SPECIAL

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

Deliverable 5.3

Pilot implementations and testing plans V2

Document version: 1.0

SPECIAL DELIVERABLE

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

Jessica Michel Assoumou 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:	M1 – M28
Deliverable number:	D5.3
Deliverable title	Pilot implementations and testing plans V2
Contractual Date of Delivery:	30.04.2019
Actual Date of Delivery:	30.04.2019
Editor (s):	Martin Kurze (DTAG)
Author (s):	Benedict Whittamsmith, Rudy Jacob, Martin Kurze
Reviewer (s):	Sabrina Kirrane, Eva Schlehan, Piero Bonatti, Olha Drozd
Participant(s):	TR , Prox, DTAG/TLABS
Work package no.:	WP5
Work package title:	Use Case Implementation & Evaluation V2
Work package leader:	TR
Distribution:	PU (following project closure)
Version/Revision:	1.0
Draft/Final:	Final
Total number of pages (including cover):	36

Disclaimer

This document contains description of the 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 Summary

Three industry partners (Proximus, Refinitiv and Deutsche Telekom) describe their pilots and testing plans for components, tools and concepts developed in SPECIAL by the consortium. The pilots and implementation plans are based on previous documents/deliverables (namely D5.1 and as well as D5.2, D1.1, D1.2, D1.3, D1.4 and subsequently D2.4, D3.2 and D3.3)

This document was designed for "staging", i.e. it will be reworked on a regular basis. The present version "Deliverable 5.3 V2" is the second iteration and includes implementation plans, first results of the (already implemented) pilots and the test plans. A final iteration of the document (V3) will be found in D5.5. Due to the different objectives and types of implementation, the industry partners were assigned one chapter each. These chapters may be read relatively independently of each other. However they all have certain aims and findings in common. These are collected in the overarching chapters 2 and 6.

Since this is "V2", neither a profound summary nor ultimate conclusions can be expected. The reader is kindly asked to take advantage of the current (mature but still preliminary) state of findings and wait for the subsequent final version of the deliverable (D5.5) for deeper insights.

The present document aims at giving the reader a comprehensive view into the current state of implementation of the pilots, testing plans and already achieved as well as expected findings.

2 Introduction to pilots and testing plans in SPECIAL

2.1 Types and purposes of pilots, business/industry context

Three different industry partners, each with their own use case and differing overall objectives designed pilots for implementation. This resulted in different types of pilots, tests and even different types of descriptions in this deliverable:

- **Proximus** is aiming (short- to mid-term) towards a new, innovative commercial product in the recommender-business based on personal data. In this early phase of the product development, the prototype aims at implementing and testing a relatively complex use case with relatively small amount of data subjects.
- **Refinitiv** is interested in applying methods and tools to automatically read and evaluate privacy policies and a company-internal workflow. Therefore the focus is very much on the policies, policy language and policy checking tools. The number of planned users is not so much in focus since the system will mainly be applied internally.
- **Deutsche Telekom** (with its R&D units VTI/T-Labs) is aiming more at applications that use the huge amount of (personal) data that exists in DT and today cannot be monetized due to the current tight interpretation of applicable privacy legislation, e.g. GDPR. Thus, DT needs a PoC (proof of concept) that shows that GDPR compliant collection, processing and even sharing of data is feasible in a legal way, once tools like those developed in SPECIAL are available and mature. Therefore, DT's pilot is relatively simple and straightforward (supplementing an existing process): to prove feasibility, test usability and estimate effort to reach this goal. While the use case is relatively small, the number of potential users is relatively high which will give DT a sound basis for user acceptance.

Due to the inherent differences of the pilots, the respective chapters of this document are under full authorship of the individual industry partners. This also explains the slightly different styles of writing.

2.2 Purpose and requirements for tests/testing plans

All industry partners plan to evaluate all relevant aspects of SPECIAL's results during the course of the project. Given the novelty of the approach and the complexity of implementation of any aspect of it in an "industrial" environment, industry partners decided to stepwise evaluate parts of the results or intermediate results. This not only minimizes the evaluation work, it also allowed (and still allows) the consortium to enhance work results during several iterations.

Currently, the industry partners focus on the most relevant aspect for their business, not neglecting the fact that several other aspects need to be evaluated and are planned to be implemented in the operational business succeeding the project duration. Fundamental requirements will be tested repeatedly (Security, Privacy and Usability; see below).

Iteration 1 (previous document, deliverable D5.1)
Proximus evaluated mainly the overall architecture and the composition of building blocks, general feasibility needed to be checked, and first experiences with corporate internal processes needed to be collected. First tests in conjunction with Proximus' recommender engine were carried out.
Refinitiv has a strong focus on the policy language and checked its' expressivity and compliance in detail.
Deutsche Telekom *(DT)* used this phase for a complementary approach: internal corporate (IT) processes were checked or revised to implement core aspects of SPECIAL. This lead to an in-depth evaluation of SPECIAL's modularity. Also scalability was (and is) tested relatively early with a

"minimal viable prototype" (put in quotation marks because DT does not expect a product level tool but rather a prototype or PoC – Proof of Concept –that delivers "viable"/expedient results) focussing on a small set of privacy relevant data.

Iteration 2 (this document, deliverable 5.3)
Proximus will extend the user group and thus plans to focus on scalability of the approach. Focus will be on transparency and compliance.
Refinitiv in this phase looks towards generalising some of the lessons of applying the Special Technology to its use case into wider/arbitrary use cases in the financial data supply chain.
Deutsche Telekom focuses on technical ease of implementation and applicability of DT's corporate design and corporate identity rules of the tools. Detailed alignments with corporate regulation and affected departments/subsidiaries took place and lead to a comprehensive view and product (feature) opportunity. In addition, DT also ran a first evaluation of business relevance.

Iteration 3 (upcoming deliverable 5.5)
All industry partners will evaluate the applicability of their respective pilots in their organizations. Also the overall concepts of SPECIAL (linked data, usage policies etc.) will be evaluated utilizing first experiences with the pilots. Finally, a first approximation of the cost/effect ratio will be sketched, i.e. the question of whether the effort of using SPECIAL technology pays off in the given pilots and potentially in other industry use cases will be given a first (preliminary) answer.

Testing and test plans are based on use cases and requirements. Since the use cases and objectives are very specific for each industry partner, purpose and testing requirements for the tests are use-case specific as well.

Nevertheless, two requirements apply to all pilots:

Security and Privacy: While these are "sanitary features" of usual products (security and privacy need to be present and sufficient with respect to applicable laws and state-of-the-art technology), in the case of SPECIAL, particular attention needs to be put on fulfilling all privacy needs. SPECIAL needs to provide methods and tools to implement GDPR compliant applications, while the business purpose of the applications is not "privacy". This results in the need for special attention to security and privacy on the conceptual as well as on the implementation level.

Usability: Even though the number of users of the initial versions of pilot implementations is limited, it is obvious that usability needs extra devotion and effort since users will not make use of their control forces if they are not willing or able to use the respective tools/interfaces. Thus, bad usability will either result in poor functionality of the products (because users will not allow any use of personal data) or it will leave the impression that user's don't care anyway.

3 Pilot 1 (Proximus)

3.1 Summary

A detailed description of the Proximus use case can be found in deliverable D1.5 (2nd version of the requirements definition). The use case concentrates on the following concepts:

- Recommender Engine for events at the Belgian coast
- Mobile user interface
- Data subjects of Proximus
- Data requested from data subjects:
  - Location
  - Television viewing

The first iteration, an initial end-to-end version, albeit for only 5 data subjects, was ready for internal Proximus beta testing in 2018. In 2019, a second iteration is being worked on. This second iteration will extend the data processing and aggregation with transparency and compliance functionality based on deliverables D3.4 & D4.3.
And for the SPECIAL project itself, Proximus is asked to evaluate the usefulness of the SPECIAL components (called building blocks) for its use case.

3.2 Objective and evaluation for Proximus

As a general objective, Proximus wants to test the willingness of its customers to share personal data.

The current use case is not commercial, precisely to avoid being valued for any immediate commercial return. What is more important, is the question as to whether sharing personal data attracts or scares people. We expect this answer to be dependent on several variables:

- Intuitive interface
- Getting something in return
- Age of the data subject (e.g. Is there a difference between millennials and 50+ people?)
- (Mobile) IT awareness of the data subject
- Privacy awareness of the data subject

Specifically, in the first iteration (with 5 data subjects), we were looking into technically testing whether the solution works end-to-end, and focused highly on the **intuitive interface**, to “attract” enough data subjects for the second iteration (with 50 data subjects). This was successful as all data subjects agreed to sign up for the second iteration of tests. **The data subject’s age range was from early 30’s to 60+, and all were very much privacy/mobile/IT aware**. They found the interface intuitive, but it must be said that the interface only asked for basic consent on three types of personal data and did not yet have a privacy dashboard.
The ”**getting something in return**” was not good, as the quality of the recommendations was rather low, due to a capacity issue within Proximus on the data science side to improve the recommender engine. This was addressed to the Consortium, but the building of the recommender engine is considered not part of SPECIAL and therefore, impossible to reassess the use of Consortium capacity/funds. As an alternative, the Proximus team got the help from a trainee student whom developed the first version of the recommender engine and gave suggestions how to further enhance it. For the second iteration of the tests with the data subjects, we hope but cannot guarantee, an improved version of the recommender engine.

