MIDTERM REVIEW REPORT
(July 2020 to June 2022)

as Part of the Funding of Research and Development in the Field of"Human-technology Interaction for Digital Sovereignty" by the BMBF
SIMPORT V5DISO084-01

Title of the project:
"Sovereign and Intuitive Management of Personal Location Information (SIMPORT)"

Contributors:

Corinna Balkow
Gina Buchwald-Chassee
Jerome Dreyer
Felix Erdmann
Sven Heitmann
Prof. Dr. Christian Kray
Prof. Dr. Rainer Mühlhoff
Dr. Simge Özdal Oktay

Table of Contents

This report summarizes the main achievements and findings of the SIMPORT project during its first two years. Since the project start coincided with the beginning of the COVID pandemic, several activities could not be conducted as planned, and there were substantial delays, for example, regarding recruitment. In order to overcome these issues, several measures were put into place that enabled the project team to still deliver many of the planned outcomes as well as alternative results to planned ones that were not feasible anymore. Key outcomes of SIMPORT during its initial two years include

- a thorough analysis of related work on location privacy;
- a detailed analysis of common apps regarding how users can configure them;
- a first version of the learning app that enables users to easily see what location data is collected about them;
- an implementation of inference/attack strategies that can be included into the learning app to convey the implications of locations sharing to app users;
- a generic architecture to provide fine-grained control to users over what location information is being shared, and a prototypical implementation of it.

Further contributions include workshops with developers and users, initial insights into how to integrate ethical considerations into the development process of LBS as well as several open-source software releases.

In the following, all achievements and milestones are discussed in detail.

1. Management (WWU)

M01.1 Kickoff meeting

The kickoff meeting took place on the 17th of September 2020 as a full day virtual meeting with a delay caused by Covid-19 and various obstacles in the recruitment processes. In the meeting the partners were introduced, the project and the work packages were described, leading partners were assigned to the work packages, the communication channels were determined, upcoming milestones were discussed, and the next steps were planned. Following the kickoff meeting, we set up the following communication tools, which enabled us to effectively collaborate during the pandemic:

- Simport mailing list for communication;
- Trello board(s) for project management mainly for planning, assigning tasks, monitoring the progress, and timely deliverance of the milestones;
- Simport calendar for sharing upcoming events;
- Zotero for resource and literature management;
- Nextcloud for file management (managed by the FH Münster);
- Discord for real time communication and video calls;
- Zoom for organizing online and hybrid meetings

The midterm review meeting took place in August 2022 as a two-day hybrid event in Osnabrück. The meeting started by all partners giving a detailed report on what was achieved within the project and reported the status of the milestones up until June 2022. These presentations served as a basis for collaboratively drafting the midterm report (this document). On the second day, the focus was on planning ahead. The first half of the day was reserved for a detailed planning session on what to focus on during the remaining time of the project and on how to best proceed. In addition, the project partners ran a design workshop for finalizing the forms of interactions that had been produced through several workshops and background research. Finally, a brainstorming session was organized to look at what further interesting research questions emerged during the project so far. The partners also assessed potential calls for funding such future research.

M18.10 Midterm Review

The midterm report (this document) was authored collaboratively by all partners at the midterm meeting and then finalized in the following days. It is available in German and English through the project website.

M19.11 Midterm Report

2. Architecture and integration (FH Münster)

Between August 2020 and February 2021, a guide for analyzing the handling of location data and user consent in location-based services was created with a focus on mobile applications. In this scope, 40 popular location based mobile applications (per platform: iOS and Android) were analyzed by two raters, giving an overview about how popular location-based applications are handling location data and user consent. The results of this analysis were published in a paper ("Informed consent in popular location-based services and digital sovereignty")[1] and presented in the LBS 2021 conference, where it received the best full paper award.

M18.06 Software Architecture V1

M18.08 Implementation V1

The results provide useful insights regarding commonalities and differences in the control and management of personal location information among existing location-based services. The results revealed that "dark patterns" are frequently used when applications are asking to be granted access to the user's location.

