SPECIAL

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

Deliverable No. D1.6

Legal requirements for a privacy-enhancing Big Data V2

SPECIAL DELIVERABLE

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

Ms Jessica Michel t: +33 4 92 38 50 89 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:	M01-M18
Deliverable number:	D1.6
Deliverable title	Legal requirements for a privacy-enhancing Big Data V2
Contractual Date of Delivery:	31/03/2018
Actual Date of Delivery:	28/04/2018
Editor (s):	Eva Schlehahn (ULD), Rigo Wenning (ERCIM)
Author (s):	Eva Schlehahn (ULD), Rigo Wenning (ERCIM), for section 2.3.1: Dennis Gräf, Martin Kurze (DTAG)
Reviewer (s):	Sabrina Kirrane (WU), Piero Bonatti (CeRICT), Uroš Milosevic (TF)
Participant(s):	ERCIM, WU, CeRICT, TUB, TF, DTAG, TR, PROX
Work package no.:	1 (T1.2 Legal and ethical requirements for use cases)
Work package title:	Use cases & Requirements
Work package leader:	CeRICT
Distribution:	Public
Version/Revision:	1.0
Draft/Final:	Final
Total number of pages (including cover):	99

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 Introduction

This deliverable is the continuation of our work in the deliverable D1.2[1]. D1.2 gave a general introduction into the European data protection framework. The legal environment was analysed, described and put into a bigger context. From this general description, conclusions were drawn for the use cases.

In this deliverable, we have chosen not to make an iteration of D1.2. Rather, D1.2 introduces the general legal preconditions for lawful personal data processing in Europe. Therefore, reading and understanding D1.2 is a prerequisite to understand this deliverable. This will give D1.6 more room to dive deeper into the complex and difficult issue of machine – mediated consent and control. Furthermore, it delves deeper into use-case-specific issues and solution approaches. In the meantime, the project has a better idea about the technology requirements done in D1.4. The use cases were further refined in D1.5., although some details and some options are still missing.

This document will first deal with the generic location based service scenario, thus working from the more general to the more detailed questions. This allows a derivation of overarching, generic realization requirements and solution approaches. These can then be applied to the more detailed use case scenarios of the implementation under way within the industry partners Proximus and DTAG.

D8.1[2] has shown that SPECIAL is confronted with non-obvious ethical challenges with regard to user control. Already in 1983, the German Federal Constitutional Court acknowledged the principle of informational self-determination (translated: '*Informationelle Selbstbestimmung*') as a constitutional right by itself in its famous Census decision[3]. Since then, the landscape of data processing has dramatically changed. Spiros Simitis had some doubts that the legal architecture of data protection would not hold given the advent of distributed and networked computing[4]. Communication streams and workflows were either ephemeral or hard to mine and search, as they were in paper registers or IT silos. The Directive 95/46EC[5] still had some central authority in mind that would store data in a database and then join several profiles to get new insights. We still do this, but the digitisation led to a world where formerly ephemeral information can be easily stored and mined. Via the progress in interoperability of data, more and more data can be joined to create big streams and big data lakes. As said in D8.1, the risk that the individual natural person doesn't know anymore who knows what about them is sharply increasing. This means they do not know whether their behaviour is monitored

[1] Deliverable D1.2 *Legal requirements for a privacy-enhancing Big Data V1*.

[2] D8.1 *H - (Ethics) Requirement No. 2*.

[3] Judgement of the German Federal Constitutional Court (in German: Volkszählungsurteil Bundesverfassungsgericht) of 15th December 1983 (Az.: 1 BvR 209, 269, 362, 420, 440, 484/83).

[4] Simitis, Spiros, 'Reicht unser Datenschutzrecht angesichts der technischen Revolution? - Strategien zur Wahrung der Freiheitsrechte' in: Staatskanzlei von Hessen (Hrsg.): Informationsgesellschaft oder Überwachungsstaat. Protokoll des Symposiums der Hessischen Landesregierung. Wiesbaden 1984, S. 27 ff.

[5] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, October 23/11/1995, 31–50, Official Journal L No. 281, 23.11.1995.

or not. Worse, after the Snowden revelations[6], people probably assume that they are monitored. This creates a strong pressure to avoid actions that would mark the person as an outlier (the so called '*chilling effect*'). This kind of self-censoring has demonstrably increased since Snowden.[7] And the German Federal Constitutional court concluded that this self censoring is a danger for democracy[8].

But with Big Data, our cognitive bandwidth is not big enough anymore to even assess legitimate data processing in the context of valid and informed consent as a data subject. The agreement on all data collection would mean a constant hammering of OK-buttons on the data subject. And with all the OK's given, who would remember what they gave their OK to?

On the other hand, there are hopes that Big Data could bring new innovation and progress in a variety of scientific domains.

Drawing 1: The promises of Big Data

For meteorological and other environmental data, this is under way[9]. But humans are social beings. This means data with a social connotation has a very high value and is needed to advance in the area of medical research, legal enforcement, but also in the way we organise useful services just-in-time. All this needs information with a link to one or more persons. There are already voices calling for new rules which are more permissive and allow the Big Data promises to materialise[10]. However, these significant expectations from Big Data have a tendency of drowning out concerns which are mostly related to fear over risks for opinion building and democracy. Still, the new populism and the media manipulations in elections with tailored messages addressed to well identified classes of people, as recently experienced in the US elections, give the doubts of the German Federal Constitutional Court a renewed sense[11].

If nothing happens, this could create a dichotomy between Big Data and the promise to save thousands of lives on the one side, and democracy, human dignity, freedom of thought and freedom of expression on the other side. So something has to happen to overcome this conflict. Or we could end where Scott McNealy, former CEO of SUN Microsystems saw us: 'You have zero privacy, get over it'[12]. So given we have Big Data and given we have informational self-determination, how would such self-determination in a Big Data scenario work? One way is to promote the end of this concept and

[6] See the STRINT Workshop for more information https://www.w3.org/2014/strint on how to identify and counter pervasive monitoring.

[7] This has been verified in a number of studies since then. See for example Penney, J.: '*Chilling Effects: Online Surveillance and Wikipedia Use*', Berkeley Technology Law Journal, Vol. 31, No. 1, p. 117, 2016.

[8] See footnote 3.

[9] See the Big Data Europe climate demonstrator: https://www.big-data-europe.eu/pilot-climate/.

[10] Representative of these expectations, see for example the BITKOM press release 2015-06-24 https://www.bitkom.org/Presse/Presseinformation/EU-Datenschutzverordnung-muss-Innovationen-ermoeglichen.html accessed 2018-02.

[11] See reports from the Guardian: e.g. Emma Graham-Harrison, Carole Cadwalladr, Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach, http://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election published 2018-03-17, accessed 2018-03-20 Similar use of personal data in elections were reported for the Brexit campaign.

try to replace it by some other control mechanism[13]. The disadvantage lies in the replacement of the self determination of the data subject. While this may work for consumer protection, it will not serve the opinion building that is so important for democracy, according to the fathers of data protection[14], the German Federal Constitutional Court[15] and the European Court of Human Rights[16]. Because the self determination will turn into a possibility for manipulation either by the entity collecting and processing the data, or by the authority determining whether this is legitimate or not. This means self determination is such a corner stone of the legal concept of data protection that a shift to a different control mechanism will create a lot of friction.

Consequently, the SPECIAL project tries to preserve the concept of data self-determination by allowing the concept to still work in a fully digitised Big Data environment. But the space for solutions is limited by the legal framework of data protection. Consent must be valid. Not any (implicit) interaction can be seen as an agreement to collection and processing of one's data. Having the computer help humans with informational self-determination does not only come with technical challenges[17]. The technical solutions have to create meaningful legal value. It is not sufficient to exchange technical tokens. The legal system has to grant some value to them in the relation between data subject and data controller. A token or message must be able to carry a consent message and these consent messages need to be recognised by the legal system. This deliverable explores how to create such legally meaningful technical messages. The requirements in this deliverable are not only addressing the content of those messages, but gravitate around an entire user experience, depending on the use case. The final goal is to create a computer-assisted informational self-determination for data subjects.[18]

The computer assisted informational self-determination has advantages for the user, but also for the data controller. The user isn't bombarded with prompts for consent as the preferences set would allow the machine to answer some, but not all of those consent requests. Which in turn, allows the controller to get more consent and thus avoid the symptom of so-called 'consent-fatigue'. In fact, many actors in the IT field try to avoid processing operations based on consent because they assume that the opt-in rate is 20% at maximum. On the other hand, if people are enrolled automatically, only 20% ever bother to opt-out again.[19] The possibility to gain 60% more clients is a significant reason to argue about consent. This means on the one hand, there are opinions in the scientific community and in the privacy advocacy community that consent and self-determination is outdated and as

[12] https://en.wikipedia.org/wiki/Scott_McNealy accessed 2018-03-01.

[13] Hildebrandt, M.: '*Technology and the end of law*' Facing the limits of the law, Heidelberg (2009). The same in Law, Human Agency and Autonomic Computing: '*The Philosophy of Law Meets the Philosophy of Technology*', Routledge (2013). There is probably a deeper dispute between the philosophical approach of Hildebrandt et al. and the one pursued here.

[14] Bernd Lutterbeck. 20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes. 1998. http://ig.cs.tu-berlin.de/bl/025/ , accessed 2004-06-14.

[15] See Footnote 3.

[16] BRINKS v. THE NETHERLANDS, http://hudoc.echr.coe.int/eng?i=001-68816 published 2005-04-05, accessed 2018-03-11

[17] See SPECIAL Deliverables D1.3 *Policy, transparency and compliance guidelines V1* and D1.4 *Technical Requirements V1*.

[18] There is the concept of agents from the 90ies of the last century, which departs from the same bases, but takes a different approach.

[19] For all see the opt-in vs opt-out comparisons in organ donation: The Rogue Medic, The Silver Lining of Epi - Organ Donation, http://roguemedic.com/2014/04/the-silver-lining-of-epi-organ-donation-part-1/ published 2014-04-22 accessed 2018-03-23 and also Different Types of Consent, http://www.privacysense.net/different-types-consent/, published 2015-07-09, accessed 2018-03-23.

concepts not fit for purpose anymore.[20] On the other hand, they get applauded by businesses losing too many customers over consent requirements. As seen above, this creates a problematic situation for democracy and the initial goals of data protection in the seventies. SPECIAL as a project intends to make the acquisition of valid, free and informed consent easier, thereby supporting informational self-determination as a concept. Nothing less is at stake.

A lower barrier for consent must be compensated by additional measures. The SPECIAL approach is to compensate by an easy first contact with a data subject that is supported by semi-automatic consent requests with a layered control interface. Such an interface would allow data subjects to come back to the decisions made based on their preferences and revert them. In order to avoid a system where a data subject would be required to understand a large quantity of information before being able to give informed consent, the interface has a layered approach with innovative user experience features. Those may be developed in work package 4. They should be taken into account in the legal considerations here already.

[20] Most prominently Mireille Hildebrandt, e.g. "Slaves to Big Data. Or Are We?" 17 IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA 2013, 7-44 https://works.bepress.com/mireille_hildebrandt/52/ But also firmly defended by Caspar Bowden during the works for the Dagstuhl Manifesto: Online Privacy: Towards Informational Self-Determination on the Internet (Dagstuhl Perspectives Workshop 11061) http://www.dagstuhl.de/11061 published 2011.

2 Use cases starting with location-based services

2.1 Generic location-based service

'*We are drowning in information but starved for knowledge*'[21]. This prediction from 1982 is even more true today. John Naisbitt did not predict the Web, and its abundance of services and information. Which means it is ever more important to have appropriate filters for this abundance to be able to handle this shiny new world. Context is one of the most promising concepts to filter information so that only the most relevant things are shown. And one of the possible filters for context is location.

The collection and processing of location information is thus subject to special safeguards laid down in Directive 2002/58EC. This is re-iterated in the Draft ePrivacy Regulation. Location information is rather sensitive[22], because the collection and analysis of accurate location information allows for the inference of highly sensitive information about an individual. Users of LBSs may be confronted with these inferences either immediately or in the future, where the '*future*' could be minutes, days, weeks and even up to years and decades ahead since location data, once available, may persist in Big Data Space.[23] A further hint can be found in the '*contextual integrity*'(CI), a concept coined by Helen Nissenbaum.[24] Communications happen between people in a specific context. Hildebrandt et al summarise the concept by stating that CI is violated if user privacy is breached when information is shared with disregard for the transmission principle implied in the context where the information was first shared.[25] Data subjects should be enabled to be on top of the management of the self as well as the relationship management.

But location-based services are also very promising as a contextual filter. In an example for restaurant recommendations, all restaurants in Brussels do not have to be shown, but rather only those in close proximity to the data subject. It allows for relevant information to be presented, as people move around. There are an infinite number of possibilities where actual location information can help bring more relevant information to people. But location information also makes the data subject vulnerable. Because an operator and data controller can deduct a lot of very intimate information from the trail of location information that a data subject leaves behind. Under circumstances, this may even mean physical damage or life threats to the data subject, because someone is tracking their location, or has access to the trails used by a benign service or application.[26] But not only the actual location information is dangerous, the accumulation of location

[21] John Naisbitt & Patricia Aburdene, '*Megatrends: Ten New Directions Transforming Our Lives*', Warner Books (1982).

[22] Recital 75 GDPR; Recital 32 and Art. 9 of Directive 2002/58EC.

[23] Herrmann, Michael, Hildebrandt, Mireille, Tielemans, Laura, Diaz, Claudia: Privacy in Location-Based Services: An Interdisciplinary Approach, SCRIPTed Volume 13, Issue 2, 2016 https://securewww.esat.kuleuven.be/cosic/publications/article-2725.pdf .

[24] Nissenbaum, H. F.: Privacy as Contextual Integrity, Washington Law Review 79(1), 2004 and Privacy in Context: Technology, Policy, and the Integrity of Social Life, Palo Alto, Stanford University Press, 2009.

[25] See footnote 23.

[26] As an example from the rather unregulated area in the US, the case of Jackie Wisniewski can be mentioned, which was reported in an article on the PrivacySOS blog run by the American Civil Liberties union (ACLU): https://privacysos.org/blog/nowhere-to-hide-location-tracking-by-domestic-violence-abusers-and-government-spooks/, published 2013-06-04, accessed 2018-03-11. In this case, a stalker put a GPS device on

information can reveal many things. In a recent incident widely reported in media and social networks, a fitness application that uses GPS trails released a map with all GPS points ever submitted to it.[27] This information was then correlated with map data. But analysts quickly found a problem:

> *'Nathan Ruser, an analyst with the Institute for United Conflict Analysts, first noted the lapse. The heatmap "looks very pretty" he wrote, but is "not amazing for Op-Sec" – short for operational security. "US Bases are clearly identifiable and mappable.'*[28]

The multitude of problems around the use of location data has also led to the failure of services that use location data. The best example may be Google latitude. This is a service where people could reveal their location to 'friends'. If the system was started, one was able to see all the 'friends' who were in the same town. The application did not take off and had very creepy email alerts.[29]

The SPECIAL concept aims to prevent such incidents and to enhance the acceptance of location-based services, which are often perceived as 'creepy' by many. It takes into account the sensitive character of location information and gives the user full control over the services while trying not to overwhelm the data subject. In this deliverable, we identify the legal framework that sets the environment for such a system. This is a challenging task.

