SPECIAL

Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance

Deliverable D5.2

Public challenge report V1

Document version: 1.0

SPECIAL DELIVERABLE

Name, title and organisation of the scientific representative of the project's coordinator:

Ms. Jessica Michel t: +33 4 97 15 53 06 f: +33 4 92 38 78 22 e: jessica.michel@ercim.eu

GEIE ERCIM, 2004, route des Lucioles, Sophia Antipolis, 06410 Biot, France

Project website address: http://www.specialprivacy.eu/

Project	
Grant Agreement number	731601
Project acronym:	SPECIAL
Project title:	Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance
Funding Scheme:	Research & Innovation Action (RIA)
Date of latest version of DoW against which the assessment will be made:	17/10/2016
Document	
Period covered:	M18-M21
Deliverable number:	D5.2
Deliverable title	Public challenge report V1
Contractual Date of Delivery:	30-09-2018
Actual Date of Delivery:	28-09-2018
Editor (s):	Uroš Milošević (TF)
Author (s):	Uroš Milošević (TF), Wouter Dullaert (TF)
Reviewer (s):	Rigo Wenning (ERCIM), Harald Zwingelberg (ULD)
Participant(s):	
Work package no.:	5
Work package title:	Use Case Implementation & Evaluation
Work package leader:	TR
Distribution:	PU
Version/Revision:	1.0
Draft/Final:	Final
Total number of pages (including cover):	21

Disclaimer

This document contains description of the Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance (SPECIAL) project work and findings.

The authors of this document have taken any available measure in order for its content to be accurate, consistent and lawful. However, neither the project consortium as a whole nor the individual partners that implicitly or explicitly participated in the creation and publication of this document hold any responsibility for actions that might occur as a result of using its content.

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of the SPECIAL consortium and can in no way be taken to reflect the views of the European Union.

The European Union is established in accordance with the Treaty on European Union (Maastricht). There are currently 28 Member States of the Union. It is based on the European Communities and the Member States cooperation in the fields of Common Foreign and Security Policy and Justice and Home Affairs. The five main institutions of the European Union are the European Parliament, the Council of Ministers, the European Commission, the Court of Justice and the Court of Auditors (http://europa.eu/).

SPECIAL has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731601.

Table of Contents

1 Introduction

Driven by use case scenarios, WP5 aims to evaluate the results obtained in WP 2 (Policy and Transparency Framework), WP 3 (Big Data Policy Engine), and WP 4 (User Interaction) under real-world conditions. More specifically, the goal of T5.3 Public challenges is to expose the developed system and its components to public hacking challenges, which would, together with the internal backend scalability and robustness testing performed in WP3 (D3.3 and D3.5) and frontend testing in WP4 (D4.2 and D4.4), provide the necessary feedback for further development of the SPECIAL platform.

To guarantee the robustness of our architecture, such tests must focus on ensuring that both the individual components and the infrastructure as a whole are capable of sharing data only with authorized parties, while guaranteeing that policies and regulations are being adhered to. This means that the challenges should span beyond just penetration testing, and involve other aspects of the system, be it technical or legal, highlighting any limitations.

Moreover, WP 6 (Collaboration, Dissemination & Standardisation) will organize public workshops to present and discuss such limitations and obtain input with respect to possible additional challenges. The experiences gained from all these activities will be merged, generalized, and translated into a set of methodological guidelines for future implementations.

1.1 Deliverable scope

This deliverable discusses the technical, legal, and practical requirements for running a public hacking challenge program and maximizing its outcome. It also provides a concrete plan and delivers the first challenge call for entries and the accompanying program policy (provided in the Annex of this document). D5.4 Public challenge report V2 will report on the program results.

2 Challenge scope

The goal of the challenges is to learn about any shortcomings of the SPECIAL platform that could result in a data breach or a violated data usage policy. Such shortcoming could include bugs pertaining to authentication/authorization, the APIs or other bugs related to data flows, the logs or log formats, the front-ends, or even the policy language. Any tests should cover only what is directly within SPECIAL's span of control (that is, being developed by the project partners) and not involve third party solutions, be it commercial or open-source. Moreover, any known flaws in the system should be also made public and excluded from the challenge scope.

More specifically, we hereby explicitly define what we believe should be in and out of scope of the SPECIAL Public Challenge (Table 1).