In order to gain insights into the developers' perspectives regarding location privacy and to develop an architecture that allows users to stay in full control of their location data, we ran two developer workshops. The first one was held at the rc3 2020 ("remote Chaos Experience", the online version of the well-known Chaos Communication Congress). It featured a diverse set of people who were in some way connected to software development and who were especially interested in data privacy. This gave us useful ideas and insights about the developers' perspective in order to develop a privacy toolkit, which would make it easier for developers of location-based services to implement location privacy features. For example, the general need for such a toolkit and various ideas on how the implementation could look like were discussed – e.g. architecture documentation versus actual development as an integratable library. The second

[1] Jerome Dreyer, Sven Heitmann, Felix Erdmann, Gernot Bauer & Christian Kray (2022) ' Informierte Zustimmung zu beliebten ortsbezogenen Diensten und digitaler Souveränität, Journal of Location Based Services, DOI: 10.1080/17489725.2021.2017495

workshop was held in June 2021 and featured a selection of various app-developers, mostly working on actual location-based-services. Therefore, this workshop was more focused on the broad topic of location privacy and how an architecture / a toolkit could actually look like. Among other aspects, specific features were brainstormed, which eventually helped to narrow down the scope of the development.

Based on the insights from the developer workshops a first version of an architecture was conceptualized and implemented in the form of a “location privacy toolkit”. This library works on the technological base of Angular and Ionic. It is designed to be mainly used for mobile apps using Capacitor. This toolkit serves as a replacement for the usual OS API for location access and comes with several control mechanisms for users. By using an integrated set of user interface elements (forms of interaction), users can control which of their location data is accessed how and when (e.g., by setting the sampling interval or the accuracy of that data). The goal was to improve users’ sovereignty over their location data. The first versions of the toolkit with an initial set of control mechanisms have been fully implemented. They have already been released via the npm-registry and are thus ready to be used by other developers.

The playground finder app is a prototypical implementation of how a typical location based service can look like. Using the device's location, one can search for actual playgrounds in the user's area, including the navigation function to a nearby playground. It serves as a sandbox and demonstrator for the location privacy toolkit. The application provided a realistic use case scenario that the architecture can be implemented and tested directly. This enables rapid prototyping for quick results, e.g., regarding forms of interaction and location privacy control mechanisms (see figure 1). In addition, the playground finder app also serves as a blueprint for other developers who want to integrate the privacy toolkit into their own apps.

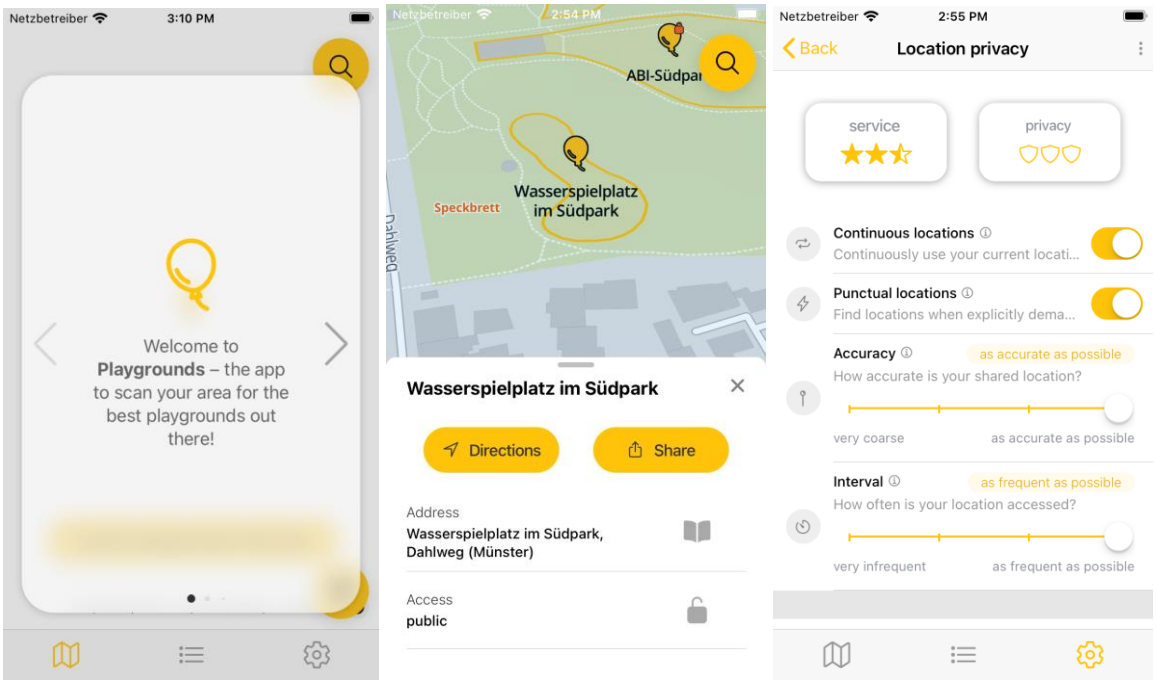

Figure 1: The Playground app **a)** opening screen **b)** detailed view from the search results **c)** privacy controls

The first version of the toolkit is implemented using a technology stack consisting of Angular, Capacitor and Ionic. The current implementation of the location privacy toolkit is realized as a library that can be integrated into (location based) applications. It is freely available as open source and integrated in the playgrounds app that was built as a prototypical test-platform for this architecture.