Taking out the perceived 'creepiness' is not sufficient. The EU has given itself an ambitious regulatory environment for personal data protection and digital services. This regulatory environment generates a number of requirements for location-based services. The challenge is that SPECIAL uses new ways to fulfil those requirements. In this deliverable, we try to match the new tools we develop to the existing requirements. Thereby, we give certain high level recommendations for the technical implementation within the location-based project use cases.

The generic location-based service is described in more detail in deliverable D1.1.[30] The scenario focuses on a data subject with a mobile device. First, there is an enrolment into the service by an initial interaction. Location information is collected while using the service. Depending in the exact service provided by the data controller, the location information can be matched against other information inorder to offer a personalized service value to the user. The other information matched can be anything collected within or outside the given context, personal and non-personal data. Choices of the user are played back into the profile to improve the correlation and matching quality of the system. By playing back, the non-personal data becomes personal data in this context. With the enrolment, the data subject also acquires access to a dashboard. The dashboard is layered in broad categories and allows data subjects to drill down to the data records stored about them.

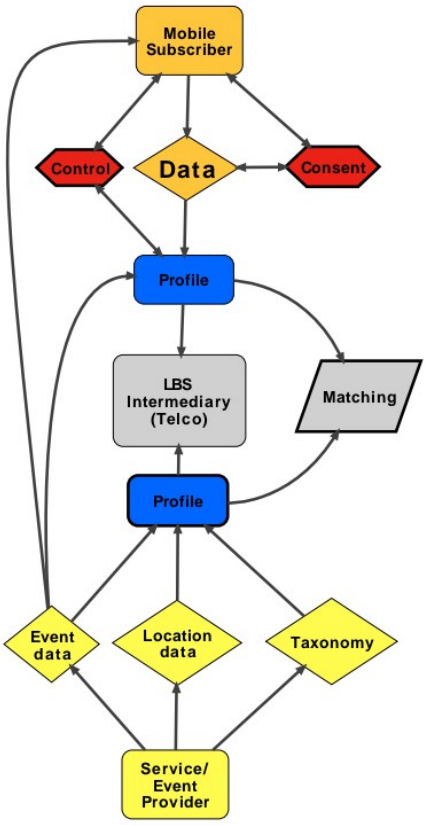
the victims' car and later killed her.

[27] Hern, A.: '*Fitness tracking app Strava gives away location of secret US army bases*', The Guardian, http://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases published 2018-01-28, accessed 2018-01-29.

[28] See FN 27.

[29] Siegler, M. G.: '*Google Quietly Kills Their Creepy Latitude Location Alerts Feature*', TechCrunch, http://social.techcrunch.com/2010/12/18/google-latitude-location-alerts-dead/ published on 2010-12-18 , accessed 2018-03-11.

[30] D1.1 *Use case scenarios V1*, pages 34 ff.



Drawing 2: A schema for location-based services

2.1.1 Installation and Subscription

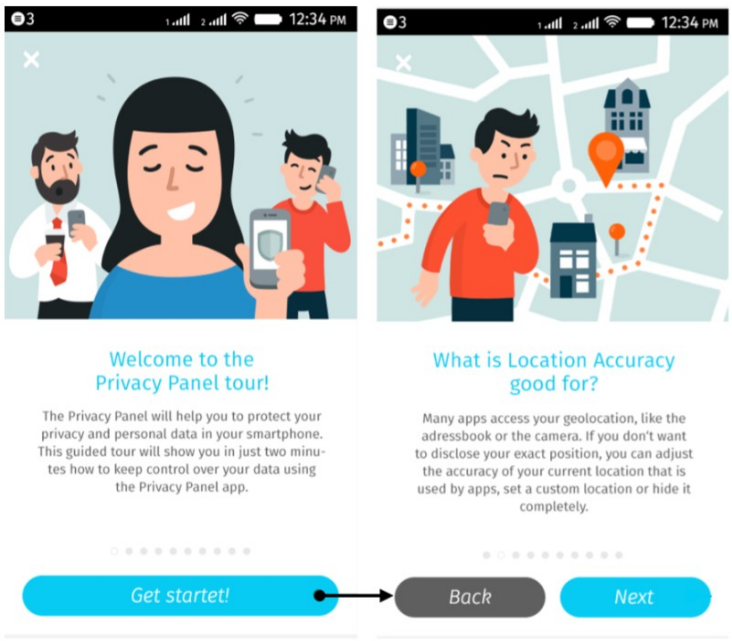
We assume that at some point, a data subject installs a mobile application on their smartphone. This is equivalent to the first ever GET request to a website. At this point in time, there is no data collection other than the usual internet HTTP logging yet, which is subject to the general privacy policy or simply necessary data collection according to Art. 6 para. 1 (b) GDPR.

The idea in SPECIAL is now to only ask basic questions up front. It is one of the failures of the privacy notification systems that they overburden the data subject with pages of legalese.[31] It is important to begin simple, yet give the data subject a perspective to extend the consent. Additional consent requests may then be triggered within a situational context before another data category starts being collected. The repeated additional requests in context would extend upon and update the original consent to build up an overall consent for the data collection and processing that is actually taking place within the entire system. And this overall consent would be controlled within the SPECIAL layered control interface. To make this more tangible, some kind of step-by-step fictional use case storytelling is used. Thereby, the technology enablers and the relevant legal considerations will be explained alongside this use case story.

[31] For all, McDonald, Aleecia M, Cranor, Lorrie Faith: The cost of reading privacy policies, ISJLP 4, https://kb.osu.edu/dspace/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf published 2008-09-26 accessed 2008-10-15.

The story starts when data subjects are not just looking at static web information, but request additional services. In our case here, those are services that give information and possibilities dependent on the location of data subjects collected from their respective devices.

The data subject, let's say Alice, is told by a friend about this very nice new tool that provides information and opportunities based on the location collected from their smartphone. Alice opens the app-store application of her mobile operating system, finds the tool and installs it. The installation is similar to a first hit on a website offering similar functionality. The application is used in this document because it is easier and more tangible to describe the steps in this environment.

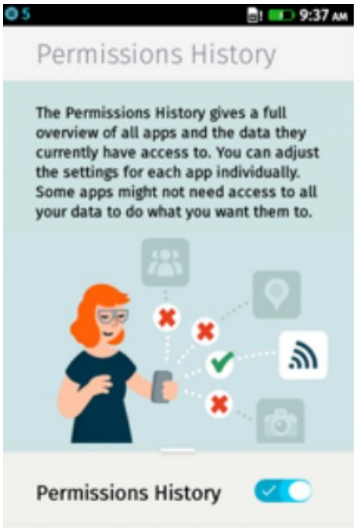


Drawing 3: A Privacy Wizard

On first run, the tool opens by asking certain preferences upfront. This has already been done by the SPECIAL – Partner Deutsche Telekom in their Firefox – OS initiative. The exemplary image on the left shows how the welcome screen of the FirefoxOS phone was done in a cooperation with Mozilla and Deutsche Telekom. Such a screen may also be necessary for the data subject to get a basic understanding of the application in context. At the very beginning, this needs a basic description of the service offered. In the generic location based services use case, a message could say that the application or the website could collect or re-use already existing location data to provide the user with information in that location context. This enrolment is very important as it allows the system to create the identity management needed later for the control interface. Such an enrolment could theoretically be fully pseudonymous, but some identity is needed to avoid giving the information to the wrong person. However, in scenarios where the service provider is the same as the provider of the telecommunication service for the smartphone, this service provider will know the subscription SIM and the precise identity of the data subject. Therefore, in such cases where the controller would be able to re-trace the identity of its customer, the data should be considered as pseudonymous at best, even if there is no enrolment or profile at all. If the user does not want a profile, the recommendations and services could only be rather basic. Still, such an option is imaginable in the initial setup dialogue. One can also imagine a 'not now Button'. If it is pressed, the device issues a do not track DNT:1 token to the service and the service does no or only minimal data collection. A similar setup can be envisioned if the service is entirely web-based.

In order to allow for later context-based extensions for consent, the data subject has to agree to the modalities that are used to gather that consent. As explained previously, asking for consent for every extension or renewal will lead to '*click – fatigue*'.[32] It is therefore important to allow for new and innovative interfaces. In order to do that, the initial setup should gather an agreement for this new innovative consent-collection-system. First of all, data subjects have to agree that the machine will send consent – confirmation – tokens on their behalf to the system. Furthermore, the user must be informed that the system will automatically do so if the offered contextual new consent request matches their preferences that could alternatively already be recorded, during the setup period, or even later. It is important that a non-invasive interface can be created starting from that broad

[32] See footnote 31.



Drawing 4: Simple permission management

consent. One of the concepts in the PrimeLife project was to have a shade coming down from the top of the screen asking for 'Yes', 'No' or 'More information'[33]. But this shade went away after 5 -10 seconds and the system assumed that the data subject either agreed or did not mind. We could think of something similar here. As this is going beyond what consent normally looks like, the data subject needs to agree to this modality up front at the beginning.

The upfront agreement is legally necessary. Recital 32 of the GDPR states that consent should be given by '*clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her'*. According to this Recital 32, this includes: '*choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data'*.

Sending a technical signal like DNT after configuration of preferences can thus be seen as a valid way to express consent. This is reinforced by the draft of the ePrivacy Regulation that was agreed upon in the European Parliament and is now in the Trilogue.[34] The current version, as voted by the LIBE Committee and introduced into the Trilogue by the plenary vote on the 20th of October 2017 contains a number of provisions and considerations which support this approach in SPECIAL.

Article 8 draft ePrivacy Regulation states:

> *'Protection of information transmitted to, stored in, related to, processed by and collected from end-users' terminal equipment*
>
> > *1. The use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware, other than by the end-user concerned shall be prohibited, except on the following grounds:*
> >
> > > *(a) it is strictly necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or*
> > >
> > > *(b) the user has given his or her specific consent; or*
> > >
> > > *(c) it is strictly technically necessary for providing an information society service specifically requested by the user; or […]'*

The GPS or Galileo signal hits the terminal equipment or device of the data subject and allows the device to determine and record its own position. Another way is to triangulate between GSM/LTE Towers around the device and thus translate this into position coordinates. However this is done, the information about the position is now recorded within the terminal equipment. In order for the service to use the position data, it must be collected from the data subject's terminal equipment or

[33] The Primelife Dashboard is a Firefox extension that collects data about those collecting data from the firefox user. It is able to block things http://primelife.ercim.eu/results/opensource/76-dashboard published 2011, participated in 2011.

[34] See the procedure file of the European Parliament, 2017/0003(COD), available at: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2017/0003(COD)&l=en accessed 2018-03-11 with a link to the text: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A8-2017-0324&language=EN accessed 2018-03-11.

device. According to Article 8, the collection of information from the data subject's terminal equipment is explicitly and generally prohibited. However, this general prohibition comes along with a permission reservation under certain preconditions.

For the normal web access without trackers or even an unfiltered access to the events database, Article 8 para. 1 (a) or (c) draft ePrivacy Regulation could be used. Location data itself is more sensitive. Recital 21 of the draft explicitly mentions that sometimes, very sensitive data can be derived from location data. Thus, location data and data on the terminal equipment in general needs enhanced protection. The goal of the generic use case is not only to provide information based on location, but to also build up a profile helping the user with the filtering of the abundance of information available. Such a stepwise extension of the profile with data from other, various sources adding up to the location data needs consent. Art. 8 para. 1 (b) requires that the consent is specific. A further definition of what that means is given in Art. 9 and Art. 10 of the draft ePrivacy Regulation.

Article 9 draft ePrivacy Regulation states:

> *'1. The definition of and conditions for consent provided for in Regulation (EU) 2016/679/EU shall apply.*
>
> *2. Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed or withdrawn by using technical specifications for electronic communications services or information society services which allow for specific consent for specific purposes and with regard to specific service providers actively selected by the user in each case, pursuant to paragraph 1.*
> *When such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party.*
>
> *3. Users who have consented to the processing of electronic communications data as set out in point (c) of Article 6(2) and points (a) and (b) of Article 6(3), point (b) of Article 8(1) and point (aa) of Article 8(2) shall be given the possibility to withdraw their consent at any time as set forth under Article 7(3) of Regulation (EU) 2016/679 as long as the processing continues.'*

Article 9 basically provides a blue print for the SPECIAL approach. The data controller may follow a technical specification like the W3C tracking protection specification[35] that defines tokens with a specific meaning. It also defines the protocol to exchange those tokens between the terminal equipment and the backend. In principle, this means a technical signal based on preferences and the alteration of those preferences during the course of the application execution, or while using the respective functionalities of a modern website is a legally valid means to give and prove consent. This is decisive for the SPECIAL system. It is further encouraged in Art. 10 para. 1 (c) draft ePrivacy Regulation:

> *'Article 10 Privacy settings and signals to be provided*
>
> *1. Software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet, shall:*
>
> *[...]*
>
> *(c) offer the user the possibility to express specific consent through the settings after the installation of the software.*
>
> *Before the first use of the software, the software shall inform the user about the privacy settings and the available granular setting options according to the information society service accessed. These settings shall be easily accessible during the use of the software*

[35] https://www.w3.org/TR/tracking-dnt/ accessed 11 March 2018.

> *and presented in a manner that gives the user the possibility for making an informed decision.'*

At the time of writing this deliverable, the text of the ePrivacy Regulation is only a DRAFT. Nevertheless, the concept of expressing consent via technical means is not exclusive to this draft legal framework. Rather, it can be found in Art. 21 para. 5 GDPR as well, which states:

> *'In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.'*

This means the general concept of having technical signals expressing specific consent is already present in the GDPR. This concept is then further refined in the Trilogue version of the draft ePrivacy Regulation. For SPECIAL, it would be beneficial and promising if these provisions survive the political process, as they allow for innovative new ways to preserve the fundamental right of informational self-determination.

