D3.10

Fundamental Rights Protection by Design for Online Social Networks – v3: Update of Deliverable 3.6

v 1.0 / 2015-05-19

Katja de Vries, Niels van Dijk, Sari Depreeuw and Mireille Hildebrandt (iCIS-RU).

The USEMP project has developed a web application called DataBait. DataBait is a transparency tool that empowers online social network (OSN) users by supporting them in exercizing their fundamental rights in the context of behavioural tracking and personalized advertising. This document shows that DataBait can function as an exemplary case of succesful Data Protection by Design (DPbD). DataBait's architecture and design aim for full compliance with all relevant European fundamental rights as well as to maximize supportive empowerment of OSN users in the exercise of their informational rights with regard to their digital trail created by the use of OSNs and browsers. This document does not only provide an overview of design implications for DataBait based on the legal research on the relevant fundamental rights protection, but also can offer a wealth of useful information for other developers of transparency tools or policy makers engaged with user empowerment in online environments.

Project acronym	USEMP
Full title	User Empowerment for Enhanced Online Presence Management
Grant agreement number	611596
Funding scheme	Specific Targeted Research Project (STREP)
Work program topic	Objective ICT-2013.1.7 Future Internet Research Experimentation
Project start date	2013-10-01
Project Duration	36 months

Workpackage	WP3
Deliverable lead org.	ICIS
Deliverable type	Report
Authors	Katja de Vries, Niels van Dijk, Sari Depreeuw and Mireille Hildebrandt (iCIS)
Reviewers	Alexandru Gisca (CEA) Marita Holst (LTU)
Version	0.2
Status	Final
Dissemination level	PU: Public
Due date	2016-09-30
Delivery date	2016-11-24

Version	Changes
0.1	Initial Release, Katja de Vries (iCIS)
0.2	Adjustments after two internal review, Katja de Vries (iCIS)

Table of Contents

Summary

This document presents an overview of the possibilities for fundamental rights protection by design (FRPbD), and more specifically data protection by design (DPbD), in the context of behavioural tracking and personalized advertising based on the digital trail created by the use of Online Social Networks (OSNs) and browsers. We focus on end users' rights derived from data protection law. Other relevant fundamental rights protection of internet users can be derived from Art. 8 ECHR (respect for private life) and EU anti-discrimination law. We discuss the latter in relation to the protection for the processing sensitive data in data protection law. Respect for private life is discussed in D3.12 as part of the analysis of portrait rights of internet users with regard to profiling practices.

We combine the legal analysis of these fundamental rights with a critical reflection on the architectural design of the DataBait tool created by the USEMP consortium. This results in a set of practical specifications for the design of the DataBait tool, based on legal design requirements which drive, frame and complement the technical and social requirements for DataBait.

One important set of design requirements following from the legal research presented in this document relates to the provision of support of OSN users in their right to profile transparency and the compliance of DataBait's own data processing with this requirement.

Another important design requirement following from this document is the development of the so-called *Data Licensing Agreement* (DLA) signed between the USEMP consortium and each DataBait user. This DLA enables OSN users to license the processing of their personal data in compliance with current EU Data Protection Law in exchange for the use of a profile transparency tool (the DataBait tool). The DLA used during the duration of the USEMP project was developed for a scientific consortium that processes these data for a purely scientific purpose (i.e., the USEMP consortium). In this deliverable we also show how the basic structure of the DLA is easily generalizable to similar transparency tools provided by other providers: only a few modifications are needed. We also explore whether this type of DLA could be used in conjunction with what we call "granular licensing". Granular licensing would mean that, based on the specified purpose and within the confines of use limitation, data subjects could set defaults as the context for further processing as well as the type of data controllers with whom the data may be shared, supported through a fixed set of standardized licensing options which might be presented in a layered format. We conclude that in the current setting (a transparency tool for OSN users) the possibilities for granular licensing are limited (firstly from the perspective of EU data protection law and, secondly, from the perspective of the current commercial ecology in which it would have to find a niche). However, in other settings (e.g. a medical setting where patients could be enabled through a personal data management system to set limits as to which health professional has access to which data) it might function well.