3.3 Data protection considerations

On July 19th, 2018, the current state of the pilot implementation was presented to the internal Proximus Privacy Council and approval was obtained to formally approach 5 data subjects (internal to Proximus and all part of - or very close to - the SPECIAL project team who showed informal willingness to participate) and to explore the technical solution to retrieve and store the TV viewing records.

Having access to location/TV viewing/browsing history is a very sensitive matter for the Privacy Council, and to get an initial Go, it was decided to withhold location and browsing history for future iterations. This incremental approach was recommended to avoid ending up in the more complicated governance of the Proximus project methodology with a release calendar beyond our control.

The project team will have to go back to this Privacy Council on June 20th, 2019, to ask for more approvals for the second iteration (higher number of data subjects (50) and adding location as a data source).

The SPECIAL project team made the following assessment as to the identity of the Data Controller and the Data Processor.

- Proximus is the Data Controller.
- Proximus itself uses many external cloud services when it comes to prototyping, as it is simply faster and cheaper. For the SPECIAL project, budget and time constraints led us also in this direction and therefore we use Microsoft Azure as a Data Processor for the Data Science recommendations. (Please note that this will be different when running in production)

3.4 Dissemination within Proximus

The involvement of the Proximus project team is disseminated within Proximus via:

(1) Alignment with the Proximus project team working on GDPR compliance for all IT/CRM systems
(2) Alignment with the Enterprise Architecture team: One SPECIAL project team member is part of the Enterprise Architecture team
(3) Alignment with the Proximus Privacy Council. Next meeting is foreseen on June 20th, 2019.
(4) Marketing on the internal intranet when going for the second iteration (50 data subjects). A SPECIAL project video would facilitate this task. The making of a project video was discussed in the Consortium but the SPECIAL components and the use case implementations were considered not mature enough yet. We will make use of more static content.
(5) Alignment with the Consumer Business Unit with its innovation initiatives.

The volume and streaming of payload consumer data for the SPECIAL Proximus use case obviously qualifies to be called Big Data at Proximus. In 2017, Proximus decided that all (old and new (Big) data) initiatives will simply be called Data initiatives.

3.5 Iterations of the Proximus use case

An estimated path to integrate the SPECIAL use case into the existing MyProximus consumer APP is shown in Table 3.1 .

Table 3.1 Iterations of the SPECIAL use case at Proximus

Functional area	**Iteration 1 (M20):** **(End-to-End Proof of Concept with 5 data subjects)**	**Iteration 2 (M34):** **(limited pilot with 50 data subjects)**	**POST SPECIAL:** **Possible Integration within Proximus**
Identity & Access Management	Firebase (manual)	Based on JSON webtokens https://jwt.io/ (open, industry standard RFC 7519); Secure but not production ready	MyProximus Identity & Access Management
Frontend UI	(developed by TUB) One basic vertical page (React.js)	(developed by TUB) Compliant interface validated by the Consortium Legal partners (incl T&Cs) (React.js)	MyProximus libraries with input from Iteration 2
Privacy Dashboard (TUB)	Was not implemented	Implemented and contains the data subject's rights (right to access; limited rectification; limited erasure)	Integrate in MyProximus which currently only has a basic Privacy Dashboard (no right to access/rectify/erase)
Layered Privacy Statement/Notice	Dynamic Consent suggested by SPECIAL team but still in ideation phase	Dynamic Consent suggested by SPECIAL team but still in ideation phase	Evaluate
Consent Datastore	Firebase Database	MongoDB with https://nodejs.org/en/ and http://expressjs.com/	MyProximus Identity & Access Management
Event Datastore	MS Azure	MS Azure	MS Azure
Profile Datastore	MS Azure (MySQL / MongoDB)	MS Azure (MongoDB)	MyProximus Interest Profile dB
Payload data filtered input stream	MS Azure MySQL for (real) TV viewing records, or manually marked TV viewing list by each data subject	MS Azure MySQL for (real) TV viewing records, or manually marked TV viewing list by each data subject	Kafka + datastore (MySQL / ElasticSearch)
Machine learning	Python	Python	Python
SMS / email sending	Proximus Enco SMS API	Will be in the APP; No more need for additional SMS/email	In the APP

3.6 Use of SPECIAL components

The following section describes where and how the Proximus use case is using components from SPECIAL.

3.6.1 Policy Language

As mentioned in D2.5 (Policy Language V2), the usage policy language is meant to express both data subjects' consent and data usage policies of data controllers in formal terms, understandable by a computer, to automatically verify that the usage of personal data complies with data subjects' consent.
For an industry partner the challenge is to convert the theoretical basis of the policy language into a workable product. This has been accomplished with the help of Consortium partners CeRict and TUB. Figure 3.1 explains the relation that exists for a data subject between permission (=consent), policy and data.

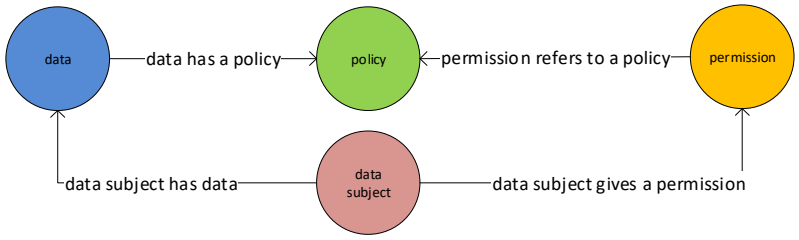


Figure 3.1. Relation between Data Subject and Data/Policy/Permission (in RDF notation).

Below is a theoretical example of a possible implementation of such a policy for the Proximus use case (source CeRict and D2.5):

```
P2: Use personal data for recommendations
{
      hasData:    {
                  Personal Identifiable Information
                  AudiovisualActivity + Demographic +
Location + Navigation + OnlineActivity
                        + TelecomActivity
                  }
      hasProcessing:   Collect + Copy + Transfer
      hasPurpose:      PxsEventRecommendation
      hasRecipient:    Ours
      hasStorage:      {
                  hasDuration:     StatedPurpose
                  durationInDays   < 42
                  hasLocation: { EU ControllerServers }
                  }
      hasLegalBasis:   Art6_1_a_Consent
      hasDuty:    GetValidConsent
}
```

The above example is formulated in an extension of JSON, that can be related to the standard OWL2 formulation described in D2.5 as follows:

- curly brackets correspond to ObjectIntersectionOf
- '+' corresponds to ObjectUnionOf
- has XXX:Y corresponds to ObjectSomeValueFrom(hasXXX,Y)

A more practical implementation of a policy, at the cost of enlarging it, is the following (source TUB). The policy P2 above would convert into 18 policies of the type below. This policy also has an internal identifier inside its definition ("id":1):

```
{
  // Collect location data
  "id": 1,
  "data":
"http://www.specialprivacy.eu/vocabs/data#Location",
  "purpose":
"http://www.specialprivacy.eu/vocabs/purposes#Telemarketi
ng",
  "processing":
"http://www.specialprivacy.eu/vocabs/processing#Collect",
  "storage":
"http://www.specialprivacy.eu/vocabs/locations#OurServers
",
  "recipient":
"http://www.specialprivacy.eu/vocabs/recipients#Ours",
}
```

The links in the above policy elaborate on the details.

Remaining areas for investigation are:

- Negation: The currently defined policy language does not allow negation nor exclusion. For instance, "you can track my location everywhere except on weekends at certain locations" is currently not possible.
- Linked data used in policy definition: What if the content at the link location changes? Does this require a new consent from the data subject? Perhaps policy versioning is a solution for this.

3.6.2 Sticky Policies

The sticky policies concept is still in the mission statement of SPECIAL[1] but research into it has not really materialized and there is only one proposal as to how to encode it. It is not a requirement for the Proximus use case but would nevertheless be seen within Proximus as an added value for other use cases. A minimum (grid) overview of the possible solutions or research lines could be expected from SPECIAL. WU will further explore how sticky policies could be used in SPECIAL.

[1] https://www.specialprivacy.eu/ … harness them with *sticky* policies….

One proposal for encoding sticky policies (source CeRict) in business policies and consent policies consists of attaching the sticky policy to the recipient.
For example:

```
Transfer Policy with Sticky Policy:
{
  hasData: XXX
  hasProcessing: Transfer
  hasPurpose: YYY
  hasStorage:ZZZ
  hasRecipient: {
   RecipientA
   underStickyPolicy:
    {
     hasData: XXX'
     hasProcessing: YYY'
     hasPurpose: ZZZ'
     ...
    }
  }
}
```

It does however not seem to solve the issue of keeping the policy with the data (wherever the data travels).

3.6.3 Privacy Dashboard

The development of the Privacy Dashboard is of high interest to Proximus as well as the usability research and tests that are ongoing in WP4.
It will be essential to display the innovative nature of SPECIAL as this will be the consumer facing part that wants to be the alternative to pages of legal text that everyone just blindly accepts when wanting a service.
Proximus and probably many industry partners have quite a challenge to get consent in a user-friendly way in its own privacy interfaces for one or more purposes that they might have.
The data subject's rights (right to access; limited rectification; limited erasure) are being implemented and are shown in the figures 3.2 to 3.6 (unfinished version).