M20.12 Software Release

To ensure the quality and validation of the architecture and to gain insights on improving the management of personal location information the results of our developments are evaluated. As stated before the prototypical playgrounds app serves as a test-platform by integrating the location privacy toolkit. This gives us direct understanding on which parts of the toolkit are working as intended when being used in an actual app and where there is room for improvements. Furthermore, an implementation in react native by re:edu is being worked on. Both of these implementations provide useful insights in how this architecture works out in real app development scenarios.

M24.13 Evaluation Software Architecture V1

3. Learning tool, Exploration and UI (WWU)

M09.3 Sovereignty and PLI

During the first year of the project, we carried out extensive background research on the meaning, terms and relations of digital sovereignty and personal location privacy. Via a systematic meta-review of survey papers, we were able to identify and define key concepts of location privacy and digital sovereignty, common use cases, location privacy risks and attack strategies, location privacy protection mechanisms, as well as relevant stakeholders within the scope of processing location information. The results were integrated into a conceptual model that links stakeholders and key concepts in a systematic way (see figure 2). A first draft of a paper based on the results of the meta-review and their analysis is currently in the process of submission. After its publication, we will summarize our key findings on the SIMPORT web page.

Conceptual Model

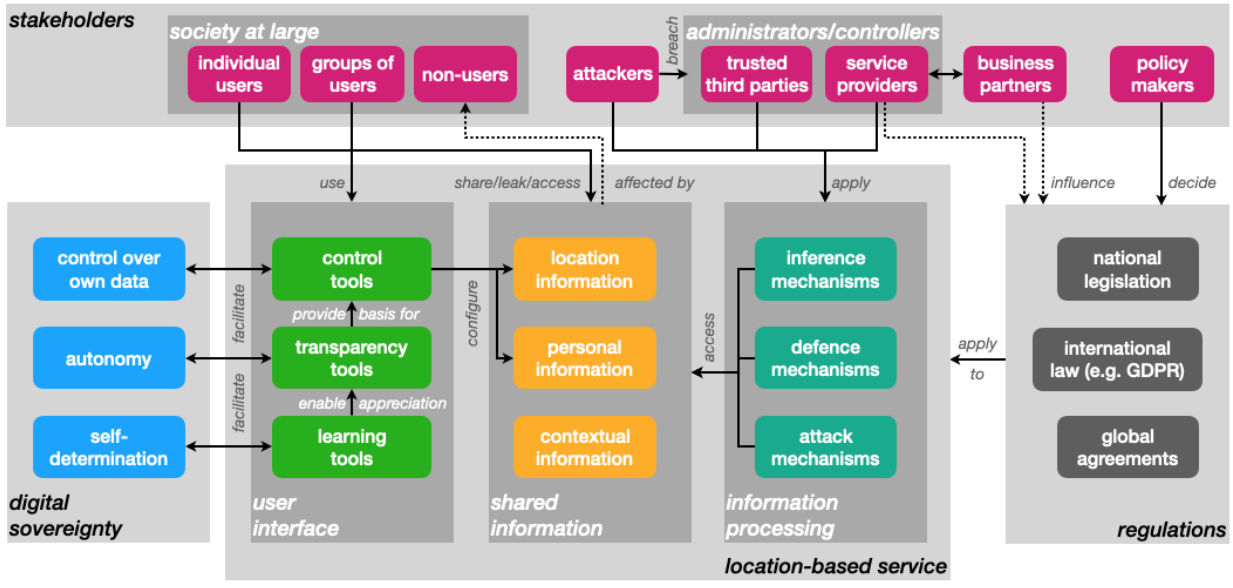

Figure 2: Conceptual model connecting stakeholders, location-based services, regulations and digital sovereignty

Learning tool:

M18.7 Learning tool V1

As one way of educating users, a digital learning tool was conceptualized and implemented as a prototypical mobile cross-platform application. The aim of this application was to educate users about risks and consequences of sharing personal location information (PLI) and possible protection mechanisms.