For the general location-based services, we can draw a number of conclusions:

1. Upon installation, the data subjects must be informed about the specific privacy configurations available to them in the application. For the website functionality, this should happen at first visit. A way to imagine such information is a wizard that helps on first run, or the option for first run expert configuration like it is done in most software today and as shown in Drawing 3: A Privacy Wizard. The concrete messages then depend on the specific service that is offered on the basis of location data since they need to communicate the purpose of the processing to the user.
2. From Art. 9 para. 2 draft ePrivacy Regulation, we can also deduct that if consent is acquired over such a technical mechanism, the same mechanism, where possible, must also offer a way to withdraw consent. The '*where possible'* is important, because current operations may still be under way and can not be stopped immediately without disruption. Sometimes, withdrawal of consent may be in conflict with the need to invoice past uses of the service in the context of a certain invoicing period. There are many other potential situations where deletion only works in an asynchronous way and after some lapse of time. The goal must be to serve the user without creating undue disruption in the system.
3. The consent can evolve and extend over time, depending on contextual add-on requests. This will lead to a stateful consent system that may concern one or more objects, functionalities, services and relations. This means the application or website will have to offer a way to control those preferences, even after they have been set during the installation process or at first hit.
4. We need an agreement from the data subject regarding the modus operandi for the further gathering of consent. This concerns the handling of the above mentioned extensions to the initial very basic consent needed to start the application. Concrete wordings need to be determined for each use case. This will be subject to the UX innovations from work package 4.
5. As soon as sensitive data in the sense of Art. 9 GDPR is concerned, the system should never give automatic consent. Rather, it must prompt the user for explicit confirmation. But one can imagine a context or location-based system, like a medical system, where there is a constant collection of sensitive data. In this case, the challenging trade-off between click fatigue and the very specific requirements in Art. 9 GDPR have to be considered carefully to find a tailored solution. In this case the automatic functioning must have additional

precautions and functions. The more sensitive the data, the more control functions are needed, during collection and later in the control interface.

The controller might obtain some information from the user's device that does not need the explicit consent of the data subject because other legal grounds allow for its collection and processing. This does not need to be communicated upfront to the data subject when requesting consent for the usage of the location data for the service provision. Rather, a layered approach can be applied to make this information accessible in the user control interface (dashboard). This way, the data subject can drill down into all the data collection, whether based on consent or legal ground. As it is layered, this approach avoids exposing the data subject to information overload.

Example data categories which might not need to be mentioned due to other applicable legal grounds and which can be exposed in a second or third layer could be:

- Log data
- Collection done for security reasons
- Session cookies

The installation wizard should also indicate the basic purpose of the application or the website functionality. This can be very general as the SPECIAL system has a control interface (dashboard) that allows refinements over time. The following points should be covered:

1. The overall purpose of the application (e.g. recommending cultural events)
2. A short summary of the machine-assisted consent mechanism, explaining that this makes it possible to give additional permissions in future depending on context. This explanation should express that this may entail purpose changes or the possibility to add more data sources in future to achieve better personalization of the service.
3. A basic explanation of the control interface, including the information that it is possible to drill down to the details of data collection and processing.
4. Offering the possibility to revoke permissions and to ask for the erasure of personal information
5. Showing the '*Off*' or '*Not now*' button that allows all collection and correlation activities to be temporarily suspend. This way, the data subject can go '*incognito*' and perhaps even control what is added to their profile.
6. A link to a full privacy policy somewhere on the web.

Once the data subject has installed the application and has gone through the wizard, the agreement must be sent to the ledger as a proof that the initial consent has been given. This must explicitly include the consent to machine-assisted consent management.

2.1.2 Enriching the profile

Once the application is installed and the controller has consent for the use of the machine-assisted consent management, the SPECIAL regime can start to function. In order to provide sophisticated filters, the data subject has to allow the data controller to add more information sources that are

used to build up of a profile. The better and more precise the profile of interest, the better the filtering. Location alone is already a pretty good filter, however it can be augmented by additional interests or preferences.

The goal in the general location based use case is to augment the experience of the data subject with relevant information that is useful for the user or data subject in that location context. To do so, it is necessary to match the data subject's interest and profile against the information available. Depending on the context and the location brought together, this may reveal preferences, even ones that are sensitive like political opinion. To justify that this still can work, we argue that the user has an 'off' button and a control interface, that can be used to demonstrate that they agreed to both.

New data sources thus serve the purpose of the application the data subject installed, or the web functionality the data subject subscribed to, or is using pseudonymously. If there is a new purpose, it means there is a new service, or that the data acquired within the context of a given service is used for a different purpose in another context. If this is the case, the semi-automatic consent acquisition has its limits and so the initial considerations mentioned above for the installation / first use in Section 2.1.1 will have to be taken into account. But one could imagine that a location-based service gives a push notification asking for additional processing purposes, e.g. for statistical insight, or new services.

Here we benefit from the fact that the initial installation or first-use wizard has given a very general purpose that frames the overall area of consent. The goal is now to avoid the '*consent-fatigue*' described in the section 1. Instead of describing the entire location-based service with all of its options, we only describe the option that the data subjects chooses to add, and we only describe it when they actually add the option. To add an option, the system does not have to describe the overall context again and again, overwhelming the user. Asked in context, the data subject may well understand the impact of giving consent. And the application is capable of managing the time-frame for consent. A data subject may allow access to their location for a taxi service and later erase the traces left. In this context, the data subject understands what they are doing. Adding sources of information and preferences in a well defined context of an action or event within the application, or a website function gives data subjects the chance to assess the impact of data collection. If a data subject is asked to give consent for location information to be recorded and put on a profile to determine public transport usage and walking ways to stops, while she goes, it is different from explaining an overall system where people may be monitored from time to time depending on need and availability of a sufficient number of signals on a certain route. In the first case, a data subject has a well defined chunk of information to agree upon. In the second case, data subjects may assume that the application could monitor their location and traces at every moment. It becomes clear that in the second case, consent is much harder to get, because the consent is potentially unbound. Already as children we learned that an agreement to unbound obligations or commitments is a dangerous thing to do. Consequently, data subjects will probably deny the collection use and processing of data with an all encompassing system-wide consent that is detailed in many pages of written text.[36] Thus, the contextual adding of enriching sources or new purposes has the goal to better inform data subjects in the hope that they are then more eager to say '*Yes*'.

If a new information stream is added to the data collection used in the context of the location-based service, this new information source can be data collected from the data subject directly. For such directly collected data, the controller's information obligations according to Article 13 GDPR apply. But the system may want to use data that was either acquired from third parties, or data that was already collected by the controller under a different purpose, most probably under a legal purpose in the sense of Article 6 para. 1 (c) or (e) GDPR. In this case, the controller's information obligations according to Article 14 GDPR have to be fulfilled. For a general overview of the information

[36] See Footnote 31.

requirements, see D1.2, chapter 2, section 2.2.6. In the following, some additional considerations will be made with regard to both Article 13 and 14 GDPR within the context of a general LBS use case.

2.1.2.1 Notifications according to Article 13 GDPR

A telecom operator has a lot of information about their subscribers. This information is normally very regulated and can only be used for purposes specified by the (telecommunication) law. The same goes for Internet Service Providers. The fact that our entire life with all of its social interactions becomes increasingly affected by the digitisation produces a variety of data sources that could be usefully combined. In this context, the SPECIAL system could offer an interface providing the opportunity of getting permission for a re-purposing of interesting information for useful services. The interface is there to ask and to receive specific limitations to the use of that information. In most cases, the service provider in need of the location information may be identical with the telecommunication operator or the Internet Service Provider. So if this controller wants consent for the further use of the location data for other purposes, it is the same legal entity which is subject to the information obligations of Art. 13 GDPR. Therefore, the data controller must provide the information as required by Art. 13 GDPR again when data (that has been collected from the data subject under a different permission) is intended for further processing.

The question is now how to re-purpose that data with the permission of the data subject. This needs additional consent and prior information from the controller, as explained above.

While the identity and the contact details of the data controller will be most probably identical to the contact already established during installation, the purpose(s) according to Art. 13 para. 1 (c) GDPR, and perhaps some asserted legitimate interest according to Art. 13 para. 1 (d) need to be communicated to the data subject. If the new processing purpose involves new recipients, those have to be listed. They could be written back into the control interface. One could imagine a location-based restaurant reservation system. In this case, the restaurant, and not only the service provider, would receive and process personal information from the data subject. Location and contact information could serve the data subject to find the restaurant, but also to complain in case there were some issues. Of course, the famous social networking sites would have to assert that they transfer data into a third country that has no adequate protections.

Art. 13 para. 1 and 2 GDPR have a rather long list of points of information to be provided to the data subject. This could, again, overwhelm the data subject. Yet, this could be remedied by using a layered approach. In a first layer, the new purpose, the data categories and the context should be mentioned. If data is given to third parties, this should be mentioned shortly on the first layer with a link to a more complete explanation. The overall control interface in SPECIAL allows to push data retention times, international transfer, the access and rectification rights to a layer further down. Probably, most of that was already covered by the initial installation and does not have to be repeated. The hint towards the right to object to automated decision making etc. was also already in the initial consent for the overall SPECIAL framework. This suggested approach is additionally supported by Art. 13 para. 4 GDPR stating that information obligations do not apply where the data subject already has the information.

2.1.2.2 Notifications according to Article 14 GDPR

A service may not only be intended for re-purposing information, but also to acquire information from third parties, as well as to combine this third party information with the information already collected. This could significantly enrich the profile e.g. to allow for better filtering, or for better scientific research.

Adding information from third parties to a profile collected directly from the data subject is an undertaking in need of a sensitive approach. An example where this was handled unprofessionally is

the famous acquisition of Abacus Direct Corp. by DoubleClick Inc. in 1999 turned into a public relations disaster for DoubleClick.[37] This means that adding information from third parties needs a careful course of action. Again, the layered approach and the contextual fences of the consent request will probably take away most of the perceived '*creepiness*' that can occur if profile information is correlated to, or augmented by third party information. But it can be really benign, e.g. if my location information is correlated with the traffic information in general, or even the traffic jam situation of friends on their way to a get-together. In all those cases, utmost attention has to be given to the perceivable '*creepiness*' factor.

The GDPR enforces transparency towards the data subject by requiring a number of information points to be communicated in cases personal information is not collected from the data subject directly. This is governed by Art. 14 GDPR.[38]

Yet, while the communication with the data subject must in some way convey all information required by Art. 14 GDPR, this can also be done in a layered approach, as seen above. This information has to be provided at the latest within one month and in case of further processing (which is the case here) before any of this processing of the third party information occurs.

A layered approach would make it possible to hide most of the points required by Art. 14 GDPR in a second or even third layer. This is possible because Art. 14 para. 5 (a) gives a dispensation if the data subject has the information already. So the SPECIAL control interface (dashboard) needs to take into account Art. 14 para. 2 (f) GDPR, which requires that information about the origins of the third party personal data is given.

Due to the aforementioned considerations and requirements, an initial suggestion is to take the W3C provenance framework into account in order to make the third party information machine-readable. This will benefit the control interface. As the control interface gets more sophisticated, it is argued here that the barrier to consent should be lower, the messages and information notices could be shorter, and the first layers non-intrusive.

One specific situation for location-based services is if the location information is not only exposed to the service, but also to other data subjects in order to connect them. In this case, the system must enable and maintain a double consent management:

- The consent from each data subject for the service to use the information and
- the mutual agreement between both data subjects as users of the system to exchange location information.

Such a consent management needs special safeguards, as sharing location information between data subjects may under circumstances be seen by them as a very sensitive form of personal information. Not always, when data subjects call each other, they also want to let the other know where they are. Therefore, it is suggested that in this case, large parts of the messaging system that the service already used for enrolment could probably be re-used to take this specific scenario into account.

[37] From the web archive: https://web.archive.org/web/20000302160653/http://www.usatoday.com/life/cyber/tech/cth211.htm Will Rodger, USATODAY, Activists charge DoubleClick double cross, Web users have lost privacy with the drop of a cookie, they say, published 2000-01-21.

[38] For the details which information must at minimum be communicated, see D1.2 page 33.

2.1.3 Using live information

The beauty of location based services is that they are able to help people on the go. This means that live information from the device is used to provide information or a service depending on that live information. The most prominent services in this respect are probably car navigation systems. But services like eCall can also count as live information services. Live location information is not sensitive information in the sense of Art. 9 GDPR. It is nevertheless very sensitive information in the commonly used sense of that term because it can reveal a lot of information about a data subject. It is highly recommended, if not required to indicate in the user interface that live location data is actually sent to the service provider or data controller.

The dangers of live location information are twofold: The live information creates a security issue and a data protection issue.

2.1.3.1 Live location information as a security issue

The live location information obviously tells where a person is actually located, thus permitting a physical access to this person. Having physical access may cause physical damage. This means there is a security issue with access to the live location information. And this is not a data protection issue as it is not the creation of a dossier that creates the danger, but the single information. We are thus confronted here with a challenge to maintain the secrecy of the live location information. Data protection rules do not help here as they are made to prevent the creation of dossiers. This is a typical access control problem with its attached identity management challenges. If we imagine a service provider and data controller mediates the access of two data subjects to their respective location information as has been done in the Google latitude service, it is important to get the access control management right. There are no deep legal considerations needed other than perhaps the liability of the service provider while spreading live location information to others without control. In the European telecommunications industry, such protections are obviously already taken into account. The experience from Google latitude teaches us that the live location information exchanged between more people than the data subject and the data controller/service needs a well crafted live control system. It needs a system that can switch on and off the visibility of the data subject at any time. Perhaps even with the possibility to switch visibility off for specific groups while at the same time leaving it on for others. One of the critics to the Google latitude project, was that it was too complicated to go incognito. It would be a really nice feature to be visible to only one friend or a certain category of friends. The work of Primelife in privacy enhanced social networking[39] may help there.

It is important to enable the data subject to switch off the service in cases where they wants to change context. Obviously this needs information about the context in the interface. Where am I, who can currently see my location? Which groups can see my location? Can I switch them on/off? Can they record my location information? Finally, because of the risk of stalking and assault, switching off live location information may not be good enough. One could imagine an interface allowing a person to give a fake location to another person. This may even include police notifications and exact location information for them.

2.1.3.2 Live information as a data protection issue

Live information can be ephemeral. While using the navigation system, it shows a moving point on a map. But there are systems that can record your journey. This can be interesting, or annoying. With a

[39] Van den Berg, Leenes, Privacy Enabled Communities, Primelife D1.2.1, http://primelife.ercim.eu/images/stories/deliverables/d1.2.1-10.04.23-privacy_enabled_communities-public.pdf published 2010-04-23 accessed 2018-03-10.

connected device, location information present on the device can be recorded by the provider of the app. While navigating with Google maps, Google collects location information. It is impossible to find out from their privacy policy for which other purpose the location data is used when navigating[40]. The policy then hints that data may be shared with others and it may be used in an anonymized way. In fact it is often the case that the service provider is collecting live information and reusing it in other contexts. This is the classic data protection issue where over time, a record is built up. At the beginning this recording is not creepy at all, but a recording over time may be very creepy. A story that got a lot of public attention came from Malte Spitz, a green party politician. He made a data access request for his phone data to his telecommunications provider for the past 6 month. He than made the data available to the journal Die Zeit who made a profile by combining his location data with a map and his other online activities, namely on social networking[41]. The resulting application showed how potentially invasive location based services are if they accumulate data over time. This is reason enough, to pay special attention to the accumulation of information over time in location based services.

The Directive 2002/58EC contains explicit rules on live location data. Art. 9 para. 1 of the Directive explicitly requires that service providers allow users to withdraw their consent at any time. The new ePrivacy Draft has those rules in Art. 9 that allows for specific consent and withdrawal of consent through the same interface. The rules remain the same, but the ways in which they can be implemented are more modern with the ePrivacy Draft.