In-scope platform components	***Out of scope platform components***
• *Integrated system as a whole* • *Compliance engine* • *Consent management front-end(s)* • *Transparency & compliance front-end(s)* • *Usage policy language* • *Policy log vocabulary*	• Apache Kafka • RethinkDB • Keycloak • HermiT • Any other components not built and maintained by the SPECIAL Consortium

Table 1: In and out of scope platform components

2.1 Attacks and vulnerabilities

Similarly, both possible attacks and vulnerabilities should be confined to a clearly defined list to get the desired outcome and avoid potential misinterpretations of the policy or abuse of the public challenge program.

Table 2 lists what we see as qualifying and non-qualifying vulnerabilities and attacks.

Qualifying attacks & vulnerabilities	***Non-qualifying attacks & vulnerabilities***
• *Authentication vulnerabilities* • *Privilege escalation* • *Significant Security Misconfiguration* • *Information Disclosure* • *Injection vulnerabilities*	• Clickjacking • Denial of service attacks • Phishing attacks • Social engineering attacks • Content spoofing • Issues requiring direct physical access • Flaws affecting out-of-date browsers and

	plugins • Weak password policies • HTTP 404 codes/pages or other HTTP non-200 codes/pages

Table 2: Qualifying and non-qualifying attacks and vulnerabilities

2.2 Use cases

Although inspired by the three pilots, the public challenges are not meant to happen in live setups involving real data subjects. Moreover, due to the sensitivity of the information, business and security concerns, disclosing the details on the real-world setups of the pilots partners is also not an option. For this reason, the participants will be offered a simulated environment, running on synthesized data, without direct references to the pilot partners or their use cases.

2.2.1 Fictional use case “BeFit”

To avoid potential business, security and legal obstacles, the platform setup could default to BeFit, a fictional use case. In this scenario, a fitness tracking application collects personal data, such as physical characteristics and workout activity, for different commercial purposes.

The BeFit scenario covers all aspects of the current architecture – consent management per user, compliance checking, and transparency for both the data controller and the data subject. In addition to this, the setup should be accompanied by a log generator for synthesizing application processing events.

3 Challenge conditions

Participation in the SPECIAL Public Challenge should be entirely voluntary. All participants will have to read and agree to the official challenge terms and conditions to be eligible for any challenge benefits. The SPECIAL Consortium will reserve the right to change or modify the terms of the program at any time.

3.1 Ground Rules

To ensure healthy competition and desired challenge outcome, but also prevent abuse, we will set forth some ground rules for all participants:

- All participants should aways research and disclose bugs and vulnerabilities in good faith.
- No participant should ever leave any system or its components in a more vulnerable state than they found it.
- No participant should ever publicly disclose a vulnerability without the SPECIAL Consortium's consent, unless the vulnerability has already been disclosed by the SPECIAL Consortium.

3.2 Eligibility to Participate

For the sake of fairness, we will also ensure all challenge participants meet the challenge eligibility criteria. Namely, the participants must:

- Not be directly affiliated with SPECIAL or any of the project partners.
- Not be in violation of any law or regulation with respect to any activities directly or indirectly related to the SPECIAL Public Challenge and the involvement must not be an infringement of any law or regulation for SPECIAL or its project partners (e.g. export regulations).

Not meeting the above eligibility criteria or breaching these Terms in any other way will give us the right to, in our sole discretion, remove the participant from the SPECIAL Public Challenge and disqualify them from receiving any benefit of the SPECIAL Public Challenge.

3.3 Personal Data

Participation in the challenge will not be conditioned on providing any personal data. Nevertheless, to qualify for any benefits of the challenge, the participants will be required to share the data necessary for processing vulnerability reports and paying out bounties. The SPECIAL Consortium will never collect more than what is requested of the participants for these purposes, and any redundant data will be deleted on receipt.

4 Process

4.1 Testing environment

Due to the nature of the challenge and the resources at the Consortium's disposal, an adequate shared testing environment would be considerably more difficult to provide than a dedicated setup per challenge participant. A possible solution is to offer preconfigured installation packages representing different real-world scenarios inspired by our pilot use cases. The platform could then be deployed and tested locally or on any remote server under the participant's control. Additionally, the policy language could be tested outside the platform setup.