First, a simplified version was released as an internal beta version on the Google Play Store which will be used for a deployment study. For this study, the app collects and displays location data of the user on a map, including frequently visited points of interest. Therefore, the influence of reviewing user's collected location data will be investigated. Participants will reflect on their collected data every day (for two weeks) in the form of a diary. Currently, the study is fully conceptualized, including a first draft of a corresponding paper describing the methodology of the study. At the time of writing this document (September 2022), a pre-study is conducted to evaluate and refine the study design.

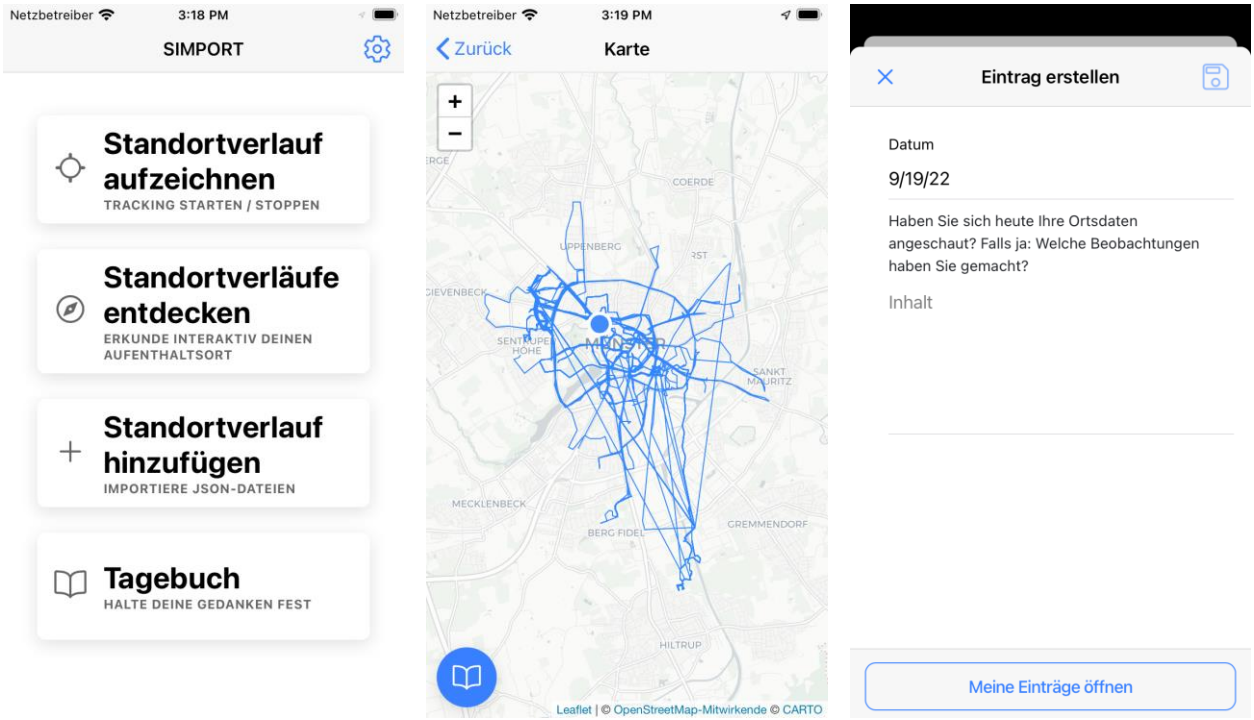

Figure 3: The Simport Learning App **a)** opening screen **b)** map view **c)** journal entry view

In addition to the pre-study, a consecutive deployment study with a richer feature set is planned. During the deployment study, participants will be confronted with inferences (e.g., inferred home and work locations) and predictions based on their personal location data. The necessary feature set (computation and visualization of inferences and predictions) for the second study is already

implemented. The source code and documentation for the learning app are freely available on github (https://github.com/sitcomlab/simport-learning-app/).