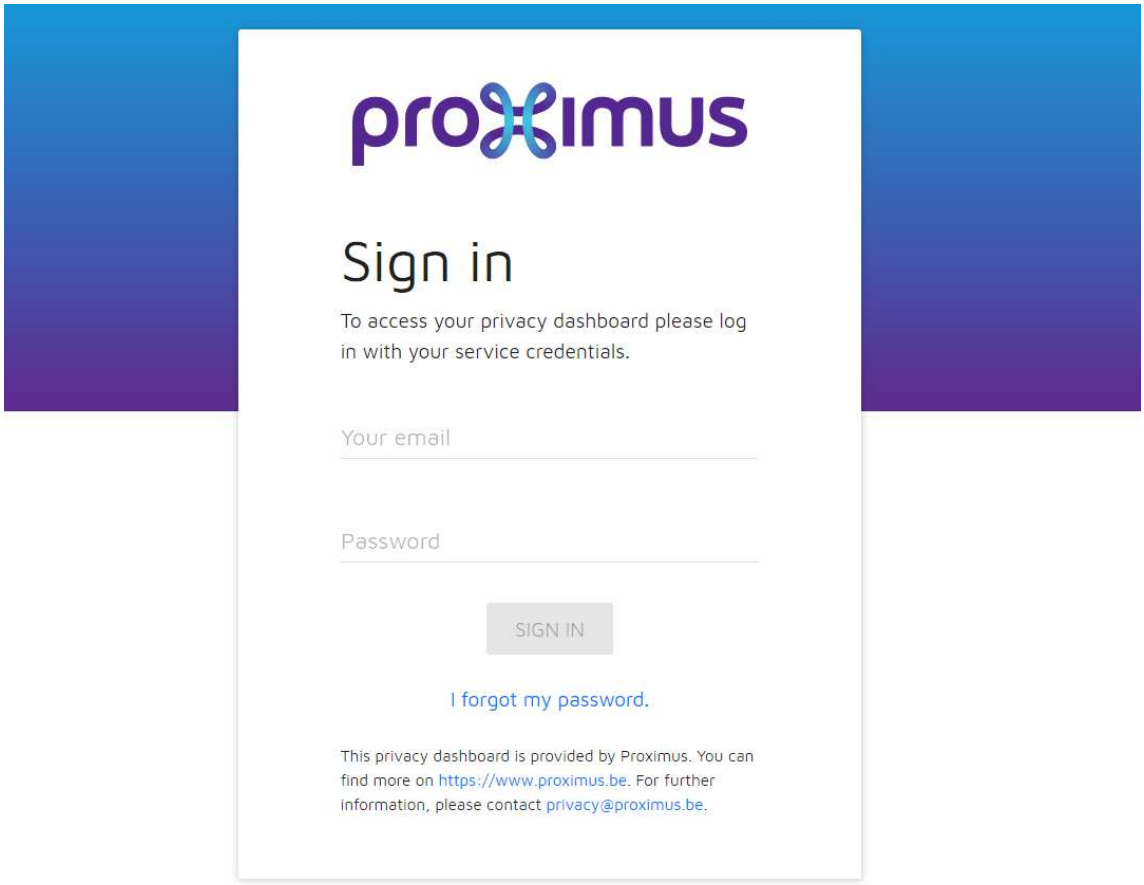


Figure 3.2 Login screen

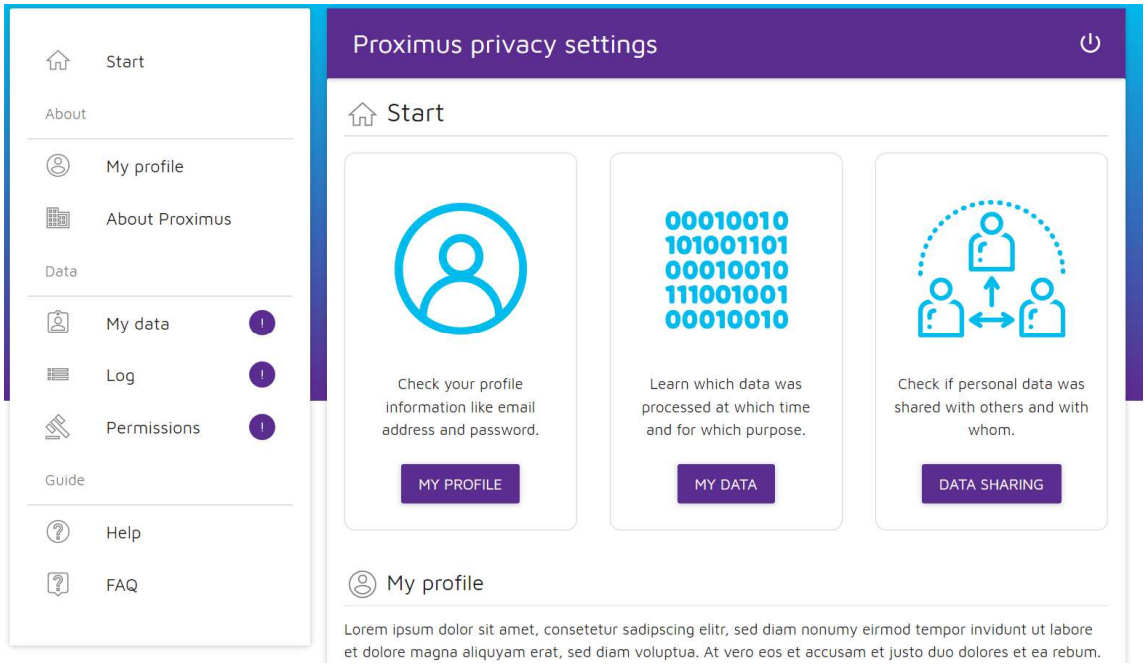


Figure 3.3 Menu of Privacy Dashboard

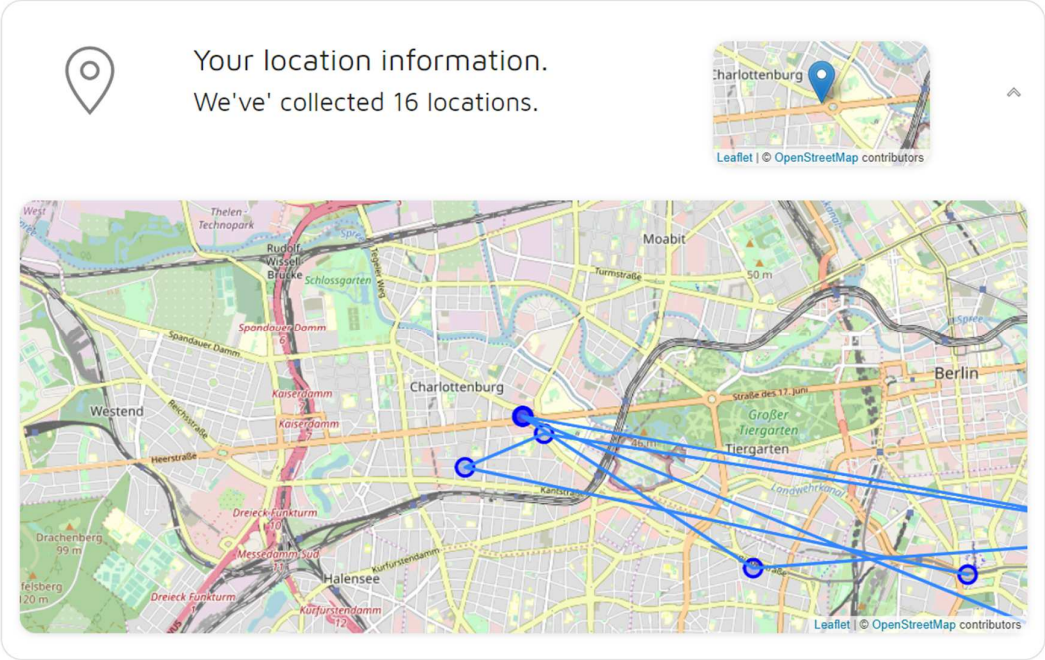


Figure 3.4 Log of locations that were collected for the data subject.

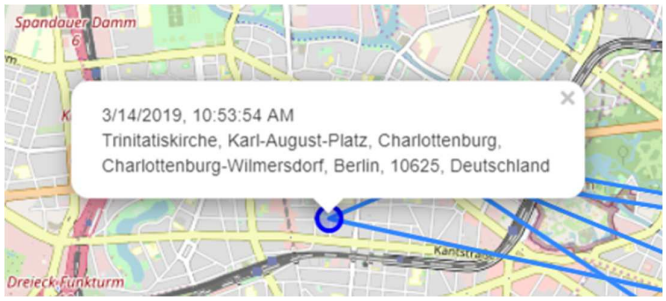


Figure 3.5 Details of one collected location.

Figure 3.6 Menu item TV viewing data events.

3.6.4 Compliance checker

Proximus experimented with the ex-post compliance checker as described in D3.4 and available at https://git.ai.wu.ac.at/. It demonstrates the capabilities of such a compliance checker. In the current Proximus use case, which has also been built from scratch, compliance is inherent to the design and ex-ante checking is done by default. Proximus did not experiment yet with the ex-ante compliance

checker as mentioned in D3.4 as the 'personal-data-gateway' component was not developed at the time of doing the first experiments.

3.6.5 Event log

Proximus has not specifically deployed the SPLog mechanism as described in D2.7 by WU. However, it used the content of D2.7 as inspiration to implement a derived version.