In addition to the profile transparency requirements and DLA, this document proposes two other sets of legal requirements applicable to profiling in OSN settings and tools which aims to provide transparency about it. The first set regards the anonymization/pseudonimization of profiling data. The second set concerns requirements for the handling of sensitive data (Art. 8 DPD/ Art. 9 GDPR) and the creation of awareness with regard to profiling with possibly illegitimate discriminatory applications.

1.Introducing DataBait. Juxtaposing first and third party providers of profile transparency.

The USEMP project has created DataBait. DataBait is a web application which shows users the kinds of surprising and sometimes invasive inferences that can be drawn from their behavior and disclosures (posts, uploads, likes, browsing behavior, etc.) on online platforms (such as Facebook). DataBait is a transparency tool that both educates and empowers. It expands the users' sense of the inferable—and unsettles the notion that users are in full control of what they choose to disclose. This helps users in the 'factual' control of their disclosures (e.g., deleting certain posts and uploads, adjusting visibility settings, blocking trackers) and in exercising their legal rights following from EU data protection law (e.g., requesting profile transparency from the data controller, especially with regard to the processing of sensitive data and/or differential treatments based on profiling). DataBait is both a first party provider of *actual* profile transparency (giving users insight in how the USEMP consortium processes the data of DataBait users) as well as an independent, third party provider of *speculative* profile "transparency" (showing what *could* be extracted) with regard to the processing performed by OSNs such as Facebook. Below we elaborate on the distinction between first and third party providers of profile transparency. Parts of section 1.1 (on first party profile transparency) have been included in DataBait as part of a tutorial to educate users and support them to more effectively control their disclosure behavior. The full tutorial and its role within DataBait is described in more detail in Annex 3 of D6.5 ("USEMP disclosure scoring framework and disclosure setting framework – v3").

With regard to profile transparency a distinction has to be made between:

- **First party provision of profile transparency *by the data controller*** which has to be provided in order to ***comply*** with EU data protection law,
- **Independent, third party provision of profile transparency *by tools such as DataBait*,** in order to ***empower*** users towards other data controllers

DataBait is both a first party provider of *actual* profile transparency (giving users insight in how the USEMP consortium processes the data of DataBait users) as well as an independent, third party provider of *speculative* profile "transparency" (showing what *could* be extracted) with regard to the processing performed by OSNs such as Facebook.

1.1. First party profile transparency

How can users of online platforms know what can be inferred from their online disclosures and behavior, who has access to this information and how it can be used commercially and otherwise? According to EU data protection law, providers of online services who process information relating to individuals have all kind of duties. These duties include, for example, that a data controller only collects and processes data based on one of the legal grounds listed in Art. 6(1) GDPR 2016/679[1] (for example, a legitimate interest of the controller that is not overruled by user interests, explicit user consent or a contract the user that necessitates processing), that she does not process data in a way that is unforeseeable (that is,

[1] 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).

incompatible with the specified, explicit and legitimate purposes set out at the moment of data collection), that she keeps the data safe, secure and up-to-date, and that she deletes them as soon as they are no longer necessary. Data controllers also have certain *informational* duties (see Arts. 12-15 GDPR 2016/679) with regard to their users when they process their data. These informational duties include providing some basic information at the time of data collection (e.g., purpose for collecting the data, contact details of the data controller, persons to whom the data may be disclosed, indication when the data will be deleted, existence of the right of access and rectification) and the duty to provide access to the data upon a user's request. When data processing includes *profiling* of users, these informational duties also entail that the data controller has to inform users about the fact that they are subjected to profiling and provide "meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject".

When data processing includes profiling of users, the data controller's informational duties also entail that users (1) are informed about the fact that they are profiled, (2) provided with "meaningful information about the logic involved", and about (3) the "significance and the envisaged consequences" of the profiling.

What does it mean to provide "meaningful information"? This is still largely open to interpretation. During the last few years one can see that large internet companies like Facebook or Google make increasing efforts in their experimentation with various ways of inform users about why they see certain advertisements.

What does it mean to provide "meaningful information"? This is still largely open to interpretation. During the last few years one can see that large internet companies like Facebook or Google make increasing efforts in their experimentation with various ways of inform users about why they see certain advertisements.

