves as a robust foundation that third parties can leverage and expand, whether in technological applications, regulatory developments, or academic research.