For example:


```
{
  "success": true,
  "message": "Successfully loaded log entries",
  "result": [
    {
      "_id": "5c8913ec3c827659934b59e9",
      "user": "5c8791202be791080a464af9",
      "process": "5c6e96a849199380c2388497",
      "data": "http://www.specialprivacy.eu/vocabs/data#Location",
      "purpose":
"http://www.specialprivacy.eu/vocabs/purposes#Telemarketing",
      "processing":
"http://www.specialprivacy.eu/vocabs/processing#Collect",
      "storage":
"http://www.specialprivacy.eu/vocabs/locations#OurServers",
      "recipient":
"http://www.specialprivacy.eu/vocabs/recipients#Ours",
      "timestamp": 1552487404287,
      "instanceData": {
        "lat": 52.5129013,
        "lon": 13.3201085,
        "streetName": "TEL, Bismarckstrasse, Charlottenburg,
Charlottenburg-Wilmersdorf, Berlin, 10625, Deutschland",
        "decision": "Agree",
        "timestamp": 1552487403050
      }
    }
}
```


3.6.6 Dynamic Consent

Dynamic consent as proposed by ERCIM and ULD (see deliverable D4.3 for a detailed definition) is still in "research modus" and at this moment not in the Proximus use case. The backend architecture and frontend wireframes (as an example) are still under discussion. Dynamic consent could be beneficial and a possible success story of SPECIAL and the Proximus use case. It should be discussed thoroughly at the next Consortium meeting.

4 Pilot 2 (Refinitiv)

4.1 Summary

The Refinitiv pilot seeks to both satisfy our KYC use-case and then to generalising our learnings to support arbitrary use cases in the financial data supply chain. We've focussed our efforts in four key areas:

- The policy language and the possibility of situating it within a broader business information model that governs the management and distribution of data within the financial data supply chain.
- Modelling business processes in the context of the GDPR and the UX to support non-technical domain experts
- The efficacy of automated compliance checking of processing both against the GDPR (static checks) and against the consent statements of data subjects (dynamic checks)
- Product definition: the tools and services required to support the automated enforcement of the GDPR.

4.2 Pilot objectives

The pilot is designed to answer the following questions:

Policy Language, Business Information Models, and Standardisation

- Does the policy language and associated vocabularies, as currently specified, capture all the relevant information required to decide compliance to the GDPR? If not, what use cases can we describe to add to the requirements for the next iteration of that language/vocabularies.
- Can we integrate the policy language into a larger business information model that describes the rights and obligations over data in a content supply chain? (This model covers not only privacy considerations but also licensing obligations and other regulations relevant to a data supply chain).
- Can we capture the policy language within this business information model using concepts and relationships familiar to the finance industry?
- Can we import the vocabularies developed by the W3C Data Privacy Vocabularies and Controls CG (DPVCG) into the model?
- Can we then check GDPR compliance using this business information model?
- How much demand is there within the financial industry to standardise a business information model that allows automated compliance checking?

Business Process

- Can we provide a UX such that staff currently managing our Know-Your-Customer workflows can confidently specify the processes underpinning them – or will we have to rely on specialists with a technical understanding of the policy language?
- How should we surface the results of compliance testing to privacy professionals and regulators?
- How to we generalise this UX to cover a wider set of use cases?

- Do our processing policies provide a true reflection of our right to process personal information under the GDPR? If not, how should they be amended to be so
- Are our processing policies a complete and correct reflection of the processing we actually do on personally sensitive data in our Know-Your-Customer workflows? If not, do we need to amend the policy language to provide such a complete and correct description?

Compliance Checking

- Can compliance checking be fully automated – without any recourse to manual intervention? If not, what kinds of manual intervention are needed, and when?
- Given the volume of compliance checks over consent that our live systems are likely to generate, can the Special components make decisions fast enough: we're looking for millisecond response times.
- Do smart contracts on the blockchain provide a suitable implementation environment for compliance checking?
- What is the scope of the completeness and correctness guarantees that we can offer?
- If we are to virtualise, externalise, and automate compliance decisions, how should we provide/present the resulting service?

Product Definition

- What are the components required to deliver the end-to-end solution?
- Who are the human actors in the end-to-end solution - and what use cases do they need to satisfy?
- Does any single component have commercial viability independently of the end-to-end solution?

4.3 Data protection considerations

The data used in this pilot will all be synthesised data designed to support the objectives described above. No 'genuine' personally sensitive data will be used.

4.4 Pilot components

The pilot tests the following Special components:

1. The policy language and vocabularies: are they expressive enough?
2. The compliance algorithm: does it provide the answers we expect?
3. The compliance engine provided by TenForce:
    - Does it correctly implement the compliance algorithm;
    - Are there cases that require manual intervention;
    - Can we get fast enough decisions (i.e. in milliseconds)
4. The ODRL Regulatory Compliance Profile

The pilot also develops the following components:

1. A UX proof-of-concept developed internally to explore the creation and maintenance of processing policies.

The target audience for this UX are the staff that currently design and execute our Know-Your-Customer workflows. There are many of these workflows for different clients, different countries, and different types of financial transaction.

The Proof of Concept (PoC) seeks to transform this informal knowledge into the formal processing policies specified by the Special project. If successful, we will be able to expand the scope of our coverage without recourse to technical specialists with knowledge of the underlying representation.

2. Implementations of the compliance algorithm both as smart contracts on the block chain and in serverless cloud-based environments.

3. The integration of the ODRL Regulatory Compliance Profile proposed by WU and the W3C Data Privacy Vocabularies and Controls CG (DPVCG) ontologies (both of which are still under active development) into a wider business information model that governs the distribution and use of data in the financial data supply chain. A detailed description of the use of the ODRL Regulatory Compliance Profile and the DPVCG vocabularies will be provided in the final iteration of this deliverable.

4.5 Evaluation criteria

We are using the legal expertise both within the Special project itself and the Refinitiv Privacy Office to 'sense check' first the processing policies themselves and then the compliance decisions made by the compliance engine. Are we getting the results we expected?

The Know-Your-Customer team working with the UX-experts within the Refinitiv Innovations Labs are evaluating the viability of using the existing Know-Your-Customer staff to create and maintain processing policies.

Software architects attached to the product will consider the response times. Given their sizing estimates, they must decide whether to pre-compute decisions or whether to run them in real-time.

We're also working with the Proposition and Product Development functions within Refinitiv to clarify the commercial potential for tools and services based on the Special research.

5 Pilot 3 (Deutsche Telekom)

5.1 Preliminary Remark

This section on Deutsche Telekom's pilot is part of a "living document" certain sub-chapters stay unchanged or undergo only minor modifications and thus might be skipped by readers who are well aware of the context, plan and implementation as described in D5.1. However, the remarkable progress made in the pilot is covered in this chapter and deserves reader's attention. Therefore, it is recommended to focus on the following sub-chapters covering the most visible and relevant changes compared to D 5.1.

- 5.2.3. (was 5.1.3, new)
- 5.4 (architecture, revised)
- 5.5 (data flow, new sub-chapter)
- 5.5 (SPECIAL components, new sub-chapter)

Since the use case's and pilot's time schedule is now basically back on track, the present chapter 5 serves as a good overview on and starting point for the last period of the project, focussing on evaluation and test of the implemented version of the pilot.

5.2 Use case description (short recap)

5.2.1 Additional use for device (client) based QoS/location data

Prior to SPECIAL (and prior to the use case pilot implementation), a DT app (Customer Network Experience/"CNE-app", by Deutsche Telekom) collected data that was (and is) used only for network quality improvement. Some components of the collected data could also be used for other purposes and by other units, e.g. by Motionlogic, a legally independent subsidiary of DT, to improve and verify algorithms in location based services. This leads to an interesting business opportunity that was impossible to implement under EU law until SPECIAL came up with an innovative solution.

5.2.2 Current (pre-SPECIAL) situation

Users can download and install the CNE-app from the app store (Apple) or Play Store (Google). The purpose is very clear and the user interface offers the key functionality on screen. Of course, the privacy statement and terms and conditions are presented at first launch. Then, the user can initiate manual "speed tests" or change certain settings, e.g. turn on a "diagnosis mode". Figure 5.1 shows the original app.

Figure 5.1 : CNE-app (customer network experience) with a slider to activate "diagnostic mode"; we intended to switch on "non-anonymous mode" similarly

1. ***Telekom Deutschland GmbH (DT)*** collects Quality of Service data (QoS) for its' mobile network service. One source of this QoS data is a smartphone app called "CNE – Customer Network Experience" (see). Each data set collected here includes (among others) geo location information measured via device GPS. Radio data (reception quality etc.) are collected, aggregated, condensed and sent to a database. Data sets are by default anonymized and/or pseudonymized to protect user's privacy. Users give their informed consent during installation of the app. Data sets are then collected and statistically evaluated by the service quality department to improve the network quality. The department responsible for running and further developing the app and database is looking for additional use of the collected data, e.g. gain insights by applying AI (artificial intelligence) techniques to the data.
2. ***Motionlogic*** (https://www.motionlogic.de/blog/de/), an independent Spin-off company of DT, uses anonymized and time-delayed data of mobile phone usage (location data, cell-tower location) to offer Business-to-Business (B2B) location services, e.g. heat maps of population density in urban areas or traffic infrastructure. Motionlogic never exports individual data or even data sets received from DT (T-Mobile brand). Rather Motionlogic does the requested processing internally and only delivers the results (e.g. heat maps). Due to limited quality of data, the added value is limited as well. Better data, e.g. individual user tracks or even more accurate location data, would improve the results dramatically. However, due to lack of explicit "Opt-In" by end users, Motionlogic acts way below its theoretical capabilities and capacities. Motionlogic needs more "Opt-In" users among DT customers.