A SPECIAL implementation of a location based service could offer data subjects several options here. First, it could offer a button that would stop the live stream of location data to the service provider and any other user. This is the most radical measure. It could be called a stop button and be represented using a typical emergency red colour and may perhaps even be combined with an indication that the location information tracking is active. If pressed all data collection in the SPECIAL application would stop until the button is released again. Secondly, there could be a switch allowing data subjects to maintain the location based service, but indicate that the live location data collection should not be recorded into a profile. This would typically be the case if a data subject wants to use the location based service, but does not want to add the actual live information to the profile or the machine learning in the backend. Further options could play with the granularity of the location information or with tools like k-anonymity in the location based context.

2.1.3.3 Aggregation and Heatmaps

If location data is recorded with the consent of the data subject, the consent normally binds the data processing to the purpose agreed to within the consent statement. But the data protection regulation allows is not application if data is sufficiently anonymized.

The widespread use of mobile devices has rendered views on peoples movements possible that were unthinkable 15 years ago. Now everyone has a smart phone. Heat maps are possible today already. The SPECIAL system is not necessary to produce statistical data from existing data collection e.g. under some other legal ground then consent. The anonymisation techniques applied by data controllers are under the constant challenge of ever improving techniques of de-anonymisation.[42] Striping some bytes is not enough anymore. But the proportionality of the efforts has to be taken into account.[43]

[40] https://www.google.com/policies/privacy/ accessed 2018-03-26.

[41] Tell-all telephone, OpenDataCity, http://www.zeit.de/datenschutz/malte-spitz-data-retention published 2013-08-22, accessed 2018-03-23.

[42] For all see Narayanan, Arvind, Shmatikov, Vitaly: Robust de-anonymization of large sparse datasets, Security and Privacy, 2008. SP 2008. IEEE Symposium on, 111–125, 2008 .

[43] See Recital 156 of the GDPR.

A SPECIAL service may add higher quality heatmaps, e.g. by correlating location and interest. But such application would then have to make sure that the correlation does not reveal additional information that could serve to re-identify persons with specific interests or to enable the singling out of people in order to discriminate them in some way. The more sensitive the information processed, the more care has to be taken to make sure the aggregation is at the right level of granularity to prevent that some third party can again single out data subjects from that heatmap.

2.1.4 Fencing the data collection

One option to make a nicer interface for location based services is to allow data subjects to limit the application of location data recording not only in time, but also in space. An interface could be as wide as covering an entire country in the EU, but it also could be reduced to some more narrow area.

A data subject may want to use the location based service when they are outisde of their normal area of living, but may not want to have the system active when they are in the vacinity of home or work. A location based application could offer to define such areas on a map and take them into account in the SPECIAL system. This can be either realised by switching off the collection of data, but also may concern the recording of live location information. This may even help the service as they do not want to have their profile polluted with large amounts of every day repetitive data recordings that would dominate the filtering.

An interface could also allow a data subject to define certain data categories that they would prefer not to be recorded. This is challenging as such information can be explicitly sent from the device. In this case it is rather easy to determine the category and to not record the data. But it is also possible to derive certain information from the collection of traffic data, possibly combined with location data. In this case, it is much more complex to avoid all implicitly possible deductions on the data collected. A sanitization in the backend may be helped with linked data categorisations combined with a certain amount of reasoning and machine learning. But this is nothing the legal framework would require, but rather an additional feature to implement the promise to the data subject not to collect a certain type of data.

Finally, considerations about time of collection may play a role. A system may only be active during the average working hours of an employee. Or the other way around, not be active as soon as someone is in the workplace. Those are not only time constraints. Other metadata can be included into the on/off algorithms. This could go as far as switching an application off in the presence of the employer's WIFI network. It is worthwhile to note that the Internet of Things will allow such an application to collect ever more markers to fine tune the activity of the system depending on sensor data surrounding it.

2.2 Proximus use case (recommendation system)

In this chapter, the above described elements for a GDPR-compliant generic location-based service (LBS) with the potential to enrich a user profile with additional information will be matched to the Proximus recommendation system use case as it is explained in D1.5.[44]

Thereby, this document will make a couple of suggestions how to adapt the Proximus use case. These aim at facilitating the GDPR preconditions for valid consent and a data controller's transparency and information obligations. Moreover, they anticipate possibly relevant provisions of the upcoming ePrivacy Regulation in its Parliament draft version. This version is understood as a blueprint to make lawful processing of personal information in the context of a LBS possible. Yet, in the way it is described below, it can also serve industry interests by avoiding the '*consent-fatigue*' or '*click-fatigue*' of a user and help building a trustful customer relationship.

In the following, the above described walk-through steps of the generic LBS will be adapted for the Proximus use case, starting with installation and subscription, then continuing with enriching the profile, the necessary notifications, and instruction on how to use live information and to geo-fence the data collection based on the categories/amount of data needed and the user settings.

It may be highly beneficial if an icon in the interface of the app or TV application could be displayed in context when the profile learning is active.

2.2.1 Installation and Subscription

Based on the general description under section 2.1.1, the specific Proximus use case could similarly start with the installation of a mobile application on the data subjects smartphone, who would typically be the customer of telecommunication services. But we may also imagine using a service on the web where the enrolment into the service would be similar.

In the following, it will be described how this installation and subscription to the use case specific service of recommending events at the Belgian coast could occur. Thereby, suggestions will be made inline with the GDPR and the draft ePrivacy Regulation with regard to the following aspects:

- which minimum information must be communicated to the data subject at this stage; and
- which options must be given to the data subject to facilitate the needed user control.

It is the preconditioning assumption that a customer of Proximus (data subject) becomes aware of their event recommendation service and is interested in using that service. Upon installation of the application that facilitates these recommendations, some kind of installation wizard may be started to configure how this app should be run and to give the customer the (legally) necessary information to for valid consent.

As already explained in D1.2, the draft ePrivacy Regulation refers to the conditions for valid consent in the GDPR. Art. 4 (11) and 7 of the GDPR demand that consent is

- freely given, specific, informed and unambiguous (for one or more specific purposes);
- possible to withdraw at any time; and
- a statement or clear affirmative action of data subject expressing agreement.

[44] D1.5 *Use case scenarios V2*, chapter I, pages 8-14.

Usually, this would be understood in a way that a detailed and accurate description of the service, the data categories collected, and the processing modalities would be absolutely necessary. However, such an approach would in the context of the project's use cases lead to exactly the issue described in the introduction of this deliverable; a person potentially interested in such a service provided by Proximus would be overwhelmed with information in the context of a classical, lengthy and rather user-unfriendly because it is extremely difficult to read a consent request on a tiny mobile screen.

But strong arguments can be made that the above mentioned conditions can be realized still optimally by a layered approach. Such an approach would make the acquisition of valid consent in line with the GDPR possible in the digital context, such as via a small mobile screen. The Article 29 Working Party already acknowledged this necessity to avoid '*information fatigue*' of data subjects when they are bombarded with lengthy and incomprehensible masses of information at once on screen. According to the Art. 29 Working Party,

> '*Layered privacy statements/ notices can help resolve the tension between completeness and understanding by allowing users to navigate directly to the section of the notice that they wish to read. […] The design and layout of the first layer of the privacy statement/ notice should be such that the data subject has a clear overview of the information available to them on the processing of their personal data and where/ how they can find that detailed information within the layers of the privacy statement/notice. It is important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.*'[45]

For the Proximus use case, this addresses the initial UI ideas relating to the customer's introduction to the event recommendations. So the question is, which minimum information must be conveyed on the first layer, while the remaining information may be placed on subsequent layers to which the data subject can navigate if interested. Regarding this question, the Article 29 Working Party has suggested that the first layer should '*always contain information on the processing which has the most impact on the data subject and processing which could surprise the data subject.*'[46]

Applying this on the Proximus use case, our recommendation in this deliverable is that in a layered approach, the first layer should at least mention the purposes of the processing and the data category initially collected.

While this is still very basic information, the installation wizard that follows next will make up for this by giving the data subject all other needed information in comprehensible and digestible portions before the data subject is even asked for consent.

So building upon the suggestions coming from work package 4, the initial text could look like:

> '*Enjoy events near the beautiful Belgian Coast! Sign up for tourist event recommendations which this app can provide to you based on your location.*'

Next, the installation wizard needs to guide the data subject through the app installation process, thereby step by step giving all the necessary information. In this context, special care should be taken to convey all information that may '*surprise*' the data subject, such as the novel ways provided to pre-set consent modalities during the app installation, the possibility to add other data categories

[45] Cf. their '*Guidelines on transparency under Regulation 2016/679*', WP260, page 17.

[46] Ibid. page 17.

later on, and the option to access a user control interface where settings can be viewed and changed at any time, giving the data subject full control.

So progressively, the data subject needs to be informed at least about:

1. Whether there are costs attached to that service.
2. To which specific geographical area the service applies (or that you can choose a region).
3. That location data is necessary to use this specific service.
4. That Proximus as a telco provider has the location already and asks for consent to further use this information to provide this event recommendation service.
5. That the data used for this service is stored for a certain retention period (specify).
6. That the app has an '*incognito mode*' in the app to temporarily interrupt its usage of the location data without completely unsubscribing to the service (called '*Not now*' button).
7. That once the service subscription has occurred, is is possible at any time to control and manage the collected and processed data via a web interface, where you can log in to a dashboard.
   - ✗ This information should be given upfront. Provide a link to the dashboard later at the end of the installation process. Instead of a link, a QR code may be used alternatively, which facilitates the login to the dashboard.
8. That it is at any time possible to withdraw consent to the processing and to unsubscribe from the service.
9. That if the data subject wants better recommendations later on which are more tailored to personal interests, he/she has the option of adding more information later on to an interest profile.
   - ✗ At this point, the data subject can agree or disagree explicitly (select '*Yes*' or '*No thanks*') whether he/she wishes to be asked in certain situations if specific additional information may be added to the interest profile in order to get a better service.
   - ✗ If selected '*Yes*', give information that there is the possibility to pre-set how the app should behave in the case of such additional consent requests:
     - **Active reaction** by clicking '*Agree*' or '*No thanks*'.
     - **Implicit reaction** by allowing the app to assume my consent to the add-on interest enrichment, unless I react/disagree within [...] seconds/minutes during the display of the consent request. Ideally, the data subject is even given the option to pre-set how long this request is displayed on the mobile. Make clear that for sensitive information, the app will still always ask for explicit consent.
10. That it is at any time possible to withdraw completel or even partial consent to the processing of the given information and to unsubscribe to this service.
    - ✗ Be clear that location is the basis information needed for the service, so withdrawing consent there will mean to unsubscribe completely. While all other data categories can be removed without losing the service.

It is not necessary to convey this information in 10 discrete steps during installation. Rather, ways could be found to summarize and/or combine the information to make the process of getting the app up and running smoother. The following section 2.2.2 below describing the enriching the profile process provides some more substantial and exemplary phrasing suggestions.

Moreover, a layered approach can be used to guide the data subject through some parts of the setup, which means: check first whether additional add-ons to the interest profile are desired, then proceed to the consent preferences. This way, it may be easier to communicate digestible bits of information at a time.

However, **at any time**, meaning during each step of the installation process, the installing customer should be provided with the following options to control the installation process:

- '*Back*' or '*Abort*' button.
- '*Forward*' or '*Continue*' button.
- Clickable link to the relevant Proximus Privacy Policy website.

As explained in section 2.1.1 for the generic location-based use case, the guidance through the installation process including the setting of consent preferences enables the later enrichment of the profile if the data subject has agreed to that modality upfront and explicitly at the beginning. This also applies for the profile enrichment via implicit consent, which is the second modality that has to be agreed upon explicitly. Is this the case, Proximus as service provider would be allowed to assume consent IF the customer does not react within [...] second/minutes when the add-on consent request appears on the mobile screen (blend-in shade only visible for that pre-set time period). It is possible for the industry partners to combine this with information about the benefits the user of the apps gets out of this approach, namely a better, personalized service, better recommendations, etc.

This step by step approach to pre-set the data collection and consent modalities as suggested in this deliverable is compliant with the conditions for valid consent both in the GDPR as well as in the draft ePrivacy Regulation in its Parliament version.

Because by explicitly agreeing to this app behaviour with regard to further consent requests, the data subject issues a clear affirmative action or statement that is also informed and unambiguous in the sense of the GDPR. As it was already analysed in D1.2, the GDPR does indeed allow electronic means by which the data subject may express his/her wishes.[47] Moreover, D1.2 there pinpoints to Recital 32 of the GDPR, which gives examples for valid consent, such as choosing technical settings for information society services, which would cover the proposed approach for the Proximus use case perfectly. Such technical settings are pre-set by the agreements of the data subject during installation. Additionally, this pre-setting allows to assume that for later consent requests a statement or conduct indicating the data subject's acceptance if they do not react actively when the blend-in screen informing them about the additional data collection appears on the mobile display for [...] (pre-set) seconds/minutes. Therefore, this approach is in line with the GDPR conditions for valid consent.

With regard to the draft ePrivacy Regulation, this is mirrored by the Articles 8 and 9 in the Parliament version. Especially notable in this context is Article 9 para. 2 stating that when '[...] *such technical specifications are used by the user's terminal equipment or the software running on it, they may signal the user's choice based on previous active selections by him or her. These signals shall be binding on, and enforceable against, any other party.*'

In the description of the generic LBS use case under section 2.2.1, it was already explained how this provision would provide an industry-friendly, yet still also data protection compliant way to achieve an informed agreement from the data subject. By determining these setting, later interactions are made more convenient for both parties while having a far better chance at avoiding the 'click-fatigue' feared by the Big Data industry. Moreover, the data subject's level of being informed and in control will be enhanced since he/she can at any time access more information about Proximus' handling of the personal data, plus additional possibilities to actively access the dashboard and change the

[47] D1.2 *Legal requirements for a privacy-enhancing Big Data V1*, chapter 2.2, section 2.2.5 (c), page 29.

agreements made later if so desired. In any case, the status of the consent should be logged for auditability reasons.

2.2.2 Enriching the profile

This section will explain how the user's (namely the data subject's) interest profile could be enriched with information. Thereby, some very concrete examples will be given how the data subject could be informed prior to the data collection and processing. After discussions between the legally versed experts in the project, these examples have been found to comply with the controller's information obligations laid down in Articles 13 and 14 GDPR. These examples concern not only text, but also hint at implementation ways how to communicate this information to the data subject in a layered approach that may not be so overwhelming and remains digestible. Of course, the examples in this section are suggestions only, yet provide a good way how to convey the legally required minimum information to facilitate valid, informed consent form the data subject.

So at the beginning, imagine that a location-based system only records and uses location based information if the mobile device is in a certain geographical area. For such a system, it would mean that the installation procedure has not yet asked about the collection of any location-based data.

The data subject now wants to add the area 30km around Brugge. This location and radius are also only suggestions here for the purpose of exemplary showcasing the further steps.

However, adding location and radius can be done in a push or pull scenario. Imagine a push scenario with notifications. The data subject enters the region 30km around Brugge. In the initial installation wizard, consent could have been given to the mobile operator to re-use the location information '*presence in this 30km area*' to notify and to offer location-based event recommendations in this area.