Exploration and UI

M09.4 Forms of Interaction V1

An important goal of the project is to develop user interfaces (UIs) for forms of interaction to increase users' digital sovereignty in protecting personal location privacy. Therefore, forms of interaction and desired UIs were systematically explored through literature research and user studies. The exploration is currently followed by the evaluation of the UI design alternatives for managing and controlling various aspects of personal location privacy. These aspects include giving informed consent, enabling broader user control, managing, and personalizing location privacy settings as well as browsing, selecting and deleting collected personal data. The user workshops were organized both in online and physical formats as well as in German and English. 25 participants joined these studies in total and the process was also supported by two internal workshops with project partners. The aim of these workshops was gaining deeper understanding about users' needs and priorities regarding protection of their personal location privacy. The results provided insights regarding the user's awareness of location privacy and intuitive design elements. For example, users are primarily concerned about sharing too much information with the service providers without knowing and without informed consent. But on the other hand they feel obliged to use certain applications such as messaging within the social circle (e.g. WhatsApp) and navigation (Google Maps). Therefore, their common action is accepting all of the default settings that are set by the provider, because they find the current state of the available information for personalization of the settings and the consequences of their actions on the applications is very cumbersome and time consuming. As a result, they feel helpless regarding protecting their personal information.

The results of the background research and several workshops provided a baseline for the user control settings, some of which were implemented in the playground and learning apps for further evaluation. In the current state of the application, a user can a) decide the frequency that the service provider can retrieve location information through intuitive toggles and sliders, b) explore the changes in the service quality and the level of privacy based on the desired data accuracy automatically, c) explore and delete their personal location history.

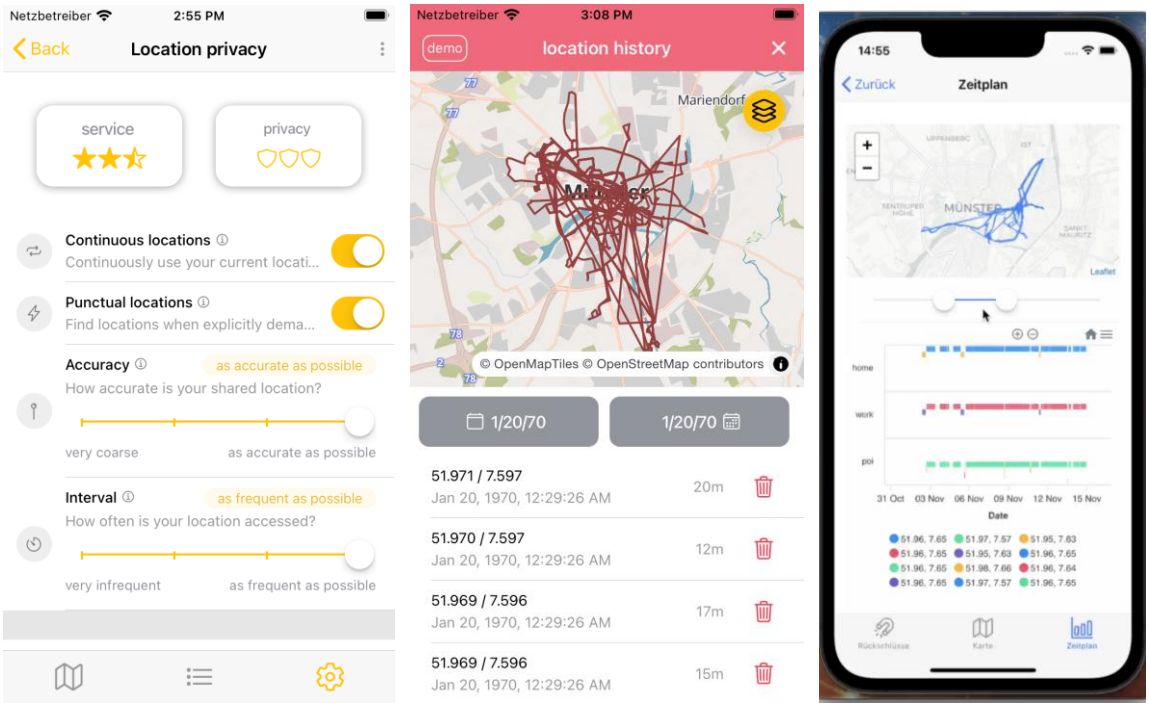

Figure 4: Prototypes **a)** playground app for exploration of service quality and the level of privacy according to the desired accuracy **b)** playground app for exploration of location history and deletion of shared data **c)** learning app for exploration and deletion of shared data.