5.2.3 Target scenario for pilot implementation

A new version of the CNE-app collects more frequently data, in particular more location data, and reduces (or abandons) anonymization/pseudonymization. The now much more valuable data is shared with Motionlogic (but not further) to enable better location based evaluation for business partners and monetization. To do so, much deeper consent needs to be given by users in the form of an explicit (and informed) "Opt-In". We assume that users choose to "Opt-In" if they keep control over their data and perceive a certain customer benefit. Policies as developed/supported by SPECIAL and the privacy dashboard are the tools to guarantee user control and transparency.

In the current implementation, the user can give consent to "additional scientific use" of his data (in German "Wissenschaftliche Zusatznutzung") as shown in Figure 5.2.

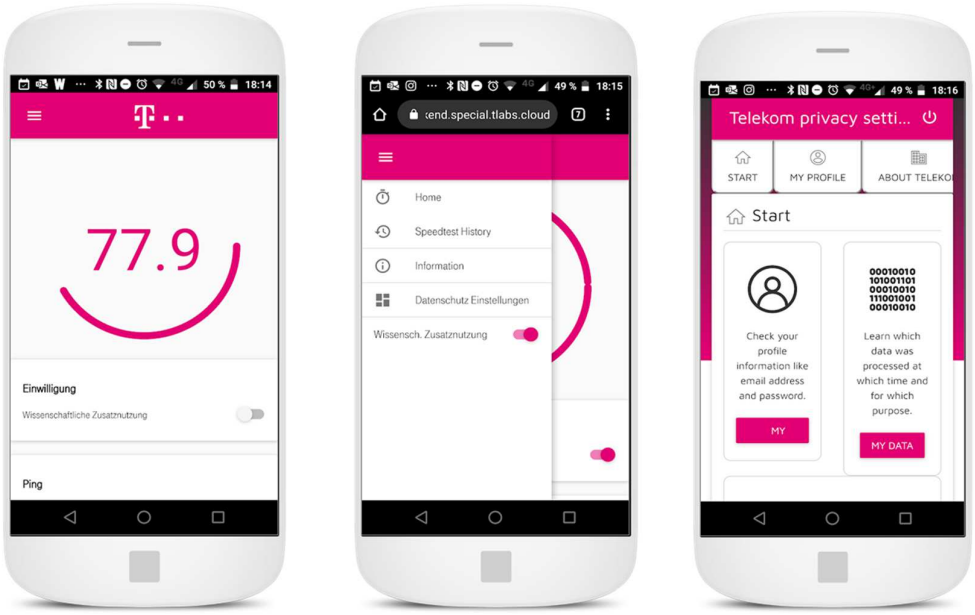


Figure 5.2 : SPECIAL version of CNE-app (customer network experience) with a sliders to activate "Scientific use" and a screenshot of the current "Telekom privacy dashboard"

Please refer to deliverable D 1.5 and D1.6 for more detailed descriptions of the use case.

As a further development of the DT use cases (especially as described D1.6), we decided to simplify the policy and minimize user's options to edit policies in favour of general applicability in DT's IT- and business infrastructure, and expect a larger number or users/data subjects to test scalability (in later iterations). In other words: dynamic consent is an optional part of the current initial implementation. The policy used here is more a stepwise (and explicit) approval. DT is currently assessing D1.6 and the concept of dynamic consent therein. In future versions DT might use the "dynamic consent" approach to simplify user interaction and reduce the individual consent-granting actions by users.

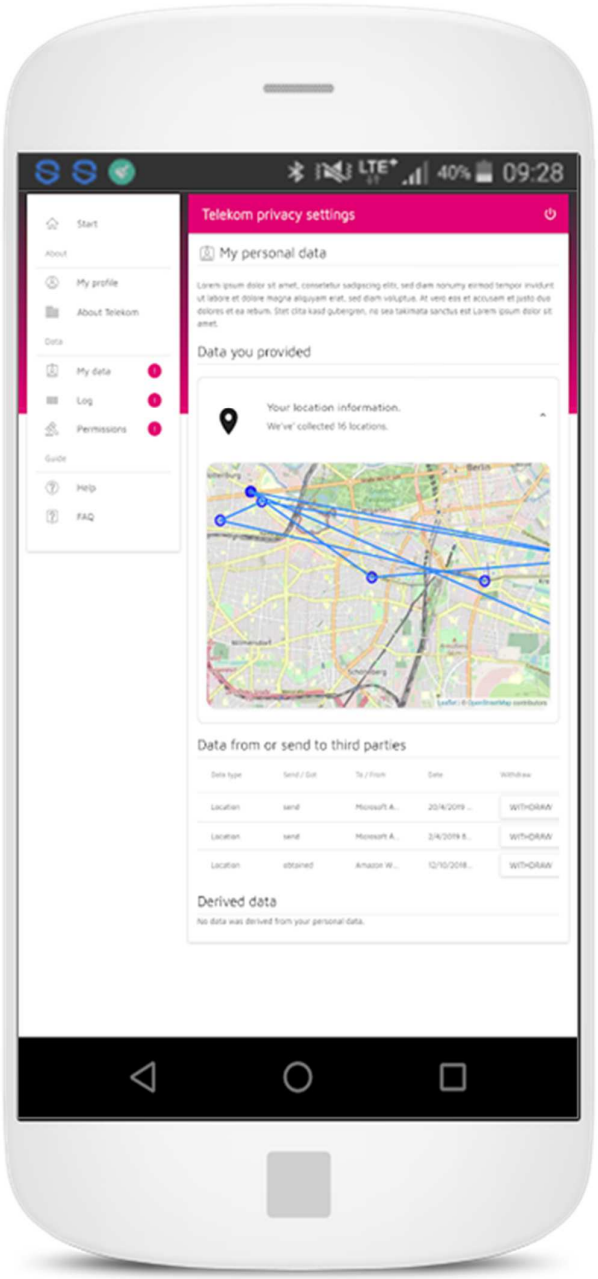


Figure 5.3 : SPECIAL privacy dashboard, launched from the CNE-app, showing the "My data" section

Since transparency is a key requirement and a core feature of SPECIAL, the use case also covers this approach by giving the end user access to his specific "privacy dashboard" directly from the app: The SPECIAL CNE app contains a link to the SPECIAL sever running the (location) data base, policy engine and privacy dashboard (transparency tool), see Figure 5.3. The user can simply follow this link on the smartphone and monitor which data has been collected and was transferred or processed to/by a third party (i.e. Motionlogic). The privacy dashboard also allows the user to remove his data from the database and/or withdraw the consent give before.

5.3 Objective of pilot implementation

5.3.1 DT's view on Big Data and AI and their relevance to SPECIAL

DT owns a large amount of valuable user data, which it needs, to deliver the high quality services the users expect. Since DT has a first class reputation in terms of security and privacy protection, DT is more than reluctant to experiment with user data, potentially breaking the valuable trust that was built up over time.

Nevertheless, DT acknowledges the potential additional value of this data and the results from the data analyses. In particular, when comparing with OTT ("over the top") players such as GAFA (Google, Amazon, Facebook or Apple), DT sees huge opportunities in adding more and better services to customers based on "Big Data Analysis" or "AI".

DT always puts the customer and customer protection first and never risks any legal or reputation threats. Therefore, SPECIAL and the observations/experiences made in the project are of particular value for DT.

In SPECIAL, DT wants to examine opportunities and limitations of privacy tools compliant with GDPR (and other legal regulations) in the context of a scalable, yet already "Big Data" use case: The CNE app today (prior to SPECIAL supplements) has about 20.000 users, usually about 5% of them (1000 users) are online concurrently.

Since the app was launched (in 2017) these users produced 20.000 to 70.000 datasets per day, about 1 M datasets per month. This is the base figure for the "original" CNE app. DT would expect somewhat smaller numbers for non-anonymizing version of the app. However, neither the "original" nor the "SPECIAL supplemented" version of the app would be pushed in app store marketing. So user numbers are assumed to be limited on purpose. The resulting numbers (of users, datasets etc) are clearly "Big Data" but still relatively small compared to the amounts of data telecommunication operators as DT usually deal with. Therefore, a successful internal evaluation of the "SPECIAL CNE app) is expected to open doors towards the monetization of real Big Data treasures that lie hidden in the carrier's operational data centers.

5.3.2 Objectives for the first iteration of DT pilot

DT's view on the pilot implementation is that it wants to see and test a "Proof of Concept" (PoC), not a product (or even a Minimal Viable Product (MVP)). This means that DT is interested in knowledge, experience and decision support for future developments. The implementation is not intended to become part of DT's regular operational IT infrastructure.

DT's pilot is based on prior work by SPECIAL consortium members. In particular, D1.6 was used as basis for intense discussions since it contains most interesting (yet not fully assessed) concepts. D4.1 (privacy dashboard) and D4.2 (Usability testing) helped to come up with implementation decisions and formed the objectives defined for this pilot. Also WP3 (in particular D3.3, Backend scalability) helped to focus on a simple use case with relatively many users/data subjects.

DT's main objectives for the pilot implementation are:

- **Proof of feasibility** of technology developed in SPECIAL (privacy policies, policy engine, privacy dashboard/transparency tools etc.) in conjunction with DT's existing IT infrastructure and internal processes. This feasibility includes technical, legal and organizational aspects. DT as an agile and modern telecommunications service provider needs to know how and how far cutting edge data processing tools, especially privacy related ones, will affect business

operations: Does DT need to change internal processes (e.g. the PSA-process, see below) to allow such technologies to be implemented?