The smartphone now pops up a notification, which says: '*Do you want event recommendations in this area? We will collect and use your precise location to provide the service. <know more>.*' '*<know more>'* is a link. Following that link leads to an information box giving the next layer of information. This could read like:

> *'In the area of 30km around Brugge, the application will use location data given by your smartphone or known to us via the network infrastructure to suggest events to you. Location and events chosen via the application will be written into a profile that you can control via this interface to provide even better recommendations in the future. The raw information will be kept for a year, the marker will remain in your profile until you delete it <here>. <Learn even more>'*

'*Learn even more*' is again a link to the next information box that has the full set of information for the data subject accessible, which is in line with Article 13 GDPR.[48] This could be something like the following exemplary message:

> *This application is provided to you by the SPECIAL corporation with its headquarters at [valid address]. If you have any questions, please contact our representative [name] under [email and/or postal address, preferably both]. If you have questions about the collection or use of your data, please contact our company-internal data protection officer [name] under [email and/or postal address, preferably both].*
>
> *Network data, namely the location, is collected following Article 6 para. 1 (b) GDPR.*

[48] For details about the required notifications, see D1.2, chapter 2.2.6, section (b), page 31.

You are about to give, or you have already given your agreement to the collection of location information and to the creation of your user interest profile to be matched with our event database in order to provide you with event recommendations.

Your data remains within the European Union and we do not give your data to third parties. We will use your data to create aggregate statistics for the events, how many people saw the event recommendation, and how many people ordered a ticket from within this application. Those aggregated statistics do not contain personal data anymore. You can object to the use of data for statistics by setting the appropriate option in the control interface.

We will store your data and the history of recommended events until you uninstall this application, erase your profile[49], or until you selectively delete some information via the control interface of this application that can be found <here>.

The profile created serves to know you better and to determine your interests according to a number of criteria. Those criteria will be matched against characteristics of the events taking place in the active area.

This control interface will provide you with the possibility to access, erase and rectify your data. In case you find a competing app that you like more, you can export the data as standardised RDF Linked Data format.

You can generally or selectively withdraw your consent any time. If you don't want to have recommendations for a certain area anymore, please delete the permission for that area in your control interface.

We collect location data as long as you are within the targeted area for recommendations, and as long as the application is active. This data is kept for 30 days. You can also use an 'incognito mode' which stops the data collection anytime by pushing the 'Not now' button.

We may come back to you and ask for further processing, which is a possibility for you to add more information to your interest profile. This can be done via various consent modalities you can choose in advance before starting the app and which you can also change at any time. By allowing us to collect and process the further information (additional to location), we will use it to personalize your interest profile further in order to give you better event recommendations.

For more information see our privacy policy at [direct URL link to the relevant full privacy policy of the controller organisation]

Adding a new area would now just change the first screen that names the area where the data subject agrees to provide location information. The granularity of location information, or any other user information is a matter of implementation and the concrete use case.

Other information can be added in a similar manner. This may include sensor information about the accelerometer inside the device used, or any other information present at the time. The high level information will change, but the large document at the lowest layer will remain mostly the same. We imagine those texts will be generated from the environmental data that is collected.

In the following, some further implementation suggestions are made to facilitate both contextually embedded further consent requests and data subject control.

- For TV viewing data, or social networking data after agreement:

[49] This is the option for websites.

- The need for a '*Not now*' button while viewing TV or using the internet.
- The timing for the consent request to use TV viewing information is during the start trailer of the film. Blend-in a consent request for a few seconds before it disappears. Ideally, the blend-in message could also re-assure the data subject that no sensitive information (read: special categories of personal data) will be processed without explicit consent.
- The timing for the consent request to use internet surfing behaviour is per site. Whenever a new site is reached out to, the shade comes down for a few seconds.

- For the further use of existing telecommunications data
  - Call data records need agreement from both ends of the call, best if both parties have this application (who else is going there). Use case partners should omit to make recommendations based on data they have without having the agreement to use that data from both customers.
- Adding the location of other customers to create a social network around the events
  - In case more than one person has such an event recommendation application that knows the location of the data subject, others may be interested to find each other at an event. Or to see what the interest of this other person is. In this case, data is shared between different customers. This could be facilitated here if two people have the same application. In this case, one customer could ask another customer to agree to share information. Again, a good layered approach could be used.

In D1.2, the general information obligations of the controller according to Article 13 GDPR for personal data directly obtained from the data subject have been explained in detail already.[50] Linking back to the specific Proximus use case and the suggested information texts above, all needed information is conveyed already as far as data is concerned that has been collected from the data subject directly, such as location.

If a future extension of the use case is intended to collect personal information from third parties, the above text would need to be adapted to comply with the information obligations of Article 14 GDPR as well. The required minimum information that needs to be communicated to the data subject in such a case is also described in D1.2.[51] In this deliverable, it is only highlighted for the time being that **additionally to the information given due to Art. 13 GDPR**, further information needs to be given to the data subject, which means the categories of personal data concerned and the data source(s), including info whether it came from publicly accessible sources

2.2.3 Additional options for user control

As was seen in the sections 2.1.3 and 2.1.4, additional features could be added to make the implementation of the use case more user and data protection friendly. If live location information is shared, the application MUST indicate this in the user interface and it MUST enable the data subject to easily switch the location data sharing with others off. Section 2.1.3.1 provides the necessary argumentation for this constraint, which is all about the security of the customer.

Another option is to better control what gets written to the profile and thus enable data subjects to influence their own profile. We could imagine that the location trail of a data subject done for their work would poison the profile for the events. In this case, events related to his work-interests are

[50] D1.2 *Legal requirements for a privacy-enhancing Big Data V1*, chapter 2.2.6, section (b), pages 31 ff.

[51] Ibid.

shown. Now let us imagine the reason for installing was mainly private interest. In this case, the return and recommendations of the app or service will be wrong. Even worse, if the app was installed in a professional context and behaviour or things from the private sphere get recorded, this may lead to unwanted revelations concerning the data subject. One could imagine to time-box the feeding of the profile or to allow the user to easily switch on and off the feeding of the profile. This does not have to be in the first layer to avoid confusion by those not concerned by this case.

The Proximus case theoretically allows to add many data sources to feed the profile and to make it more accurate and usable. Adding those new streams of data should follow the procedure suggested in section 2.2.2.

The number of possibilities to add sources is nearly infinite. But a blind streaming of all content from a variety of sources may also feed sensitive information into the profile. This may even be sensitive information in the sense of Art. 9 GDPR, like race, gender or sexual preferences. Going beyond the contextual on/off button, there is the idea to allow the profile to detect automatically when sensitive data is involved and to block that information from being added to the profile. This could be done using machine learning techniques. Such a filter would be very important if the data subject chooses to allow his social networking information or TV watching behaviour to be used to improve the profile. As we have seen, an implicit consent, like a shade that goes away after a few seconds, works for most of the options and for the enriching, but not for the special categories of personal data of Art. 9 GDPR. In this case, the data subject has to agree explicitly and the purpose has to be narrowly defined. A filter on those data categories may therefore also help the user interface to distinguish between consent requests that only concern '*normal*' data and those involving sensitive data as defined by Art. 9.

Finally, a data subject may not want to have their profile being enriched with their day-to-day routines of going to work, coming home or going regularly to a certain location. An option would be to allow the data subject to define location areas where the system is not active and does not collect data. This concerns mostly information streams that enrich the profile while the data subject is on the go. This could be location data, but also data from the interaction with others.

In any case, whatever feature is additionally offered, it should use a layered approach where there is a simple first explanation that appears in the context of the first use. This simple first explanation should then have some '*Know more*' link to more information.

2.3 DTAG use case (Dual use for QoS & movement analytics)

In this chapter, the elements described for a GDPR-compliant generic location-based service (LBS) with the potential to enrich a user profile with additional information will be matched to the use case of DTAG. DTAG initially intended another use case that did not materialise for reasons external to the project. The SPECIAL risk mitigation strategy worked and not only one, but two very appropriate use cases with high practical relevance were found. A legal assessment is dependent on a description of the use case in sufficient detail. All other use cases were described in Deliverable D1.5. In order to be able to provide a meaningful legal assessment and as part of the SPECIAL risk mitigation strategy, a description of the DTAG use cases is provided within this chapter.

After the use case description in the following subsection, this chapter will then follow the same structure as the prior chapter for the Proximus use case, thereby providing initial thoughts from legal perspective how to facilitate a dynamic, layered approach enabling efficient consent management in line with the GDPR.

2.3.1 The current state

The use case is based on existing scenario where DTAG and its spin-off Motionlogic are involved in the collection and processing of personal data of mobile users. They collect similar data, partially from the same data sources. Data is directly anonymized upon collection and almost not shared between the two companies:

- **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*'. Each data set collected here includes (among others) geolocation information measured via device GPS. Radio data (reception quality etc.) are collected, aggregated, condensed and sent to a data base. Datasets are by default anonymized and/or pseudonymised to protect user's privacy. Users gave their informed consent during installation of the app. Data sets are then collected and evaluated statistically for improvement of network quality. The department responsible for the app and database is looking for additional use of the data collected.

- **Motionlogic** (https://www.motionlogic.de/blog/de/), an independent Spin-Off company of DTAG, uses anonymized and time-delayed data of mobile phone usage (location data, cell-tower location) to offer 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 DTAG (T-Mobile brand). Rather Motionlogic does the requested processing internally and only delivers the results (e.g. heat maps). Due to limited quality of the anonymized 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. The current rate of 'Opt-in' consent is very low. Giving users more control could lead to a higher rate of people willing to share their data.

2.3.1.1 Data collected (using today's CNE App)

The data collected today by the CNE app has about 75 data fields (attributes), all of them related to network scans. Some of these attributes are clearly person-related and/or identifying a device/contract and thus a customer.

There exists a CNE App Data Dictionary which contains all attributes. However, since these are business logic, they are not included in this deliverable. Rather they will be treated as confidential and only distributed to the necessary partners in the project to facilitate the technical realization of the use case.

Some of the most relevant attributes for the use case are NOT related to network quality, but rather to (exact GPS) location and time.

The following list shows a subset of the attributes.[52] These may be chosen for the use case:

Partial Data dictionary

Attribute	Description	Unit / datatype
user_id	Foreign key to 'user' table. Identifies an individual app user so can be used to correlate scans from one user to each other. For active scans always filled in. As well as for all scans made when opted in in diagnostic mode. For background coverage samples, the user_id is always set to / N, so that those remain untraceable to the individual.	Integer
phone_id	Foreign key to 'phone' table. Identifies an unique handset. Phone_id is mutual exclusive to user_id. For network samples and event scans always filled in, unless scans are made when opted in in diagnostic mode. For active scans and all scans made in diagnostic mode, the phone_id is always set to /N.	Integer
netcode	MCC + MNC of the IMSI of the mobile network connected to. Value is 0 when there is no connection to a mobile network (Android only)	Numeric: MCC+MNC
surrounding	User provided indication of the nature of the surroundings when performing an active scan. Value is 'Unknown' for the other scan types.	Enumeration: Car Indoor Outside Train Unknown
latitude	Latitude in the WGS 84 coordinate system, as determined by the handset.	WGS 84 coordinate
longitude	Longitude in the WGS 84 coordinate system, as determined by the handset.	WGS 84 coordinate
speed	Moving speed recorded while measuring the scan.	in km/h
accuracy	Accuracy of the coordinates provided by the handset. The accuracy depends on the method of location determination, e.g. based on an actual GPS reading or on nearby cell towers or WIFI signals	meters

[52] Due to the above described business secrecy issue, the attributes table is displayed only partially.

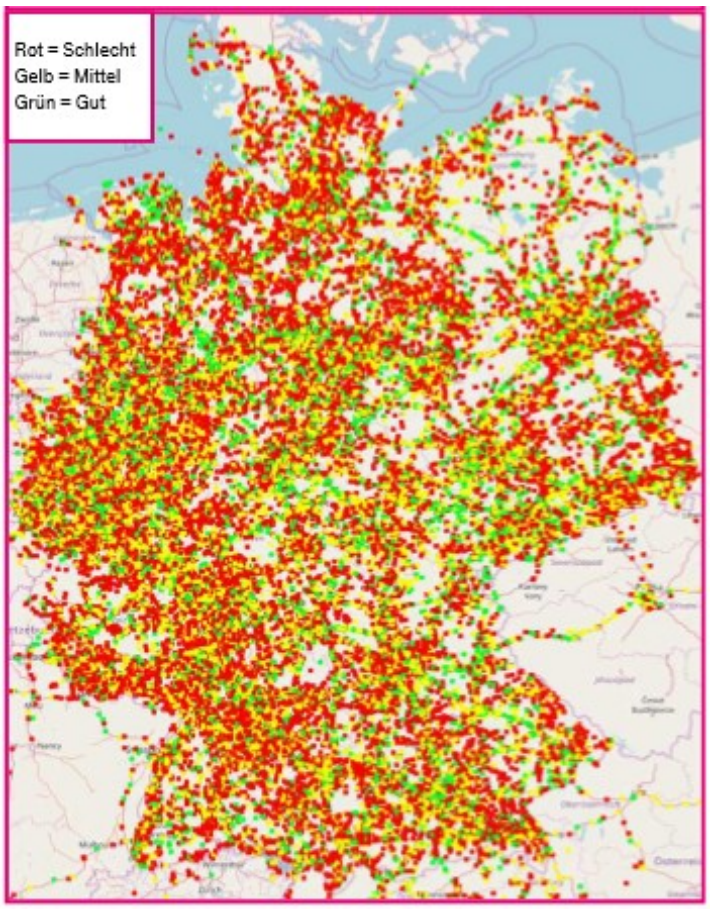
lac	Shows the LAC or TAC 16 bit Code for a Location Area: an area designated by the operator to divide the country in discrete areas. Together with the MCC and MNC, the LAC/TAC forms the Location Area Identifier. (Android only)	16 bit number
cid	Shows Cell ID. A unique number used to identify each Base transceiver station (BTS) or sector of a BTS within a Location area code. (Android only)	
ssid	Service Set Identifier; textual identifier for the WiFi network the handset is connected to.	String
bssid	Basic Service Set Identifier: MAC address of the Access Point that the handset is connected to over WiFi	MAC address
created	Time this scan was uploaded to the back end	dd/mm/yyyy hh24:mm:s
wifi_available	Shows if device could connect to wifi. Is connected to, or about to connect to wifi.	0: no connectivity ma 1: wifi -1: more certain there is
diagnostic_optedin	Is a diagnostic mode active?	0: 1: yes

The attributes '*latitude*', '*longitude*' and '*created (time)*' are very relevant. The fields '*user_id*' and '*phone_id*' are person related and this sensitive. The term '*diagnostic_optedin*' refers to a consent given for non-anonymous data analysis (and possibly sharing).

Currently the CNE-app using complex anonymisation is already in use:

- Number of unique active users (daily): 500 to 2000
- Number of measurements (samples taken daily): 20.000 to 80.000

This results in the following location measurements with a focus on Germany:



Drawing 5: Measurement locations in the TLABS use case

Note: The colours of the dots indicate network quality (perceived/measured). This is not relevant for the use case. Only the location/position is used for anonymous sharing with Motionlogic.