For example, from late 2014 onwards, Facebook has been experimenting with the provision of information in two formats: in an informational section about the users advert preferences and in informational pop-ups linked to advertisements shown to users. The exact content of both formats changes frequently – probably because it is still in the experimental trial-and-error stage. At the time of writing (August 2016) the content of these two sections (firstly, the "informational section about the users advert preferences" and secondly, the "informational pop-ups linked to advertisements shown to users") is the following:

(1) Facebook's informational section about the users advert preferences. This section (*see figure 1*) contains general information about the way advertisements are targeted at the user, a "your info" page (which invites the user to update and extend her profile information), a list of advert preferences ("interests"), and a list of advertisers with the user's contact info.

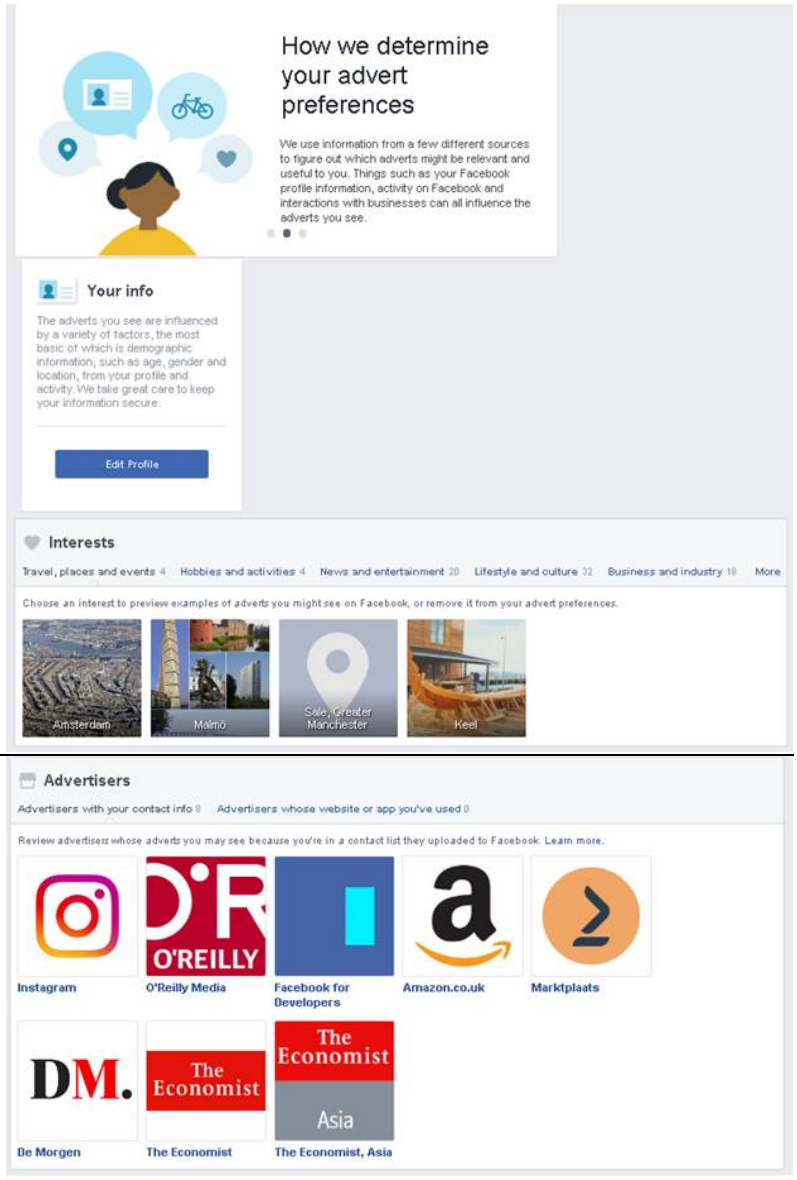

Figure 1. Facebook's informational section about the users advert preferences.

It goes beyond the scope of this report to look in detail at each of these subsections. However, in relation to DataBait it is particularly interesting to take a close look at the list of advert preferences. Each user can now inspect (and adjust) the list[2] of the advert preferences that Facebook attributes to her (figure 2).