- **Technical benefit for DT/Motionlogic (ML)** The pilot helps to optimize DT's and Motionlogic's analysis tools. The tools use anonymized user data to deduct certain insights and allow predictions on the behavior of unknown, anonymous people based on previous experiences. The optimization and validation relies on a certain amount of confirmed (and thus non-anonymized) data sets. These data sets will be comprised of the data provided with full user consent using SPECIAL's policy mechanisms.
- **Additional user benefit**: Part of the analyses by DT will be the identification of network and coverage issues. DT currently considers to share (parts of) this knowledge of the current "health" of the network with effected customers. Thus one potential additional benefit of the pilot would be to (possibly) share relevant network quality information with users. To determine for whom the information is "relevant" (i.e. who is located close to the issue scene), only personal data can be used, in our case data, from users who gave the requested consent.
- As a **"hygiene factor"** (a feature/factor that must be present anyway, even if it does not contribute to the business value of the product) we assume (and require) that the pilot fulfils DT's corporate privacy & security standards. Especially since this is a privacy related project, DT values the protection of user data not just inside its data centers, but also protects it against external threats.

5.3.3 What is NOT in scope

DT does not plan to monetize user data. Neither today nor in the foreseeable future will DT sell their users' personal data. The pilot will not result in any direct marketing activities. DT does not even plan or intend to build personalized services for the end users based on the data collected in the pilot.

5.3.4 Public challenge

The main challenge for the pilot will be to convince as many users as possible to "Opt-In" to the use of their personal data (i.e. location data). This is not so much a "hacking challenge" but rather a proposed challenge to formulate the privacy information accordingly and let the user make a truly informed decision about the use of their data.

A resulting challenge (a core feature of DT's pilot) is the use and acceptance of the "privacy dashboard". We assume that the more users check and control their settings using this tool, the better is the overall acceptance. Of course, we assume that people will not only use the tool to "opt-out". So the intensity and type of use of the transparency tool will be a key aspect of this pilot. This also applies to the next iterations of the pilot/deliverable.

5.4 Pilot implementation architecture

The original CNE app and use case (prior to the advanced version to be piloted in SPECIAL, referred to herein as "SPECIAL CNE app") is based on a straight forward data forwarding schema: Network Quality Data gained on user's/customer's device are uploaded to buffer server and then forwarded to the DT data center where they are evaluated in an anonymized form.

The analysis results are then transferred to Motionlogic for further processing and presentation. See Figure 5.4 for more details. The analysis results are completely anonymized and individual data sets cannot be reconstructed by Motionlogic. Obviously, Motionlogic also cannot assign any data set to a particular user/customer.

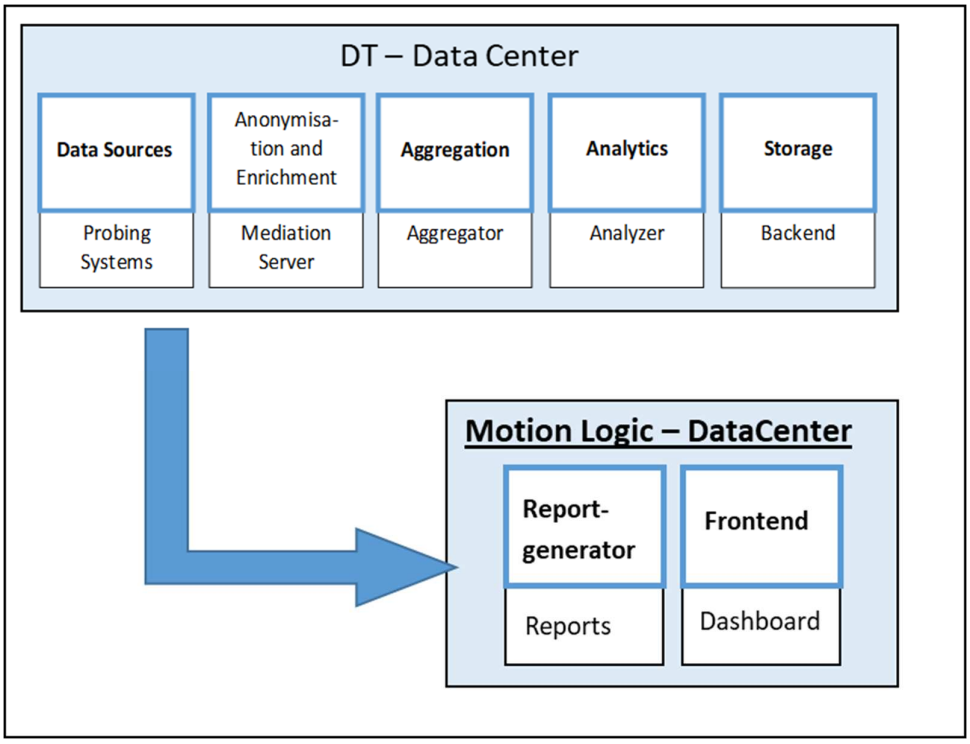


Figure 5.4 : Current situation: data is collected and analysed in DT data center. Anonymized results are exported to Motionlogic for further processing/presentation

Motionlogic's operation and business model does not require any individual data set or any link to individual users. Therefore, the current implementations and data quality seem to be "good enough" for Motionlogic.

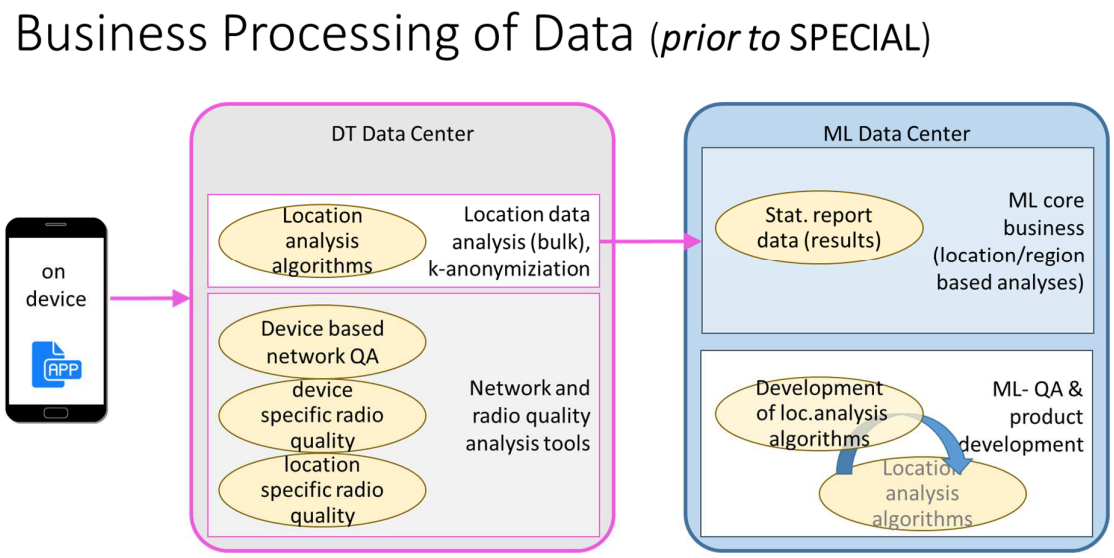


Figure 5.5 : Business model: data is collected and processed/analysed in DT data center. Monetization and software development are done by Motionlogic in the Motionlogic domain (and data center)

From the project (use case) point of view, CNE-app data are just transferred into DT data center (together with numerous other sensor data from different apps/devices) as Figure 5.5 depicts. Even though CNE-app data (location data) are of much higher value for Motionlogic (and potentially other 3rd parties), the CNE data points are merged and "equalized" to the (low) quality of standard cell-tower based resolution.

To improve quality of Motionlogic's algorithms, individual data sets with concrete (individual) users are necessary. SPECIAL delivers the necessary tools and mechanisms to collect informed user consent, give the user full transparency, allow him to remove his data (and withdraw consent) if needed. Since the pilot implementation should not put any running DT process at risk, the system architecture uses a "bypass" mechanism for the privacy data (policies, log data and user interaction). This gives the user full control and does not touch mission critical processes within the company. **Error! Reference source not found.** depicts the architecture with the "bypass" around the DT data center.