- M12.5 Interaktionsformen V1 – Evaluation of all forms of interaction

In order to effectively manage the design and implementation of the needed forms of interactions, a dedicated working group was formed with the participation of several partners. The working group meets weekly to explore, evaluate and plan each step. This includes co-designing and iterating mock-ups and prototypical implementations. An initial workshop had been conducted internally to evaluate and improve these outcomes. A third user workshop for UI design critique is planned in November 2022.

M12.5 Forms of Interactio n V1

4. Ethics by Design (UOS)

The ethics sub-project adopted a Responsible Research and Innovation (RRI) approach to implement ethics and data protection considerations in the whole consortium. The ethics research in SIMPORT is characterized by a complex and very interesting double role: On the one hand, the research is defining the relevant ethical issues that needed to be brought to the attention of the whole team. On the other hand, there had to be researched which interactive and discursive methodology can be used in the process of raising awareness and building responsible design practices in any project team.

M24.15 Ethics by design

As to the theoretical part (naming the ethical issues at stake) the ethical component focused on the as yet underrepresented *collective* issues of data ethics and data protection: By the information that a user decides to share with a platform company, potential damage can result to *other* individuals. This puts a limit to classical individualistic and liberal framings of data protection as centering around empowering data subjects to control their own personal information. In a paper on collective privacy[2], a conference presentation (Forum Privatheit, 2021) and proceedings publication on "predictive privacy"[3], this collectivist perspective was spelled out as a new and contemporary challenge to data protection and data ethics given recent technologies of artificial intelligence and predictive analytics.

On the methodological side, the ethics sub-project team conducted and tested various interactive formats to work with the whole project team on the data ethics and data protection challenges of the SIMPORT project. In the first half of the project, the focus was on interactive formats (workshops, discussions, collaborative ideation session) using Design Thinking Methodology. Individual interviews and "ethics checkups" have been conducted in the monthly project meetings, contributed to internal and external workshops (with developers and users) and organized meetings on sub-aspects of the Ethics by Design process. A main part of the methodology was the compilation of 5–10 "data ethics worksheets" that formed the basis for intensive discussion meetings. Topics included are following ethical issues: Bias, Accessibility, Vision of sovereign user, how to create empowerment, Privacy concepts - difference of educational approach, nudging, privacy as a service; implications in the choice of technology; Implications of location data - effects of inferences; UI options for Control and consent - how to transfer ethical goals into interaction design. These worksheets were tested in the project work and subsequently refined to become a central part of our ethics guidelines.

Based on the theoretical and methodological work, we set up a draft version for the structure of our ethical guidelines that will be written in the next project phase. As part of these ethics guidelines, the ethics sub-project team will create a glossary of ethical and technical concepts to help bridge the interdisciplinary gap between technical and philosophical disciplines. The process and methodology explanation will be integrated into the guidelines. The creation of the "Ethics by Design V1" continues in the interactive process mentioned above.

5. Dissemination (Re:edu)

The focus of dissemination activities in the SIMPORT project is the project website https://www.simport.net (see figure 5). The initial project website was created in July 2020 in collaboration between FH Münster and Re:edu with basic information about the project, which

M03.2 Project website V1

[2] Balkow, Corinna (2022). "Privatheit gesellschaftlich denken – von der aktuellen digitalen Welt zur möglichen digitalen Welt". In Humanistische Akademie Berlin-Brandenburg e.V *Intelligent Design? Wie der Mensch sich neu entwirft.* Im Erscheinen.

[3] Mühlhoff, Rainer (2022). „Prädiktive Privatheit: Kollektiver Datenschutz im Kontext von Big Data und KI". In Friedewald, Michael und Alexander Roßnagel (Eds.), *Künstliche Intelligenz, Demokratie und Privatheit*. https://doi.org/10.5771/9783748913344-31 .

was continuously expanded and extended – e.g., with various reports on completed work within the project. Currently the website incorporates:

- information about the partners and project goals;
- a blog about project related topics (e.g., publications, events, talks);
- a results section that provides an overview of the state of the project and links to further resources (GitHub repositories, app analysis results); and
- announcement of all workshops and registration.

Right after the project started, a twitter account (https://twitter.com/SIMPORTp) has been created and curated on a regular basis to disseminate project news, results and announcements such as, e.g. calls for participation in workshops. The aim is to expand the account even further and gain more followers.

Figure 4: Homepage of the project website

Improvements on the website are in progress regarding the theme of how to reach a better user experience on mobile devices. Currently, Re:edu is preparing further content as an animated explanatory video about the learning app and interviews (as videos) with the project partners.

M18.9 Project website V2