[2] https://www.facebook.com/ads/preferences/

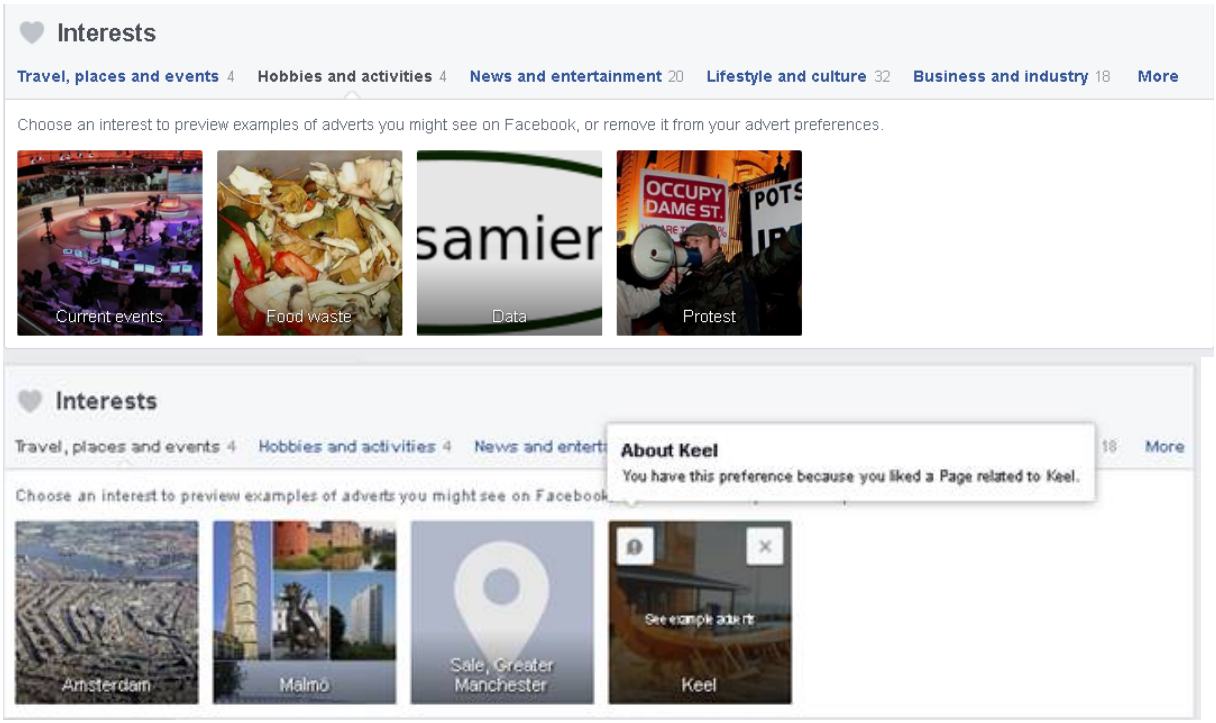

Figure 2. Two examples of sub-lists ("Hobbies and activities" and "Travel, places, events") from the complete list of the advert preferences ("interests") that Facebook attributes to a user. When clicked, each interest comes with a possible explanation as to why Facebook attributes this interest to the user (see the pop-up "About Keel", in the lower left corner).