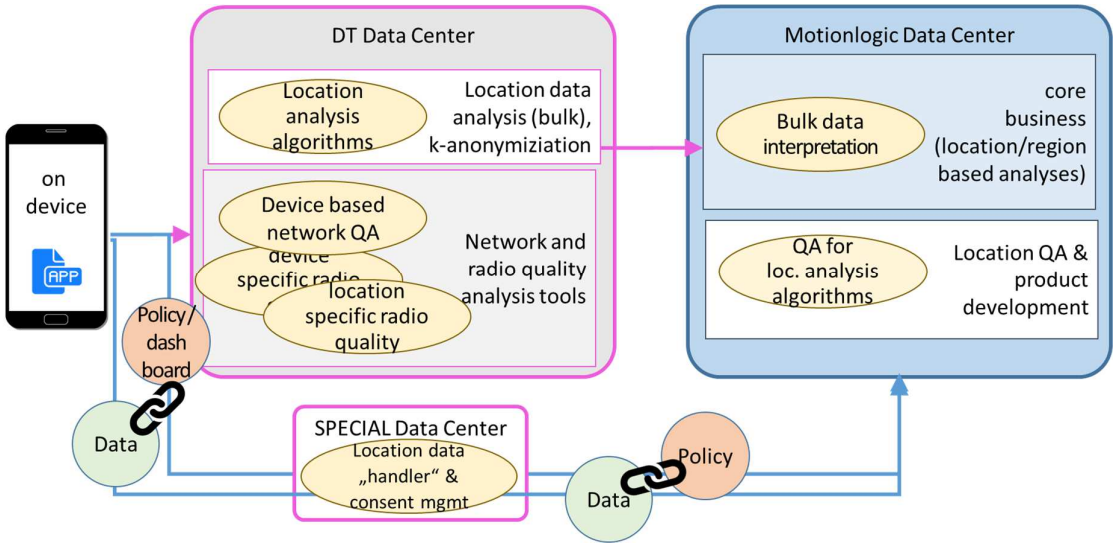


Figure 5.6 : architecture: SPECIAL tools and methods are added to the original process. Non-anonymous data will be used legally, with transparency and user control is provided

Figure 5.6 shows the pilot's approach to demonstrate the opportunities provided by SPECIAL: A dedicated "SPECIAL Data Center" handles both, the (non-anonymous) transfer and storage of "payload"/location data, and consent/privacy/transparency management:

If the user gives his consent (in the app/on device), location data ("data/payload/content") are transferred to the SPECIAL data center (green circle).

At the same time the consent (and the attached conditions, i.e. the "policy") is transferred/communicated to the (same) SPECIAL data center. Thus data and policy are linked.

Motion logic can now receive the data according to the policy from the SPECIAL data center.

Transparency and control ("privacy dashboard") for the user are conveyed via the same link between app/device and SPECIAL data center.

Even though the SPECIAL components are currently completely outside DT's core data centers, this architecture will definitely prove the validity of the approach and does not contradict the idea of integrating the functionality and concepts (linked data and privacy policies) directly in the core IT processes of DT.

5.5 Data flow

A dedicated analysis of the flow(s) of data was carried out to estimate the measures needed to comply to DT-internal rules, GDPR and other legal regulations. Since the original CNE app already was approved by security and DPO authorities, we could assume that this would be a stable starting point for the analysis. Figure 5.7 shows the pre-SPECIAL situation:

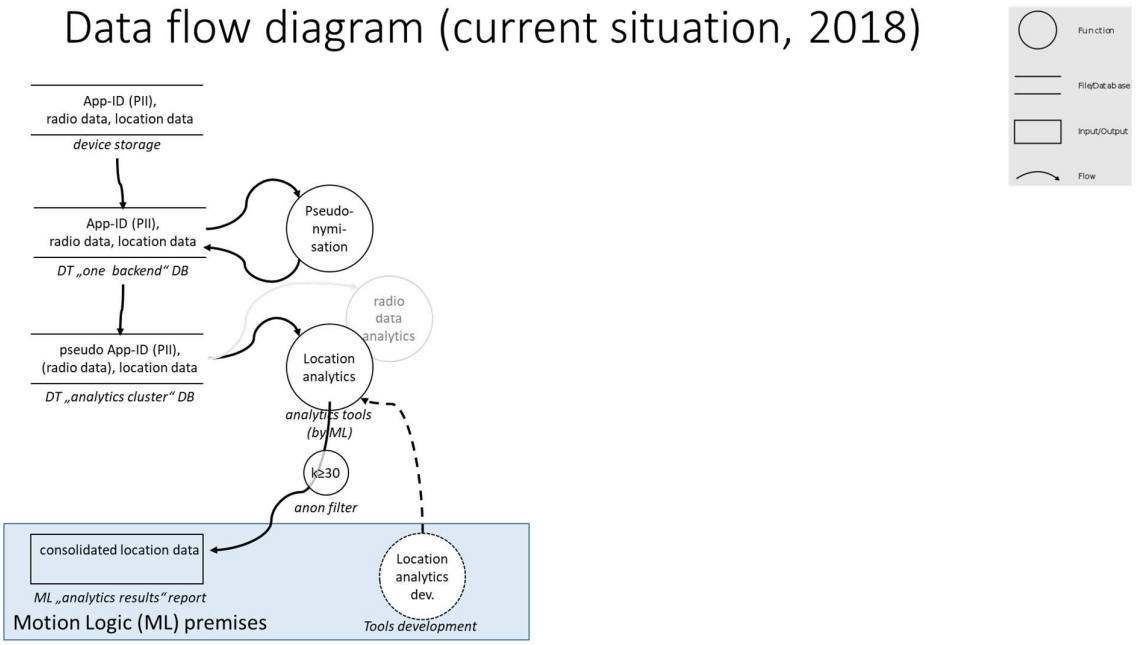


Figure 5.7 : Data flow as practised by DT and Motionlogic before SPECIAL. Only bulk anonymized location data are transferred to Motionlogic.

The figure also visualizes parts of development processes of the overall system: location analytics tools are developed outside DT's data center without access to real-world data.

Then the algorithms are installed inside the DT data center (dotted arrow) where they run and perform the actual analytics tasks.

This illustrations shows that testing, debugging and other quality assurance (QA) measures are very hard to do in the present setting. SPECIAL provides the tools and architecture to enhance QA dramatically: with a relatively small number of non-anonymized location datasets, Motionlogic could test their algorithms and enhance them for the actual task in DT's data center.

Figure 5.8 shows the newly designed setting:

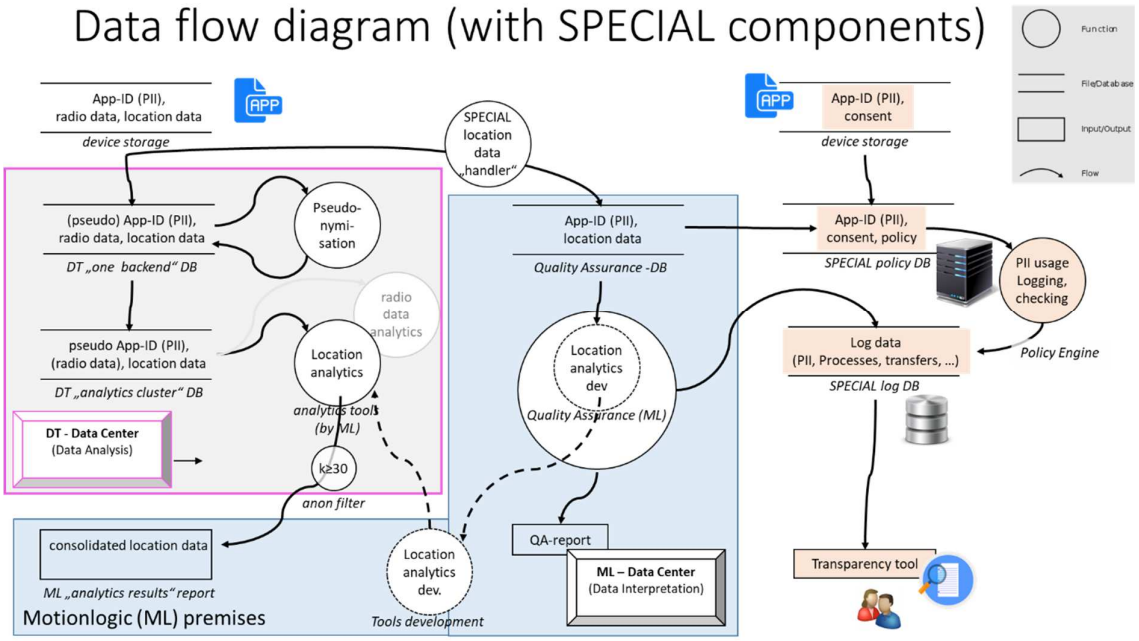
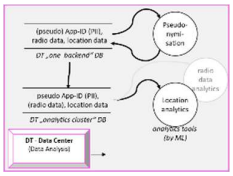
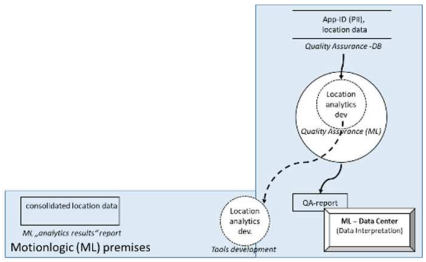


Figure 5.8 : Data flow as designed with SPECIAL components. Certain PII is transferred to Motionlogic with user consent.

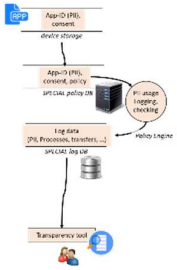
For clarification, colours have been added to the drawing:



The magenta outlined grey box contains DT's data center where analytics tools take place. These include location analytics tasks using Motionlogic's algorithms.



The blue box depicts Motionlogic's data center and development facilities. Utilizing certain non-anonymized location data (received from the "SPECIAL location data handler"), software development and QA can now legally improve the location analytics tools that work inside DT's premise.



SPECIAL components (with light orange background) take care of all the privacy and GDPR constraints and also the user interaction. This is crucial since neither DT's data center nore Motionlogic have any direct contact to end customers (the data subjects in SPECIAL terms).

The data flow designed for the new version of the overall system (CNE app, DT data center, ML data center, and privacy/tranparency/control tools) ensures minimal changes to the legacy systems and provides optimal access and exploitation of the desired location data while at the same time revealing the feasibility and value of the SPECIAL approach.

The following chapters will detail the implementation and explain certain design decisions as well as the planned test criteria and procedures.