For ease of deployment, each use case should have a dedicated installation package. Such configuration packages could be offered as Docker container images and distributed via a public repository. A straightforward choice for such a distribution channel would be the official project GitHub repository[1].

4.2 Communication

Building further on the principle of responsible disclosure, we will ensure all communication between the participant reporting a system flaw and the public challenge committee is private until the reported flaw has been fixed. To this end, the SPECIAL consortium will set up a dedicated e-mail address for such reports.

4.2.1 Report

Once a participant identifies a vulnerability, they will be expected to prepare a comprehensive report and send it to the challenge committee for assessment. If the committee finds the report valid, the participant will be awarded points, based on the severity level of the finding (Section 4.3.1).

A "comprehensive report" should include at least:

- A detailed description of the vulnerability;
- Steps (or a proof-of-concept) used to expose the vulnerability;
- Specific source code references (when possible; the report should at least list the relevant architecture components).
- Any other relevant information.

4.3 Format and timing

As a dedicated budget for the public challenge was not foreseen by the project plan, a traditional continuous bug bounty program, guaranteeing a financial reward per reported vulnerability is not

[1] https://github.com/specialprivacy/demonstrator

feasible. Therefore, the SPECIAL public challenge needs to explore alternative approaches, such as gamification, to provide enough incentives for long-term participation.

A possible strategy is to award points for each report (rather than a financial incentive), which could be then aggregated per participant and ranked. The motive behind introducing a leaderboard is threefold:

- Creating a sense of community,
- Eliciting the desire to participate and compete, and
- Paying out bounties at the end of the challenge to the top-ranking competitors, rather than every time a participant reports a vulnerability.

To further incentivize participation over a longer period of time, the challenge program could also be organized into multiple runs. During each of the runs, the participants would be given as much time as they need to examine the system and look for flaws. The final run would finish at least one month ahead of

4.3.1 Scoring, ranking, and rewards

The more convincing the demonstration of breaking defined policies and compliance rules or otherwise highlighting limitations of our system or its parts, the more points will be awarded to the participant.

The SPECIAL Consortium will reserve the right to determine the level of severity based on a number of criteria, including the CVSS score (Section **Error! Reference source not found.**), decide if the minimum severity threshold is met, and assess whether the vulnerability was previously reported.

4.3.1.1 Scoring system

The Common Vulnerability Scoring System (CVSS)[2] provides a way to capture the principal characteristics of a vulnerability, and produce a numerical score reflecting its severity, which can then be translated into a qualitative representation (such as low, medium, and high).

The CVSS score would allow us to formalize the severity levels and assign points based on a predefined policy. A sample challenge scoring system is given in Table 3.

Severity level	*Low*	*Medium*	*High*
Points	5	10	15

Table 3: Scoring system

Once a vulnerability has been confirmed, the competitor will be assigned the number of points they are due, which will then be added to their total and published along with other participants' scores on a dedicated challenge page. The information will be limited to the chosen or assigned (if not provided) competitor alias, the number of reports, and the total score (Table 4). The total score will determine the overall ranking.

[2] https://www.first.org/cvss/

POSITION	ALIAS	NUMBER OF REPORTED VULNERABILITIES			SCORE
		Low	Medium	High	

Table 4: Ranking table structure

The details of all confirmed issues will be given on a separate page, providing full transparency, while also allowing all participants to inform themselves on the already resolved vulnerabilities before starting their investigation.

4.3.1.2 Rewards

Any rewards will be based on the above described public score granted entirely at the discretion of the SPECIAL Consortium. To qualify for points under the SPECIAL public challenge program, the competitor should:

- Be the first to report a vulnerability;
- Disclose the vulnerability report directly and exclusively to the SPECIAL public challenge committee.

DTAG has offered to provide six mobile devices (three high-end and three mid-range phones) as rewards. TF will complement this with 3 Amazon vouchers of € 50, allowing us to offer three rewards per run. The partners have committed to delivering the prizes to the top 3 contributors within 30 days of a completed 3-month run. The SPECIAL Consortium, however, will reserve the right to change the aforementioned rewards without prior notice.

5 Promotion

5.1 Target audience

The SPECIAL Public Challenge should be an open call to researchers, ethical hackers, and IT professionals, but also any other individuals who would be interested in testing and inspecting the SPECIAL platform for security vulnerabilities, bugs or flaws in the system or its components.