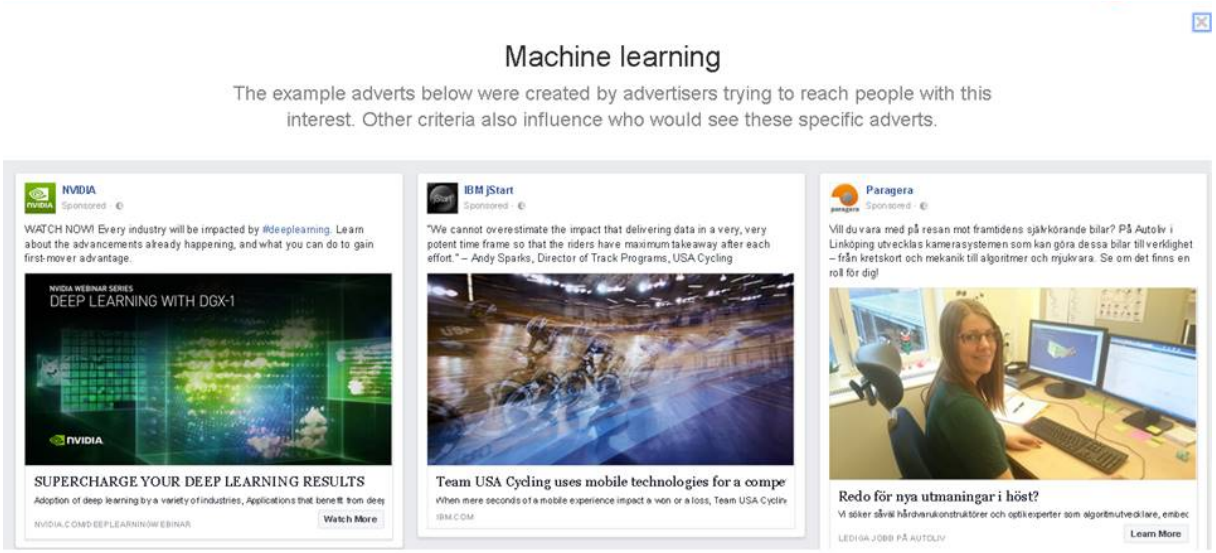

Figure 3. Facebook offers examples of advertisements that could be shown based on an interest.

Each interest (e.g., "Protest", "Wifi Connection", "Park" or "Away from hometown") comes with some examples of advertisements that could be shown based on it (figure 3) and an explanation (figure 2) as to how it was inferred. Examples of such explanations:

*"**Protest**: You have this preference because you liked a Page related to Protest"*

*"**Wifi Connection**: You have this preference because we think it may be relevant to you based on what you do on Facebook"*
*"**Park**: You have this preference because you clicked on an advert related to Park."*
*"**Away from hometown**: You have this preference because we think it may be relevant to you based on what you do on Facebook"*

The explanations are both illuminating as well as opaque. It *is* illuminating to know that my profile for advertisements contains inferred interests such as "Protest", "Wifi Connection", "Park" or "Away from hometown". It *is* also illuminating to know that the inference of some of these interests is based on likes, others on advertisement clicks and others on "*what you do on Facebook*". However, not all of these explanations make it easy to trace the attributed interest back to the actual behavior that caused the attribution. This is particularly clear with an explanation like "*based on what you do on Facebook*" – which is very general. The explanation "*because you clicked on an advert related to Park"* is also difficult to relate to actual behavior: a user might not remember clicking on an ad, nor think of this ad as relating

Facebook provides explanations to their users why certain advert preferences are attributed to them. Why is a user attributed to have an interest in, for example, "Protest"? Explanations such as "*This is based on what you do on Facebook*", "*Because you clicked on an advert related to <Protest>*" or "*Because you liked a Page related to <Protest>*" are both illuminating as well as opaque. It is not always easy to trace the attributed interest back to the actual behavior that caused the attribution.

to "Park". The explanation "*because you liked a Page related to Protest"* is a little better, because a user can inspect her list of likes and guess which of these likes is qualified as being related to "Protest". Still, guessing which liked page qualifies as related to protest is not necessarily very obvious. Is it the like for a page that advocates diminishing foodwaste? Or the like for a page that is critical of unrestrained surveillance and data collection? Or some completely different like?

(2) Facebook's informational pop-ups linked to advertisements shown to users. Facebook gives some additional information about the logic of targeted advertisements in the way shown in figure 4. It is only when users hover over the portrayed ad that a cross appears in the upper right corner. If a user would then click on this cross, then they are shown three options (see figure 4).

Figure 4. Facebook offers a (slightly hidden) button on top of each displayed advertisement that offers some information as to why a user is presented with it.

It is only when users click on the second option 'Why am I seeing this?', that they are informed of possible reasons for seeing this ad:

- *One reason why you're seeing this advert is that **Seats and Sofas België** wants to reach people who were **recently near their business**. This is based on information from your Facebook profile and your mobile device.*
- *There may be other reasons why you're seeing this advert, including that Seats and Sofas België wants to reach **people aged 25 to 64 who live near Mechelen, Flemish Region**. This is information based on your Facebook profile and where you've connected to the Internet.*[3]

The first explanation is quite straightforward, the second one includes an interesting caveat *("There may be other reasons you saw this ad"*). While Facebook informs, it still does not refer to the data that actually linked this ad to a particular user, it only refers to possibilities.