2.3.1.2 Data Privacy features of the current CNE App

The current CNE-App has a general all encompassing consent form during install. The app documentation, provided by the developer of the app in the Netherlands, Oberon contains further details. As a Dutch enterprise, Oberon followed Dutch privacy legislation. Current Dutch and German data protection legislation only derive marginally from each other. A further full conversion is expected with the GDPR coming into force on 25 May 2018. This will be taken into account when describing the target 'SPECIAL enabled' state of the application. The following requirements were elaborated by the Dutch T-Mobile legal department and taken into the account:

- SEC1: All customer data is to only be stored in systems within the T-Mobile NL domain.
- SEC2: When opted in for diagnostic mode, this option should have a time limit build in (default 1 week)
- LEG1: Guarantee that the data collected in the Background scan is fully anonymised.
- LEG2: Clear terms and conditions when user is opting-in, so when the data is matched to user-specific data.
- LEG3: Communication towards end-user what is done with the user-specific data and the improvements done in the network.

Based on this, in the current state, a number of decisions was made, notably:

- Background scans are anonymous and always activated
- Event scans are anonymous and always activated
- Active tests are only possible if the user agreed up front to the opt-in mode
- Via Diagnostic Mode all scans made within a limited period of time will be linked to the user and need the opt-in mode

Making all measurements anonymous can prevent worries about being tracked by the operator, but people have to believe it. Anonymous event scans do not have an effect on the data available for pure network improvement. But there are 2 drawbacks:

- It prevents correlation with other data sources: the MSISDN is the key by which data can be matched to external sources, like for instance correlating call drop rates measured by the radio network correlated to handset OS software versions measured by the CNE app.
- It doesn't gather customer specific information that can be helpful for solving customer complaints.
- There are limits in the analysis that can be made the quality of service for a user specific application can't be monitored and analysed, e.g. download or watching a film online while travelling.

2.3.2 Description of the target state

What would it mean to apply the SPECIAL framework to the application? To a large extend, the lessons from the Generic location-based service can be directly taken into account. This chapter looks at a description of the DTAG and Motionlogic use case with SPECIAL dynamic consent implemented. How could such a use case look like?

The current system is so typical for the state of the art. At installation time, a very wide document is presented to the data subject asking for an all encompassing agreement on data collection. Because data subjects are mostly overwhelmed and given the ambient news on data harvesting, they do not trust. As a result, there is on consent. As a remedy, applications try to work with anonymous data collection. This needs the application to be installed. Again an issue of trust. Additionally, the semantic richness of such anonymized data is rather low. As people do not trust and as the application has no on/off button and no information for the user, data subjects still may feel 'tracked' despite the promise that data is anonymous. The anonymity is challenged once data is further aggregated into movement profiles like Motionlogic provides them. Remedies to this further decrease the semantic richness of the data. At the end, a lot of effort has been spent to flee data protection rules by anonymizing with a rather poor analytics result.

The SPECIAL framework will allow the CNE-APP to work differently. First, the initial consent is very basic as described in 2.1. The main task of the application is explained to the data subject before any data collection. The user agrees to the SPECIAL way of getting consent in a non-invasive way and is informed about the control interface. The promise described in 2.1 is given: Because users can control and erase the information collected, the application can be much more user friendly when collecting initial consent. While pseudonymisation may be maintained, the anonymisation could be reduced or switched on and off by the user herself. The goal is to obtain richer profiles and to reach new levels of quality for the network. Testing vehicles typically only test for signal strength and do not test the network under real use conditions. A real user using real applications running under a variety of operating systems will allow to test whether communication or data flows for applications are interrupted by network problems. This necessarily means one has to monitor a given user over a certain time across the network. This goes beyond just collecting location information and signal

strength, it also includes information as sensitive as the application used. This needs a lot of trust from the user.

Parts of the data collected could be shared with Motionlogic under the user's control. This will allow Motionlogic to provide much more accurate live information to all kinds of actors without revealing the user's identity. A good example are transport heat maps. In order to determine how streams of people are moving and in order to allow traffic planning to draw the right conclusions, an application needs to follow a given user on their way through the system. But this goes far beyond what can be done with pure anonymous aggregated data. If not aggregated heavily, data will allow the system to single out individuals showing a particular transport pattern. The more particular the pattern, the easier they can be re-identified and singled out.

In order to address the fear that insufficiently aggregated data is still dangerous and in order to remove the opacity of the data collection, the user will be put in control via the SPECIAL system. The interoperability of Linked Data will allow to not only share data between DTAG with the CNE-App and Motionlogic with their further exploitation of the data. It will also allow interoperability of the data that determines and controls the handling of the user data. This will allow the user to handle both services from one control interface, but does not exclude to have separate control interfaces for both applications if needed or wanted.

A user benefit could be that the Motionlogic application would allow the user to situate herself on a heat map. This way she can assess e.g. traffic conditions and other environmental factors to adapt her own behaviour. Such a feedback mechanism could be part of the control interface. The bet is to give more control and transparency to create trust so users will give more data to the benefit of all. Another benefit would be that Motionlogic could work with mobile services providers such as taxis to provide accurate location information in a controlled and privacy friendly way.

2.3.2.1 Controls needed

In terms of controls given to the user depend on the granularity given by the policy engine and the data collected. For the given context, policies should allow a detailed control of the type of data, period of time to store and to process data (e.g. no real-time evaluation), the range of data forwarding (scope?). Details about requirements for policies will be defined in a separate document/ deliverable.

In the present context, users' locations are probably the most precious data elements for further exploitation and (restricted) circulation. Thus, policies should allow to specify not only whether or not device locations (and at the same time user locations) are shared, but also how the location data may be used. Some possible rules that policies should cover are:

- Accuracy location (+/- x meters in longitude/latitude)
- Time stamp of location data (with certain accuracy +/- y seconds/hours)
- Delay for transfer/usage (e.g. 24 h after the position was measured, it may be used by a 3rd party)
- Duration for usage (e.g. data my be used for one week, one year, forever)
- Geo-fencing (location data may only be used inside certain areas (e.g. my home country) or only outside certain areas (e.g. restricted/military areas)
- More complex rules may also be possible, e.g. report my location only if I'm in close vicinity to n other people …

The other main component of the data set would be the technical data of the radio reception test. Here, a few rules for exploitation may be applied that concern the data subject and the primary data consumer (i.e. DT's network quality department).

A powerful policy engine and an expressive policy definition language will help to allow a fine grained control over the data collection, usage and transfer. This results potentially in rather complex mechanisms to generate/formulate, sore and apply policies. Both, the policy engine and the user are thus challenged and suitable simplifications are needed. A layered approach will allow simple users of the application to have packaged policies they can select from. But it is not excluded to allow expert users to have their own set of rules and to offer them to simple users. Those expert users will be the prime source of trust for the broader range of people with less skills.

So far, the applications are concentrated on live information. One of the benefits of Big Data is that information is kept and routed into the data lake. Fishing the data lake will reveal unknown benefits. In order to fish the data lake, not only the purpose limitation is a challenge. In fact having accurate profiles going back a long time may create very creepy experiences for data subjects. Those are the very reason data protection legislation started back in the seventies. A good data retention policy may want to involve the user interactively. The challenge is also to get people to agree to purpose changes. But with the innovative easy consent mechanism that SPECIAL introduces, this may create a nice feedback loop without overwhelming the user.

The legal analysis in this Deliverable will concentrate on the assessment of the target state of the application and mainly focus on GDPR.

2.3.2.2 Description of DTAG's anticipated benefits for all sides

To make a user download and use an app and even more to consent obtaining the data from a variety of users, a specific benefit has to be presented to our potential customers in the addressed segment. The DT CNE application offers measurement of connection-quality. Since the application is downloadable at no cost and no data volume is charged for the use. Potentially, the user could also be able to connect to Telekom Hotspots in case one (hotspot) is detected in the nearby area. As a result, the user measures his connection quality, non-anonymized data is acquired in exchange and the user is able to keep his data volume in certain locations untouched.

Considering the fact that Telekom runs an official application for its sales and distribution channel, a fusion of apps might be beneficial for both the user-base and us a company (combining the CNE app for quality measurements and the Hotspot-connector app for free DTAG WiFi). Since geo-data is required for suggestions of near Telekom hotspot anyway, the user will be more open to allow the acquisition of data since it's a lot more transparent what is supposed to happen with this information. The intent is to maximize usability and customer-friendliness, since it's easier to use an all-in-one solution than using different apps for each functionality. DTAG are in discussion with responsible authorities/departments within Deutsche Telekom to confirm a possible a merge of both applications. Technical, organizational or business aspects may inhibit this merge of apps.

Nevertheless even the current CNE app and the data gained herein have been rated highly valuable for the intended new user Motionlogic. Thus the use case is ascertained by DTAG as being not only plausible, but really commercially valid.

2.3.3 Installation and Subscription

As for all other cases of mobile and location based services, during the installation of the CNE-APP a number of agreements has to be gathered. The type of process to walk through will not change, even if the CNE-APP will be combined with a Hotspot-connector app for free DTAG WiFi. This would be done by the data subject, who would typically be a DTAG customer. One could imagine that in the case of Motionlogic services, other people than DTAG customers would want to install the App. For them, the procedure may involve entering more information as data points can't be taken from the customer record. In general, a data subject should be given the option to either take over their customer data or to enter a pseudonymous identity. Otherwise, a phone subscription by a company

e.g. would not allow an individual to make individual choices. Furthermore, the GDPR encourages the use of pseudonyms.

In the following, suggestions are made to illustrate how the SPECIAL layered approach can help to convey the right information at the right time to the data subject. This takes into account the minimum information that must be given to the data subject upon when triggering a service. First and foremost, the installation introduces the overall goal of the application. This may start with a text offering the network quality measurement service, whereas the added user benefits can eventually be advertised as well directly at the beginning:

> '*Help us improve our network quality! Depending on the information you share with us from your mobile, you may get even free access to our Hotspots, or temporarily free charge of your data volume!*'

The new approach in SPECIAL already shown in the other use cases means that only the very minimal consent is gathered upon installation of the application. At the same time, consent for the layered approach and the passive agreement procedure is gathered. Which allows to collect contextual consent in a layered approach while the application is running and in a certain state and context. This sounds abstract. It describes the fact that the SPECIAL application is able to react on a consent request in a given context. The data subject is conscious about this context and can easily assess the consequences of giving consent, even though the description is minimal.

> '*The CNE-APP will ask you in context before collecting any further information. This will build a set of permissions over time. You can control all permissions in your control interface'*.

If the CNE-APP is directly bundled with the Motionlogic system, which is a choice to make, this has to be taken into account at the point of installation too. The relaxed requirements for explicit consent in the SPECIAL system being earned by the contextual messages and the control-interface by the dashboard, it is clear that adding a third party goes beyond the scope that can be covered by those relaxed requirements. If the CNE-APP also carries Motionlogic functionality and data sharing, this has to be taken into account in the installation procedure. In this case, an additional point is needed informing the user about the Motionlogic features, even if those are later integrated seamlessly into the user's dashboard. The message could look like the following:

> '*Under your control, the CNE-APP is able to share data with Motionlogic to provide useful data for traffic planning, statistics and other useful aggregation. You may, in a unified interface, subscribe and control additional services from Motionlogic'*

This freely suggested wording assumes that the CNE-APP will send identified or pseudonymised data to DTAG and that DTAG will share this data in some way with Motionlogic. This also assumes a contractual relationship between DTAG and Motionlogic which will either make them joint data controllers or a data controller and processor relation between Motionlogic and DTAG, respectively.

It may be of good practice to offer several options to the data subject. Those options could include:

- *'I want to use Motionlogic services and see how many people are doing the same thing I do, please integrate them into my control interface'*
- *'Data is shared with a reduced pseudonymous data. This would allow Motionlogic to create statistics like heat maps.'*
- *'Only anonymised data is shared with third parties'*
- *'Go away! I do not want you to share data for traffic improvement. No data will be shared.'*

From this point, it is not excluded that other services are added later using SPECIAL consent mechanism. It has to be noted though that it is highly questionable whether this can be done using the implicit mechanism of the shade that goes away after some time and assumes *'Yes'*. Legally, the more secure ground would be to have an explicit reaction of the user when adding a third party. This

could be an interactive screen that could look similar to the screen used to get the first general consent during installation.

From this first layer, there should be a link to deeper layers. The challenge is here as well to determine which information needs to be given in which layer during the interaction with the user as the data subject.

According to the Article 29 Working Party, the data subject should also get informed '*[…] where/ how they can find that detailed information within the layers of the privacy statement/notice. It is important that the information contained within the different layers of a layered notice is consistent and that the layers do not provide conflicting information.*'[53] Moreover, according to the Article 29 Working Party, the first layer should '*always contain information on the processing which has the most impact on the data subject and processing which could surprise the data subject.*'[54]

Therefore, the following list suggests further information once the data subject drills down to further layers. The second layer will have to provide information about the purposes of the processing, the data categories initially collected, that no costs are attached, and about the sharing of that information with Motionlogic, inclusive a link e.g. to a webpage + dashboard with further detail information.

In this second layer, the following information should be provided:

- If the user has opted for the full identification, the data points that will be taken from the DTAG subscription should be presented in case the data subject drills down
- If the data subject has opted to use a pseudonym, the system must drill down automatically and offer to enter the necessary data points.
- If the data subject has opted for the anonymised sharing, information about anonymisation techniques should be given although this is not legally required. This option would allow to have weaker anonymisation that is still 'good enough'.
- If the data subject has opted not to share anything and drills down, there could be an explanation that still data necessary for her communications are collected and processed. Only legally compliant anonymisation will satisfy further use here.

Whatever the option, the data subject should be informed on the second layer:

- The option to withdraw consent and to control and manage the collected and processed data via a dashboard.
- that the app has an 'incognito mode' in the app to temporarily interrupt the sharing of the personal data without completely unsubscribing to the service (called 'Not now' button)
- **assume implicit conditional consent** for the (temporal) sharing of personal data while at any other time only anonymized data will be shared with Motionlogic.
    - This goes along with notifying the user whenever the identified or pseudonymous sharing happens by a shade appearing briefly on the screen on the mobile.
    - The data subject can during installation set the preference similarly like '*Share personal data unless I react/disagree within […] seconds/minutes during the display of the notification*'. Ideally, the data subject is even given the option to pre-set how long this shade is displayed on the mobile. Make clear that for sensitive information, the app will still always ask for explicit consent.

[53] Cf. '*Guidelines on transparency under Regulation 2016/679*', WP260, page 17.

[54] Ibid. page 17.

- Again, the information must be given that it is at any time possible to withdraw generally or even partially consent to the processing of the given information other than by uninstalling or deactivating the app.
- Be clear that partial withdrawal of consent is possible, e.g. only for sharing personal data, but still sharing anonymized information for the network quality measurement.