Due to the nature of the technologies involved, basic knowledge of semantic web technologies would be desirable, but is not mandatory, as the intention is to target all aspects of the system.

5.2 Channels

To reach out to the desired audience, we intend to use all dissemination channels established in WP 6 and currently at our disposal. More specifically this means at least informing the public via our website, the social media, the universities and research projects we collaborate with, and the BDV PPP. A more detailed overview of these channels is given in Table 5.

Channel type	***Channel***
Website	• SPECIAL website
Social media	• Twitter – project and partner profiles • LinkedIn – partner pages and profiles • Meetup – BigData.be community
Academic community	• Wirtschaftsuniversität Wien, Austria • Technische Universität Berlin, Germany • Università degli Studi di Napoli Federico II, Italy • Katholieke Universiteit Leuven, Belgium (via TenForce)
Partner projects	• RestAssured[3] • ReCRED[4] • MyHealthMyData[5] • SODA[6] • DECODE[7]
Other	• BDV PPP newsletter and website • DPVCG W3C community group

[3] https://restassuredh2020.eu

[4] https://www.recred.eu

[5] http://www.myhealthmydata.eu

[6] https://www.soda-project.eu

[7] https://decodeproject.eu

Table 5: Dissemination channels

6 Conclusion

This deliverable gave an overview of what we see as the technical, legal, and practical requirements for a successful SPECIAL public hacking challenge program. We defined the scope, the challenge terms and conditions, provided a format and a concrete plan, and explained the reasoning behind our decisions. Based on this information, we published the first challenge call for entries and the accompanying program policy on our website[8] (available in the Annex).

The final of the planned runs ends in month 29. D5.4 Public challenge report V2, which is conveniently due at the end of month 30, will report on the challenge outcome.

[8] https://www.specialprivacy.eu/platform/public-challenge

7 Annex: Public challenge call for entries and program policy

Discover security vulnerabilities, bugs or flaws in the system or its components, and win interesting prizes!

What is SPECIAL?

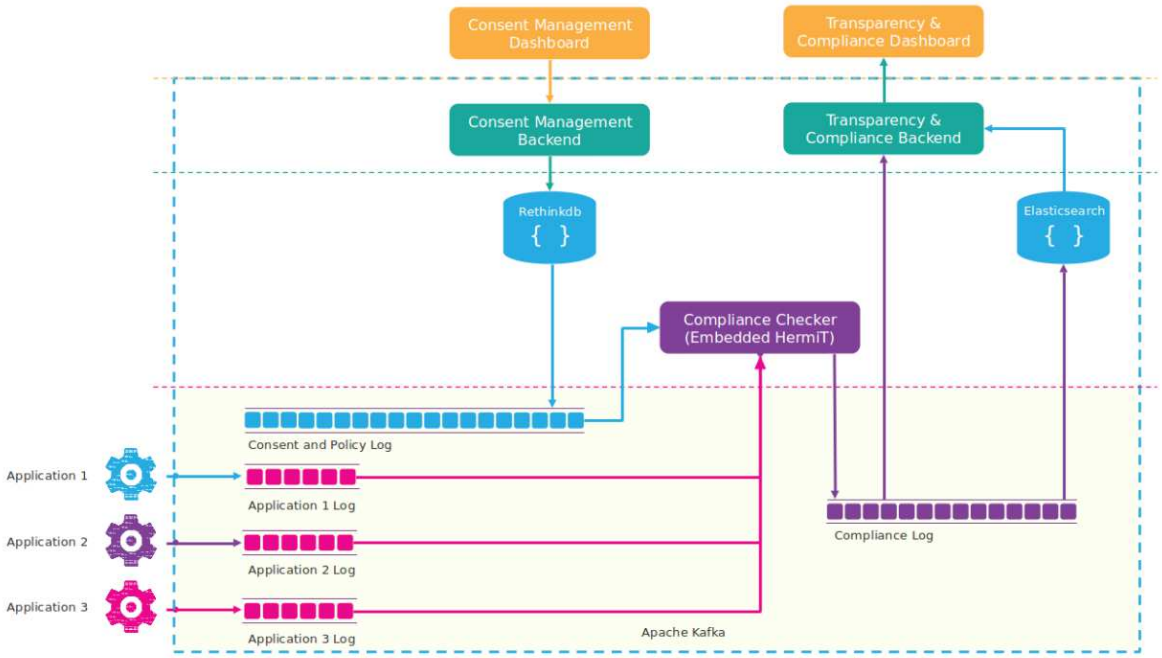
The SPECIAL project[9] addresses the contradiction between Big Data innovation and privacy-aware data protection by proposing a technical solution that makes both of these goals realistic. SPECIAL allows citizens and organisations to share more data, while guaranteeing data protection compliance, thus enabling both trust and the creation of valuable new insights from shared data. We develop technology which:

- supports the acquisition of user consent at collection time and the recording of both data and metadata (consent policies, event data, context) according to legislative and user-specified policies;
- caters for privacy-aware, secure workflows which include usage/access control, transparency and compliance verification;
- aims to be robust in terms of performance, scalability and security, all of which are necessary to support privacy preserving innovation in Big Data environments; and
- provides a dashboard with feedback and control features which make privacy in Big Data comprehensible and manageable for data subjects, controllers, and processors.

SPECIAL Platform

The SPECIAL platform is an extensible environment for managing personal data usage policies, ensuring compliance with such policies, and tracking personal data usage along with the context it is being used in. The high-level overview of this policy-aware Linked Data architecture and engine is given below:

[9] The project “Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compliance” (SPECIAL) has received funding from the European Union’s Horizon 2020 research and innovation programme under grant agreement No No. 731601.



A demo video is available here[10]. For a detailed description of the system and its components, we strongly recommend consulting at least:

- Deliverable 3.2 - Policy & events release (M16)[11]

Other relevant project deliverables are also public and can be found here[12]. Additionally, we also suggest reading about:

- The SPECIAL Usage Policy Language[13]
- The SPECIAL Policy Log Vocabulary[14]

What is the SPECIAL Public Challenge?

The SPECIAL Public Challenge is an open call to researchers, ethical hackers, IT professionals and other interested individuals to test and inspect the SPECIAL platform and point out any security vulnerabilities, bugs or flaws in the system or its components.

[10] https://www.specialprivacy.eu/images/videos/ESWC%20demo%20submssion.mp4

[11] https://www.specialprivacy.eu/images/documents/SPECIAL_D3.2_M16_V1.0.pdf

[12] https://www.specialprivacy.eu/publications/public-deliverables

[13] https://aic.ai.wu.ac.at/qadlod/policyLanguage/

[14] https://aic.ai.wu.ac.at/qadlod/policyLog/

"I am not familiar with some of the technologies. Can I still participate?"

Basic knowledge of semantic web technologies (OWL, RDF, reasoning engines) is desirable, but not mandatory. There are many other ways you can contribute. Please see the description of the program scope below.

Scope

We are interested in learning about any shortcomings of the SPECIAL platform that could result in a data breach or a violated data usage policy. Examples of such shortcoming could include bugs pertaining to authentication/authorization, the APIs or other bugs related to data flows, the logs or log formats, the front-ends, the policy language, etc. The platform can be deployed and tested locally or on any remote server under your control. Additionally, the policy language can be tested outside the platform setup.

Note: This is an early prototype of what is expected to reach TRL5[15] by 2020. It is, therefore, not production ready.

Below, we describe what is in and out of scope of our Public Challenge program.

In-scope platform components

- Integrated system as a whole
- Compliance engine (but not HermiT itself)
- Consent management front-end(s)
- Transparency & compliance front-end(s)
- Usage policy language
- Policy log vocabulary

Out of scope platform components

- Apache Kafka
- RethinkDB
- Keycloak
- HermiT
- Any other components not built and maintained by the SPECIAL Consortium

Qualifying attacks & vulnerabilities

[15] https://en.wikipedia.org/wiki/Technology_readiness_level

- Authentication vulnerabilities
- Privilege escalation
- Significant Security Misconfiguration
- Information Disclosure
- Injection vulnerabilities

Non-qualifying attacks & vulnerabilities

- Clickjacking
- Denial of service attacks
- Phishing attacks
- Social engineering attacks
- Content spoofing
- Issues requiring direct physical access
- Flaws affecting out-of-date browsers and plugins
- Weak password policies
- HTTP 404 codes/pages or other HTTP non-200 codes/pages

Process

The process is simple. The challenge program is organized into three 3-month runs, with the last one ending on May 31, 2019. During each of the runs, you get as much time as you want to examine the system and look for flaws. Any time you find something you consider worth mentioning, you prepare a comprehensive report and send it to us for assessment. If we find the report valid, we will immediately reward you with points, based on the severity level of the finding. (Please see 'Rewards' below.)