5.6 Use of SPECIAL components

5.6.1 Policy Language

Since the use case of DT's pilot is rather "straight forward" with a limited number (and sequence) of possible consents, the SPECIAL policy language is not fully exploited. Rather, we experimented with formulating the current consent statements in the form of "policies" and succeeded easily.

In addition, DT is considering to use/define more complex policies for other use cases. To be able to judge the applicability of SPECIAL's policy language, complex and partially "synthetic" requirements have been contributed to WP2. As a result, the policy language was found to be a full match of even the most advanced future requirements.

In the current pilot, DT only scratches the surface of the policy language's potential. Even with the (present) limited use, DT is able to cover a very large portion of "real-world" requirements.

5.6.2 Sticky Policies

"Sticky policies" are charming feature and an attractive technical concept. On this (conceptual) level, the pilot uses sticky policies in the "SPECIAL SERVER". However, there is no end-to-end implementation of the concept available at this time. DT's use of the concept is meant to be a step towards the eventual implementation.

5.6.3 Privacy Dashboard

Since transparency and control for the end user are of utmost importance for DT in this pilot (and beyond), special attention was given to the implementation of the privacy dashboard. This tool grants not only the legally required data transparency, but also is a convincing proof of DT's reputation of being not only responsible and protective with user's data but also innovation friendly and "leading edge" in terms of technology. DT puts the user/customer in the front and takes care of the users security and wellbeing while using DT's products.

The privacy dashboard is used to underline this reputation and as an argument to gain user consent. In fact, the dashboard was the main argument to get DT involved in the project.

5.6.4 Compliance Checker

DT evaluated the various versions of the ex-post compliance checker (see D3.4 for details on this tool). Since the used policies in the current DT pilot are very simple and the type of processing/transmitting data is at the same time simple and conceptually happening outside the SPECIAL server scope, no explicit ex-ante compliance check was implemented. However, the method of collecting and storing relevant information (in the event log) is a perfect precondition for formal compliance checks.

5.6.5 Event log

The current version of the pilot uses SPECIAL event logs to conceptually check compliance (ex-post) and to feed the privacy dashboard.

5.6.6 Dynamic consent

Dynamic consent as a concept would fit nicely to the use case, in particular if you consider ongoing and extended use of PII by DT or at least under DT's management. DT considers dynamic consent an extremely valuable concept and a key reason for DT to continue evaluation and work on SPECIAL results even after the official termination of the project (in 2020 ff)

5.7 Testing plans

In addition to the usual software tests (for meeting software quality requirements) and security and privacy tests, T-Labs intends to run qualitative tests based on user questionnaires and expert interviews:

All those tests will be executed by experienced test experts, collaborating with experts from all relevant DT-business units (CNE-app, Motionlogic, T-Labs) and SPECIAL experts.

The tests will be carried out during a dedicated test period. The new (SPECIAL supplemented) version of the CNE app will be made available for download and install for designated test users.

During the first use of the new CNE app version, the user will be asked to renew the acknowledgement of the (updated) privacy statement (by changing a switch in the interface). This can be considered a "minimalistic version" of the dynamic consent mechanism described in D1.6. Due to the earlier decision to start with a minimal feature set, it is assumed to be fine starting with the smallest non-zero dynamics at this stage (i.e. no consent or minimal consent (anonymous use))

In addition, the user will be asked if he is willing to participate in the non-anonymized procedure for further quality enhancement. The user then gives his informed consent via checkbox/slider and is provided a link to the privacy dashboard (transparency tool). The whole setting will clearly be marked as test procedure.

The test run is planned for at least one month with an option to extend the period. Of course, the test can be aborted anytime by stopping the data collection on the device or the server side. Users will be informed immediately via the transparency tool.

During the test period and after the first month, the mentioned expert interviews and survey will take place.

5.8 Expected results & evaluation criteria

5.8.1 Expected Results

Given the ***qualitative objectives*** of the pilot and the tests, DT expects pretty simple, almost binary (Yes/No), answers to a few strategic questions. All of these are based on the situation of a large European telecommunications provider with an excellent reputation in many aspects including privacy trustworthiness.

Thus the expected results can be summarized as answers to the following list of questions:

1. Does it work? (Does SPECIAL enable DT and business partners collecting, storing and processing personal data?)

2. Does it pay off? (Is the effort in a reasonable ratio to the revenue?)
3. Are real world users satisfied? (user satisfaction regarding usability and functionality of SPECIAL tools)
4. Is it legal? (This is not the least question, but rather the most critical one since it is directly relate to DT's reputation. We assume that the tools are "legally acceptable", but we expect more: the tools are meant to be accepted by end-users as legal and justifiable, not only (but also) by lawyers.

These four questions need to be asked and evaluated using the criteria described in the next chapter where we explain the evaluation criteria that ultimately lead to the four answers to the four questions. The last question ("is it legal? ") can obviously answered best by legal experts, e.g. those participating in the consortium.

While these questions might be answered on the basis of the pilot implementation with a limited number of users, the real value of the approach will be extrapolated to the assumed application to DT's "real" Big Data assets.

5.8.2 Evaluation Criteria

The evaluation criteria has not changed since the first version of this deliverable. It will be done on a qualitative level (no exact quantitative measurements planned). Since the overall goals (objectives, see chapter 5.3) are feasibility and effects on existing IT infrastructure and user acceptance, it is considered to be of secondary relevance to collect any numerical data.

Our evaluation criteria can be divided according to objectives in four groups:

5.8.2.1 Hygiene factors (criteria that need to be fulfilled in all products/prototypes anyway)

Security: Does the pilot implementation fulfil basic security requirements, e.g. is the app secured appropriately and protected against external threats. Are all databases protected against a moderately serious attacker? Is network communication encrypted and is the encryption sufficient?

Data Privacy: Does the pilot and all its' components comply with all applicable privacy [2]laws, in particular with the GDPR?

5.8.2.2 Value of Insights gained

Usefulness of gained information: Two types of information will be gained with the pilot: privacy/consent related data, and "payload" – data that is useful for Motionlogic's quality assurance. Both categories of information will be evaluated separately (simple yes/no decision, met by a subject matter expert)

Plausibility of gained information: Since the core findings (from payload data) will be based on machine learning style algorithms, they might contradict proven knowledge in this field. Even if we hope for "surprising" results with big innovation value, we will double-check the most suspicious results and thus rate the overall plausibility of the information.

Corporate fit: Organizational effort for implementation (minus re-usability effect for production version) is expected to be significant (as is usual in large organisations). Barriers for a pilot may be lower than for a fully-fledged operative system, however if the effort to get the pilot confirmed is protectively high, critical assumptions can be made regarding organizational acceptance of the final product. On the other hand, we assume that the pilot (if successful) will open doors for similar systems products in the times to come.

Basic technical criteria: Computational, storage and network load, scalability. Based on experiences with the pilot, DT needs to rate the technology (not the pilot) regarding potential impact on internal IT

[2] The goal of SPECIAL is not to demonstrate compliance to *all* privacy laws, but an assessment is necessary nevertheless.

infrastructure. This can be done with standard IT performance measurement tools but will also be based on expert opinion. The rating will be qualitative only.

Scalability for Big Data applications: The relatively simple use case, applied to a relatively large number of users and datasets is expect to allow profound statements regarding scalability. DT's mid term business interests lay in legally monetizing its Big Data assets.

5.8.2.3 User acceptance criteria

(Relative) **number of "Opt-Ins"** made with the SPECIAL / pilot. Giving consent to a collect and process personal data such as location is a specific act that a user needs to perform to allow DT/Motionlogic to process his data. We assume that not all users will give this (binary) consent. This is the minimal version of the "progressive" consent granting described in D1.6. More stages/degrees of consent (using more personal data and/or more purposes) are foreseen for later stages (not within SPECIALs current time scope). Thus, the portion (relative share) of users that give consent in a very limited experimental environment will be a most valuable insight for other situations where user consent might be asked.

User response/acceptance: In addition to the (relative) number of users who opted in, we want to collect reasons for opting in (giving consent), or rejecting the requested consent. These statements will be valuable evaluation results and be considered in future products (even outside the domain of the pilot). Thus, these user opinions will (probably) form some of the most valuable qualitative insight for future privacy related products/components in DT's user facing service offering

6 Conclusion

This deliverable is now labelled “V2”, therefore while still no final conclusions can be expected here, the pilot description and test plans should be more concrete now. As mentioned above, D5.5 will reflect on the complete implementation and testing.

However, based on the experience gained prior to and while writing this document, several observations have been made that could be seen as “preliminary conclusions”:

1. Despite the different use cases and different stages of implementation, all three pilots came up with comparable implementation objectives and testing plans:
   a. Check feasibility/effort,
   b. Check functionality,
   c. Check security and privacy.
2. The general concept of SPECIAL (using linked data, privacy policies and the established prior work of previous EU projects) succeeded in convincing the industry partners.
3. All industry partners use the implemented use cases/pilots to test “corporate compatibility” with internal processes and IT infrastructure.
4. Usability is crucial, mainly for end customers but also for admins and backend operators.
5. Big Data and AI applications require techniques beyond SPECIAL’s scope. The pilots and testing plans are designed to deliver proven experience on feasibility of respective (Big Data/AI) analyses under the governance of modern privacy regulations.

First experiences (before the actual tests run) indicate that SPECIAL’s concept and tools are very well applicable, especially since they are designed in a way to be implemented in various ways including different corporate IT infrastructure environments.