At any time during the installation process, the data subject should be provided with the following options to control the installation process:

- '*Back*' or '*Abort*' button.
- '*Forward*' or '*Continue*' button.
- Clickable link to more information. This is similarly to the '*Know more*' button suggestions in the Proximus use case, whereas reference is made to the initial text suggestions made in section 2.2.2.. It is important that the data subject there gets the more in-depth information about the processing according to Art. 13/14 GDPR, such as the controller and processor identities, data storage period, the relevant DT (or additionally even Motionlogic) Privacy Policy website, and so forth.

The layered approach during the installation may be extended if other features are added to the Application, especially if sharing is conditional upon logging into a DTAG Hotspot as a benefit. It is also clear that sensitive information as mentioned in Art. 9 GDPR will need an explicit active affirmative action from the data subject. The more sensitive the context is, the more burdensome the requirements for an active reaction, including provision of comprehensive information.

Another option is to ask upfront for the consent for specific data categories. This means the pre-setting of consent under certain conditions (such as being near a hotspot). DTAG may also come up with other consent conditions that might be beneficial for the user, which is something that can be discussed in the project.

By asking upfront how the app should behave and how consent should be handled, a clear affirmative action or statement in the sense of the GDPR is given by the data subject. Such an action or statement are being executed via electronic means, which is also possible according to the GDPR. The same goes for choosing technical settings for information society services.[55] Moreover, this approach to the DTAG use case creates not only synergies with the Proximus use case, but would also comply with Articles 8 and 9 of the draft ePrivacy Regulation in its current Parliament version.

2.3.4 Enriching the profile

During the installation process, the information given was very basic. This is done because it is very hard to convey information to users about a system they will use in the future. In the installation process the data subject has given basic information and agreed to the contextual consent mechanism and to the relaxed requirements for consent in case no sensitive information is given.

Once the application starts running, the data subject is in a certain context. Within that context, the data subject will better understand the collection, its causes, benefits, purposes etc. There is a thing specific to the DTAG use case, which is that it constantly gathers data while in the Proximus use case a punctual collection of location information is used to augment the profile and match the event data base. Having constant location collection, for network quality as well as for the movement profile requires well defined conditions. In fact Art. 9 of Directive 2002/58EC already ruled that '*Users or subscribers shall be given the possibility to withdraw their consent for the processing of location data*

[55] D1.2 *Legal requirements for a privacy-enhancing Big Data V1*, chapter 2.2, section 2.2.5 (c), page 29.

other than traffic data at any time.' Art. 9 also requires that a data subject has the option to temporarily suspend the collection of location information. This is only possible of the CNE-App is visible in the status bar of the mobile device. Most mobile devices already show a symbol if the GPS is active. A similar indication should be shown if the CNE-App collects location information. If location information is shared with Motionlogic, the symbol could change color e.g. Tapping or otherwise interacting with the symbol should then open the dashboard for the CNE-App with appropriate controls, including:

- A switch to temporarily switch off the data collection while the app keeps running
- A switch to start or stop the data sharing with Motionlogic
- A link to a layered control – interface that allows to erase historic data

To not drain the battery, we may imagine that the device will only start monitoring once the network quality measured inside the device goes below a certain threshold. In this case, a shade would be shown for some time to indicate that the monitoring starts again.

The dashboard in layer 2 behind the indication of activity of the app in the default screen, the information required by Art. 13 and 14 GDPR has to be provided. It can be summarized with a link to a layer 3 within the dashboard.

If e.g. the CNE-App has chosen to have free Hotspot connections included or if the App only becomes active near DTAG Hotspots, such notifications can be done behind a half-transparent shade on the screen of the user's mobile device. This could be done e.g. whenever the data subject is near a DTAG Hotspot, or once a month when a new billing period has started, so the consent request can be advertised with the corresponding user benefits. An idea for a text requesting this consent could be as follows:

> '*You are near a hotspot area! Use it for free and allow us in exchange to share your [specify categories of personal information] with Motionlogic for [name purpose(s)]? [Yes/Only as long as I am near the hotspot/Not now/Learn more]*'

Alternatively, the text could be like this:

> '*Benefit from free [or reduced] data volume charges! Allow us in exchange to share your [specify categories of personal information] with Motionlogic for [name purpose(s)]? [Yes/Yes, but only this month [or any other billing period this user has]/Not now/Learn more]*'

The suggested texts may be shortened by further UI design work in Workpackage 4 and include further layers to include all information necessary. The detail of the content needed for notification can only be determined later in the process once the implementation decisions have matured.

Depending on the options chosen during install, the reaction on the shade may range from the user clicking '*Yes*' to allow personal information sharing with Motionlogic to options like '*Only as long as I am near the hotspot*' or ' *Yes, but only this month*'. The backend would react on such choices and sharing would only affect the time frame when the user is near this hotspot, or as long as the current billing period lasts.

Has the user clicked '*Not now*', no consent can be assumed at all.

If the '*Learn more*' button is clicked, the user would be directed to a subsequent site (layer) that provides more detail information about the processing, including further access to the relevant DT/Motionlogic privacy policies. How this could happen is explained in detail after the second use choice case below.

The mentioned layer from the messages could be triggered by '*Learn more*'. In this case, a link takes the data subject to further information going more into detail about the intended data processing

and makes all information accessible, depending on whether compliance with Article 13 + 14 GDPR is needed.[56] This could be something like the following exemplary text:

> *This application is provided to you by [name controller(s), depending on whether only DTAG is controller or whether a DTAG/Motionlogic joint controllership is envisaged] with its headquarters at [valid address]. If you have any questions, please contact our representative [name] under [email and/or postal address, preferably both]. If you have questions about the collection or use of your data, please contact our company-internal data protection officer [name] under [email and/or postal address, preferably both].*
>
> *If consent is given, the following categories of personal data will be is collected following Article 6 para. 1 (b) GDPR: [specify]*
>
> *You are about to give, or you have already given your agreement to the collection of [reference above specified personal data] and to the creation of a user profile of you for [specify purpose(s)].*
>
> *Your data remains within the European Union and we do not give your data to third parties except Motionlogic.*
>
> *[Describe the relationship between DT + Motionlogic, making clear who is controller and who is processor. If Motionlogic is processor, make clear that they are bound by instructions from DT.]*
>
> *[Describe further in detail the processing by Motionlogic, the corresponding purpose(s), the retention period and so forth.]*
>
> *We will store your data and the history of recommended events until you uninstall this application, erase your profile[57], or until you selectively delete some information via the control interface of this application that can be found <here> [provide link to dashboard].*
>
> *The profile created serves to know you better and to determine your interests according to [name processing purpose(s) and why the data is necessary].*
>
> *The dashboard control interface will provide you with the possibility to access, erase and rectify your data. In case you find a competing app that you like more, you can export the data as standardised RDF Linked Data format.*
>
> *You can generally or selectively withdraw your consent any time. If you don't want to have personal data shared with Motionlogic anymore, please delete the permission for that sharing in your control interface.*
>
> *If you have agreed to allow the assumption of your implicit conditional consent once you are in a hotspot area, we will share your personal information as long as you are within area of this hotspot, and as long as the application is active.*
>
> *Your data is kept for [specify…] days. You can also use an 'incognito mode' which stops the data collection. This can be done either using the 'Not now' button directly within the application, or when this option is given during our consent requests and notifications.*
>
> *For more information see our privacy policy at [direct URL link to the relevant full privacy policy of the controller organisation + processor]*

[56] For details about the required notifications, see D1.2, chapter 2.2.6, section (b), page 31.

[57] This is the option for websites.

The above suggestions are only there to give a preliminary idea about who things could look like in the layered approach. They must be further refined with the iterations within the SPECIAL agile process.

2.3.5 Additional options for user control

Because of the time lapse, the DTAG use case is not fully assessed yet and needs more precision. There are a variety of options that can be given to the data subject. Most importantly it has to be noted that the Article 29 working Party has acknowledged a layered approach as a possible solution to avoid 'consent-fatigue' of a data subject, yet still provide all necessary information step by step. The condition to facilitate this is to provide balancing means of user control, so the first layer of information does not need to be completely in-depth about the details of the processing.

The challenge is not only a legal one. By involving another data controller, the DTAG use case also raises interoperability challenges concerning agreements, consent and restrictions. Consent and constraints may be collected by the user interface of the DTAG customer, our data subject. But the permissions involve a well determined third party, Motionlogic, that also provides location based services. The attributes needed and shared in this context need further elucidation. A number of options seems possible if Motionlogic offers something back to the user and if it is only to show them their own context in a heat map. It may also be possible to apply a certain number of innovative privacy preserving practices here, e.g. by splitting tables so that only DTAG gets the full picture and Motionlogic has only the data they need, e.g. that the person in point A at time 1 and point B at time 2 are the same person.

2.3.6 Challenges ahead

So additionally to the information that must be given according to the GDPR[58], this dashboard needs to provide certain functionalities of user control. Given that there is a third party involved, the dashboard needs to cover two service providers and data controllers at the same time. The dashboard, once drilled down to the very and should contain at least:

- Clear and easy to understand overview of available information
    - For example for the data collected, processed and shared, information who is controller and who processor, contact information, data protection officer contact, eventual cross-border transfers, location of storage, retention period.
    - This includes the possibility to drill down even further, e.g. to the specific privacy policies of DTAG and Motionlogic.

The user interface will certainly have the following challenges, if such option is made available:

- Managing consent in a fine-grained way
    - Such as partial granting or withdrawal of consent being possible, e.g. by switching back and forth between anonymous or personal data sharing with Motionlogic.
    - Such as switching back and forth between different consent modalities, e.g. between always requiring explicit consent for personal data sharing in certain situations or choosing convenient assumption of implicit consent whenever near a hotspot, so it can be used for free.
- Managing the own data in an easy way

[58] See D1.2 section 2.2.6 for details about transparency and information obligations towards the data subject.

- E.g. add, delete, rectify personal data.

- Exporting the own personal information
  - Article 20 GDPR requires data portability, so this can be done e.g. by providing an export in an RDF format.
- Optionally: Possibility to access additional information in case of a data breach

Within the SPECIAL project, the partners responsible for the UI design have drafted initial ideas for a user dashboard that already provides a visual interface capable of integrating these functionalities rather easily. Since it was decided in the project to produce an additional and internal UI-focused deliverable which is currently in the making, this will be the basis for further discussions on how to optimally facility the above mentioned user control features.

From the use case description, it is not yet fully clear which attributes will be shared with Motionlogic, depending on whether anonymous data sharing or personal data sharing is allowed. A full assessment has to be done before further details can be determined in the legal messaging.

It is also not fully clear yet which purposes will be pursued. This may be a rather generic purpose. But given that location data is rather sensitive, the purpose specification can not be too broad. Which in turn raises the question on how to organise the consent for additional purposes once the data is collected. As this is a typical big data privacy challenge, the DTAG use case provides an ideal ground for further research. It will depend on how far the results by Motionlogic can still be traced back to the individual, whether there are additional location based services attached to the data collection and how the legal relation between DTAG and Motionlogic is organised.

3 Conclusions

The increasing use of digital information and communication services by European citizens leads to an also increasing dependency on these technologies. Yet, this often goes along with a significant loss of transparency and control over their personal information, which is collected and processed by organisations. This is a conflict emerging repeatedly and globally, which has led to intense societal, legal and regulatory debates over the past decades in which way citizen's fundamental rights, especially with regard to their rights to privacy and data protection may be better protected. An example is Germany, where such concepts were further developed by differing between the concept of privacy and the concept of information control.[59] This has led to the famous Census judgement of the German Federal Constitutional Court in 1983, manifesting the principle of the informational self-determination (translated: '*Informationelle Selbstbestimmung*') as a constitutional right by itself. However, informational self-determination is not just a characteristic of the German data protection framework. Rather, it was addressed by legislators on European level, which has ultimately led to the reform of the European data protection framework and the GDPR, which is applicable by May 25th 2018. This regulatory instrument will affect all industries wanting to do business in Europe and intend to do so while collecting and processing the personal information of EU citizens.[60] Moreover, the EU legislators are currently working on the ePrivacy Regulation, which is anticipated to be relevant for providers of Over-The-Top (OTT) services in addition to traditional telecom operators. This regulation is currently in the Trilogue between EU Commission, Parliament and Council, whereas in this deliverable, we refer to the latest official version of the Parliament, with its suggested changes to the original proposal from the Commission. Both legal frameworks impose constraints on Big Data businesses due to their objective of protecting individual's fundamental rights, especially their rights to privacy and data protection.

SPECIAL aims at finding way how to work within these constraints of the GDPR, enabling data protection friendly technologies for Big Data businesses respecting their customers as data subjects. But the project also aims at finding ways how to reconcile this objective with the commercial interests of organisations. So the question in the research context of the SPECIAL project is how to facilitate informed, free and valid consent of data subjects in the digital age and to give them sufficient control over their personal information in order to build and maintain trustful customer relationships also to the benefit of private companies.

In D1.2, an identification and analysis of the general data protection requirements deriving from the GDPR and from the expected ePrivacy Regulation (which is still in the legislative process) was conducted. Moreover, an initial first analysis of the project's foreseen use cases has been done.

This deliverable however, has delved deeper into the factual issues of the individual use cases with the objective to find out in which ways the technologies researched and developed within SPECIAL may contribute to a data protection compliant realization of these use cases. Therein it is guided not only by the explicit legal requirements, but also by the considerations of the EU legislators addressing the legal harmonization and the fundamental rights of EU citizens.[61] Moreover, instead of a classical

[59] For the conjunction between the definitions of privacy and identity, see Rannenberg, K.; Royer, D.; Deuker, A. (ed.): '*The Future of Identity in Information Society - Challenges and Opportunities*', pages 292 ff. (section 7.3: '*When Idem meets Ipse: The Identity of the European Citizen*').

[60] See for the details on the GDPR's material and territorial application scope D1.2, chapter 2.2.1, pages 12 ff.

[61] Cf. COM (2012) 9 final, titled '*Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century*'.

legal analysis, it follows a more practical approach addressing the uses cases in such a way that deems optimal for their realization within the scope of SPECIAL.

Therefore, this deliverable has differing strategies to address the project's use cases throughout the document.

For the use cases of the industry partners Proximus and DTAG, rather exemplary suggestions were made aligned to rather concrete steps of the personal data processing operations intended. This was made on the basis of a rather generic location-based service as an implementation example. This example is meant to make suggestions how the Prox and DTAG use cases could be specified, and where needed, adapted to be realized in an optimally GDPR compliant way. Moreover, this generic example for LBS is detailed to show the applicability of the suggested approach to a variety of industry services using information technology services. Subsequently, the Proximus use case was then addressed specifically, therein giving tips in which ways the data subjects of the recommendation service intended as use case may be informed and how valid consent in the sense of the GDPR and in line with probable provisions of the future ePrivacy Regulation may be collected from them. Unfortunately, at the time of the submission of this deliverable, industry partner DTAG was not yet able to provide their adapted use case to the project. Project-internally, it is known that it may foreseeably address a network measurement app using location data of mobile users, but a detailed description is not yet available. However, it was promised that this description will follow soon, so once this is available, this deliverable will be updated and the use case integrated. Regardless of the specific of this use case, the generic LBS example has already shown that a layered approach and contextually embedded consent requests relying on technical setting of the user's device provide for a practical and still data protection compliant approach to obtain valid and informed consent from the data subjects. Therein, this approach may provide in future a way to ease the dichotomy between the interests of Big Data businesses and the informational self-determination of individuals within the context of the European data protection framework.