How do I report security issues?

Please send all your findings to special-bugs@ercim.eu, including:

- A detailed description of the vulnerability;
- Steps (or a proof-of-concept) used to expose the vulnerability;
- Specific source code references (when possible; you should at least list the relevant architecture components).
- Any other relevant information.

Rewards

Rewards are based on a public score granted entirely at the discretion of the SPECIAL Consortium. To qualify for points under this program, you should:

- Be the first to report a vulnerability;
- Disclose the vulnerability report directly and exclusively to us, unless the vulnerability has already been disclosed by us.

Severity assessment

The more convincing the demonstration of breaking defined policies and compliance rules or otherwise highlighting limitations of our system or its parts, the more points you get. The SPECIAL Consortium reserves the right to determine the level of severity (based on a number of criteria, including the CVSS score), decide if the minimum severity threshold is met, and assess whether the vulnerability was previously reported.

Severity level	Low	Medium	High
Points	5	10	15

Ranking

The first time your report is resolved and closed, your name or chosen alias will be added to our public “Thank you” scoreboard. (Please see ‘Personal data’ for additional information.) For that and every subsequent report, the awarded points will be added to your total score. The total number of accumulated “Thank you” points will determine the participant ranking at the end of the run. The top-3 contributors at the end of each run will get rewards!

This run's bounties

The prizes will be sent out to the top 3 contributors within 30 days of a completed 3-month run. The SPECIAL Consortium reserves the right to change any of the below awards without prior notice.

1st place	A high-end smartphone
2nd place	A mid-range smartphone
3rd place	A € 50 Amazon voucher

Terms

Participation in the SPECIAL Public Challenge is entirely voluntary. By submitting a report, you are indicating that you have read and agree to our Terms, as outlined below. The SPECIAL Consortium reserves the right to change or modify the terms of this program at any time.

Ground Rules

- Always research and disclose in good faith.
- Never leave any system in a more vulnerable state than you found it.
- Never publicly disclose a vulnerability without our consent.

Eligibility to Participate

To be eligible to participate in our Public Challenge, you must:

- Not be directly affiliated with SPECIAL or any of the project partners.
- Not be in violation of any law or regulation with respect to any activities directly or indirectly related to the SPECIAL Public Challenge and the involvement must not be an infringement of any law or regulation for SPECIAL or its project partners (e.g. export regulations).

Not meeting the above eligibility criteria or breaching these Terms in any other way gives us the right to, in our sole discretion, remove you from the SPECIAL Public Challenge and disqualify you from receiving any benefit of the SPECIAL Public Challenge.

Personal Data

Please keep in mind that we do not require any personal data apart from what we believe is absolutely necessary for processing vulnerability reports and paying out bounties. We will never ask for more than this. Should you ever disclose more than what is requested of you, we will erase such data on receipt.

As a privacy project SPECIAL allows anonymous or pseudonymous (alias) submissions to be processed for conducting the hacking challenge. Contact data are however greatly appreciated for questions and getting back to you. Your name or alias will be publicly displayed on the scoreboard. To hand out prizes to winners these will be asked their name and address for shipment as well as a confirmation that the prize has been received. Depending on the regulatory framework of the partner donating the prize in question the the latter information may be necessary to be stored with their financial information for audit-purposes. Contact information of the contributors will be deleted at latest three month after the SPECIAL project has ended.

You have the right to access your personal data processed by us. You may withdraw your consent to process your personal data – your contributions will then be handled as anonymous or under an alias of your choice.

Getting started

We offer preconfigured installation packages representing different real-world scenarios inspired by our pilot use cases.

BeFit

This is the default package. In this scenario, a fitness tracking application collects personal data, such as physical characteristics and workout activity, for different commercial purposes. It comes with a simple UI for consent management per user, a log generator for synthesizing application processing events, and a transparency and compliance dashboard.

You will find everything you need to get started in our official GitHub repository.

Questions?

Feel free to drop us an e-mail at special-bugs@ercim.eu