As an outlook to the further work in the project, it is noted that the legal requirements for the acquisition of informed, valid consent for the Prox and DTAG use cases are relatively clear, yet their practical implementation will be subject for further discussion in the project.

4 References

Note: URL addresses listed in the references section to point to the respective document sources originate from those which could be found on the Internet at the time of writing this report, i. e. were valid links at the appointed date of 29 March 2018. No guarantee is given that those URLs still function at the time of any recipient reading this document.

4.1 Legislation, European case law and policy documents

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

OJ L 281, 23.11.1995, p. 31-50

Available at:

http://eur-lex.europa.eu/eli/dir/1995/46/oj

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

Abbreviated as 4AMLD

OJ L 141, 5.6.2015, p. 73-117

Available at:

http://eur-lex.europa.eu/eli/dir/2015/849/oj

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Abbreviated as GDPR

OJ L 119, 4.5.2016, p. 1–88

Available at:

http://eur-lex.europa.eu/eli/reg/2016/679/oj

European Court of Human Rights

Judgement of the Court (Plenary) of 7 December 1976

Handyside v. The United Kingdom

Application no. 5493/72

Available at:

https://hudoc.echr.coe.int/eng#{%22dmdocnumber%22:[%22695376%22],%22itemid%22:[%22001-57499%22]}

European Court of Human Rights

Judgement of the Court (Plenary) of 6 November 1980

The Sunday Times v. The United Kingdom

Application no. 538/74

Available at:

https://www.eui.eu/Projects/CentreForJudicialCooperation/Documents/2011-10-28-29/ECtHRSundayTimesvUK.pdf

European Court of Human Rights

Third Section Decision as to the Admissibility of

Jan Herman Brinks vs The Netherlands

Application no. 9940/04
5 April 2005

Available at:

http://hudoc.echr.coe.int/eng?i=001-68816

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber)

Kadi and Al Barakaat International Foundation v Council and Commission

C-402/05 P and C-415/05 P of 3 September 2008

Available at:

http://curia.europa.eu/juris/liste.jsf?num=C-402/05&language=en

European Court of Human Rights

Judgement of the Court (Grand Chamber) of 4 December 2008

S & Marper v. United Kingdom

Applications nos. 30562/04 and 30566/04

Available at:

http://www.bailii.org/eu/cases/ECHR/2008/1581.html

Court of Justice of the European Union (CJEU)

Judgement of the Court (Third Chamber) of 24 November 2011

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) v Administración del Estado

Joined cases C-468/10 and C-469/10

Available at:

http://curia.europa.eu/juris/liste.jsf?num=C-468/10&language=en

Court of Justice of the European Union (CJEU)

Judgement of the Court (Third Chamber) of 15 November 2012

Al-Aqsa v Council

C-550/10 P

Available at:

http://curia.europa.eu/juris/liste.jsf?num=C-539/10&language=EN

Court of Justice of the European Union (CJEU)

Judgement of the Court (Third Chamber) of 25 April 2013

Jyske Bank Gibraltar Ltd v Administración del Estado

C-212/11

Available at:

http://curia.europa.eu/juris/liste.jsf?num=C-212/11&language=EN

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber) of 8 April 2014

Digital Rights Ireland

Joined Cases C-293/12 and C-594/12

Available at:

http://curia.europa.eu/juris/liste.jsf?num=293/12&language=en

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber) of 13 May 2014

Google Spain SL, Google Inc. v Agencia Española de Protección de Datos (AEPD), Mario Costeja González

C-131/12

Available at:

http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=EN

Census court decision of the German Federal Constitutional Court

(In German: Volkszählungsurteil Bundesverfassungsgericht)

15th December 1983

Az.: 1 BvR 209, 269, 362, 420, 440, 484/83

Available at:

https://freiheitsfoo.de/census-act/

Communication from the Commission to the European Parliament and the Council

Communication on further measures to enhance transparency and the fight against tax evasion and avoidance

Strasbourg, 5.7.2016

COM(2016) 451 final

Available at:

https://ec.europa.eu/transparency/regdoc/rep/1/2016/EN/1-2016-451-EN-F1-1.PDF

European Data Protection Supervisor

EDPS Opinion on a Commission Proposal amending Directive (EU) 2015/849 and Directive 2009/101/EC Access to beneficial ownership information and data protection implications

Opinion 1/2017 of 2 February

Available at:

https://edps.europa.eu/sites/edp/files/publication/17-02-02_opinion_aml_en.pdf

UK Financial Conduct Authority

'*FG 17/6 The treatment of politically exposed persons for anti-money laundering purposes*'

Finalised guidance July 2017

Available at:

https://www.fca.org.uk/publication/finalised-guidance/fg17-06.pdf

UK Information Commissioner's Office (ICO)

The Information Commissioner's Office (ICO) response to HM Treasury's consultation on Money Laundering Regulations 2017 ('the consultation')

12.04.2017 Version 1.0 (Final)

Available at:

https://ico.org.uk/about-the-ico/consultations/hm-treasury-consultation-money-laundering-regulations-2017/

Draft UK Data Protection Bill [HL] 2017-19

Available at:

https://publications.parliament.uk/pa/bills/cbill/2017-2019/0153/18153.pdf

92. Conference of the Independent Data Protection Authorities of the Bund and the Länder in Kühlungsborn

'*The Standard Data Protection Model – A concept for inspection and consultation on the basis of unified protection goals*'

V.1.0 – Trial version 9-10 November 2016

Initial English version available at:

https://www.datenschutzzentrum.de/sdm/ (improved English version currently in progress)

'*Guidance on the Management of Police information*'

Second Edition 2010

Available on the website of the UK West Midlands Police at:

https://www.west-midlands.police.uk/advice-centre/accessing-information/data-protection/index.aspx

4.2 Article 29 Working Party documents

'*Guidelines on transparency under Regulation 2016/679*'

WP260, adopted, but not yet finalised

Available at:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615250

'*Guidelines on Consent under Regulation 2016/679*'

WP259, adopted on 28 November 2017, but not yet finalised

Available at:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=615239

'*Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*'

WP 251rev.01, adopted 3 October 2017, last revised and adopted 6 February 2018

Available at:

http://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49826

'*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*'

WP248 rev.01, adopted on 4 April 2017 as last revised and adopted on 4 October 2017

Available at:

http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

'*Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*'

WP 211, adopted on 27 February 2014

Available at:

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

'*Opinion 03/2013 on purpose limitation*'

WP203, adopted on 2 April 2013

Available at:

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

'*Opinion 15/2011 on the definition of consent*'

WP187, adopted on 13 July 2011

Available at:

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

'*Opinion 1/2010 on the concepts of "controller" and "processor"*'

WP 169, adopted on 16 February 2010

Available at:

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf

4.3 Academic and other sources

Alexy, R.

'*Constitutional Rights, Balancing, and Rationality*'

Ratio Juris Volume 16, Issue 2 (2003), pages 131-140

Alexy, R.

'*Constitutional Rights and Proportionality*'

Issue 2014/22 Revus Journal for Constitutional Theory and Philosophy of Law

Available at:

http://journals.openedition.org/revus/2783

Bremert, B.; Robrahn, R.

'*Die Rechtfertigung der Verarbeitung personenbezogener Daten über eine Abwägung nach Art. 6 Abs. 1 lit. f DSGVO*'

(translated: '*The legitimisation of the processing of personal data via a weighting according to Art. 6 para. 1 (f) GDPR*')

Essay foreseen to be published in the NJW (Neue Juristische Wochenschrift) in early 2018

Engeler, M.

'*Das überschätzte Kopplungsverbot*'

(translated: '*The overestimated prohibition of coupling*')

ZD Issue 2/2018, pages 55-62

English Oxford Living Dictionaries

For the word definition of the term 'legitimate'

Available at:

https://en.oxforddictionaries.com/definition/legitimate

Ehmann/Selmayr (ed.)

'*Datenschutz-Grundverordnung*'

(translated: '*General Data Protection Regulation*')

Abbreviated in this document only as Ehmann/Selmayr (ed.)

Beck'sche Kurz-kommentare

1st Edition 2017

C.H. Beck Publishing House, Munich 2017

Gola (ed.)

'*DS-GVO Datenschutz-Grundverordnung VO (EU) 2016/679 Kommentar*'

(translated: '*GDPR General Data Protection Regulation R (EU) 2016/679 commentary*')

Abbreviated in this document only as Gola (ed.)

C.H. Beck Publishing House, Munich 2017

Herrmann, M, Hildebrandt, M, Tielemans L. Diaz, C

'*Privacy in Location – Based Services: An Interdisciplinary Approach*'

Script*ed* Volume 13, Issue 2, (2016)

Available at:

https://securewww.esat.kuleuven.be/cosic/publications/article-2725.pdf

Hildebrandt, M.

'*Technology and the end of law*'

Heidelberg Facing the limits of the law (2009)

Available at:

http://works.bepress.com/mireille_hildebrandt/16/

Hildebrandt, M.,

'Slaves to Big Data. Or Are We?'

17 IDP. REVISTA DE INTERNET, DERECHO Y POLÍTICA 2013, 7-44

Available at:

https://works.bepress.com/mireille_hildebrandt/52/

Hildebrandt, M.

'*The Philosophy of Law Meets the Philosophy of Technology*'

In: Law, Human Agency and Autonomic Computing

Routledge (2013)

Kühling, J.; Buchner, B. (ed.)

'*Datenschutzgrundverordnung – Kommentar*'

(translated: '*General Data Protection Regulation – Commentary*')

Abbreviated in this document only as Kühling, J.; Buchner, B. (ed.)

C.H. Beck Publishing House, Munich 2017

Leenes, R., Van den Berg, B., Potzsch, S., Pekarek, M., Roosendaal, A., Kuczerawy, A., Borcea-Pfitzmann, K., Neato, F.

'Privacy Enabled Communities' (2010)

Available at:

http://primelife.ercim.eu/images/stories/deliverables/d1.2.1-10.04.23-privacy_enabled_communities-public.pdf

Lutterbeck, Bernd, Sokol, Bettina (ed.)

'20 Jahre Dauerkonflikt: Die Novellierung des Bundesdatenschutzgesetzes' in: 20 Jahre Datenschutz - Individualismus oder Gemeinschaftssinn?

(translated: 20 Years of Data Protection – Individualism or Commons?

ISSN: 0179-2431, Düsseldorf 1998

McDonald, A. M., Cranor, L. F.

'*The Cost of Reading Privacy Policies*'

ISJLP 4, 543-897 (2009)

Available at:

https://kb.osu.edu/dspace/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf

Narayanan, A., Shmatikov, V.

'Robust de-anonymization of large sparse datasets'

SP 2008. IEEE Symposium on Security and Privacy, 111–125

DOI: 10.1109/SP.2008.33

ISBN: 978-0-7695-3168-7

Available at:

http://www.profsandhu.com/cs6393_s13/ns_2008.pdf

Nissenbaum, H. F.

'*Privacy as Contextual Integrity*'

Washington Law Review 79(1) (2004)

Nissenbaum, H. F.

'*Privacy in Context: Technology, Policy, and the Integrity of Social Life*'

Stanford University Press, Palo Alto 2009.

Paal/Pauly (ed.)

'Datenschutz-Grundverordnung Bundesdatenschutzgesetz'

(translated: '*General Data Protection Regulation Federal Data Protection Act*')

Abbreviated in this document only as Paal/Pauly (ed.)

Beck'sche Kompakt-Kommentare

2nd Edition

C.H. Beck Publishing House, Munich 2018

Penney, J.

'Chilling Effects: Online Surveillance and Wikipedia Use'

Berkeley Technology Law Journal

Vol. 31, No. 1, p. 117, 2016

Available at:

https://ssrn.com/abstract=2769645

Rannenberg, K.; Royer, D.; Deuker A. (ed.)

'*The Future of Identity in Information Society - Challenges and Opportunities*'

1st Edition 2009

Springer Publishing House Berlin Heidelberg

Simitis, Spiros

'Reicht unser Datenschutzrecht angesichts der technischen Revolution? - Strategien zur Wahrung der Freiheitsrechte' in Staatskanzlei von Hessen (Hrsg.): Informationsgesellschaft oder Überwachungsstaat. Protokoll des Symposiums der Hessischen Landesregierung. Wiesbaden 1984, S. 27 ff.

Wiesbaden 1984

Tague, Nancy R.

'*The Quality Toolbox*'

Second Edition, ASQ Quality Press, 2005

ISBN: 978-0-87389-639-9

4.4 SPECIAL deliverables, reports and other reference documents

D1.1 - SPECIAL Deliverable

Use case scenarios V1

Participants:

P.A. Bonatti, J. Colbeck, F. De Meersman, R. Jacob, S. Kirrane, M. Kurze, M. Piekarska,

R. Wenning, B. Whittam-Smith, H. Zwingelberg, E. Schlehahn

D1.2 - SPECIAL Deliverable

Legal requirements for a privacy-enhancing Big Data V1

Authors:

H. Zwingelberg, E. Schlehahn

D1.3

Policy, transparency and compliance guidelines V1

Authors:

P. A. Bonatti, S. Kirrane, R. Wenning

D1.4 - SPECIAL deliverable

Technical Requirements V1

Author:

Bert Van Nuffelen

D1.5 - SPECIAL Deliverable

Use case scenarios V2

Authors:

P.A. Bonatti, J. Colbeck, F. De Meersman, R. Jacob, S. Kirrane, M. Kurze, M. Piekarska, R. Wenning, B. Whittam-Smith, H. Zwingelberg, E. Schlehahn, L. Sauro

D8.1 – SPECIAL deliverable

H - (Ethics) Requirement No. 2

Author:

Rigo Wenning

5 List of illustrations

Illustration Index

6 List of acronyms and abbreviations

AML	Anti-Money-Laundering
AMLD	Anti-Money-Laundering Directive
4AMLD	Fourth Anti-Money-Laundering Directive
5AMLD	Fifth Anti-Money-Laundering Directive
CFR	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CTF	Counter-Terrorism-Financing
DPIA	Data Protection Impact Assessment
DTAG	Deutsche Telekom AG
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ePR	ePrivacy Regulation
EU	European Union
FATF	Financial Action Task Force
GDPR	General Data Protection Regulation
LBS	Location-based service
LIBE committee	Committee on Civil Liberties, Justice and Home Affairs
OJ	Official Journal of the European Communities
OJ L […]	Official Journal of the European Communities – Legislation
OJ C […]	Official Journal of the European Communities – Information and notices
PEP	Politically Exposed Person
PETs	Privacy Enhancing Technologies
Rec	Recommendation
SMO	Senior Management Official

TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TR	Thomson Reuters
UBO	Ultimate Beneficial Owner
WTO	World Trade Organisation