We will have to wait for relevant case law before we can say whether Facebook's explanations are sufficient interpretations of "meaningful information". It is difficult to predict what the outcome of a court case would be. Companies, like Facebook, might be inhibited in their provision of 'meaningful information' in at least two ways. The first inhibition is rooted in a practical problem: often machine learning models (such as neural networks) are used that are too complex to be interpretable for the human mind, which means that even the creator of a profiling algorithm is not able to tell why a particular input generates a particular output. One way to solve this could be to build an interpretable model (e.g. a decision tree or a simple linear function) that, given the inputs and outputs of the overly complex model, tries to grasp the gist of what goes on inside the algorithmic 'blackbox' (Ribeiro, Singh, & Guestrin, 2016). However, such a simple model might not always be a good representation of what is happening in the complex model because it is a simplification and because it is a guess (even if it is a guess which is grounded in sound statistical modelling) meaning that it can be *wrong* guess. It is not unimaginable that in certain business models it would be seductive to spent very little resources on building simple interpretable models on top of algorithmic blackboxes because they would only act as a sop or placebo to keep users or clients happy and give them a (false) sense of control. Another potential inhibition in the provision of meaningful information is that too much transparency could lead to the disclosure of information (possibly protected by intellectual property rights) that gives a profiling business

[3] Facebook.com, 2 August 2016.

its competitive advantage. The tension between the fulfillment of their informational duties and preservation of trade secrets is explicitly acknowledged in recital 63 of GDPR 2016/679:

“A data subject should have the right of access to personal data […]. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject.”

Recital 63 acknowledges the need to protect both commercial interests as well as individual data protection rights – and that the latter can never be *completely* be overruled by the former.

The tension between the fulfillment of informational duties and the preservation of trade secrets is explicitly acknowledged in recital 63 of GDPR 2016/679. It also states that individual data protection rights can never be completely be overruled by commercial interests

1.2. Third party profile transparency

Two ways of providing third party profile transparency:

- **Input-Output matching:**

That is: guessing what happens in the 'blackbox' of an OSN based on a matching of input (user profile) to output (advertisements served to the user). Examples of such matching tools are *XRay*, *AdFisher*, *SunLight* or the tools developed in the "*Value & Values*" project.

- **Input speculation**

That is: giving users a sense of the inferable by showing what is possible to infer from the input (user profile) based on the independent profiling algorithms of the third party transparency provider (DataBait).

This *speculative* approach is a novel approach.

Next to the information provided by data controllers based on their informational duties, independent third parties can also provide tools that offer some additional 'transparency' or 'information' about the profiling process. Such tools are often developed by independent researchers or civil society organizations and aim to empower, educate and/or fulfill a watchdog function. This is particularly useful when data controllers give a limited interpretation to their informational duties regarding the profiling of their users. Because independent third parties do not have direct access to the profiling process, they have to make educated guesses about what happens in the 'profiling blackbox'. One way to do this is *input-output matching*: experimentally studying what changes in the 'output' (advertisements, search results, items shown in news feed, etc.) if the input (posts, likes, uploads, searches, profile information, etc.) is changed. Examples of such matching tools are *XRay*[4], *AdFisher*[5], *SunLight*[6] or the tools developed in the "*Value & Values*"[7] project. In contrast to these tools, DataBait does not match output to input, but *only looks at the input*. It does not aim to mimic what a profiler like Facebook exactly does within the 'profiling blackbox' but simply shows what could be inferred from the user's input (posts, likes, photos, etc.) based on the state of the art in machine learning. Consequently, in comparison to transparency tools based on input-output matching, DataBait's insights are more *speculative*: the connection between the studied profiling process (e.g. Facebook's profiling) and the insights generated by the transparency tool is looser. This has both drawbacks as well as advantages. The advantage of DataBait is that it is less dependent on the profiling process it studies. This has at least two advantages. Firstly, companies like Facebook or Google change their 'profiling algorithms' very frequently. Input-output matching might end up 'running behind the facts' all the time, needing to adapt to the constantly changing algorithms. Secondly, for a commercial profiler it might be easier to co-exist with a

[4] *Xray* (2014) is a tool developed at Columbia University by R. Geambasu, A. Chaintreau and M. Lecuyer. See: http://xray.cs.columbia.edu/. The tool provides "reusable algorithmic building blocks in support of many targeting investigations" (Lecuyer et al., 2015, p. 556) and was used to "reverse-engineer the connection between ads shown to Gmail users and keywords in their messages". (Simonite, 2015)

[5] *AdFisher* (2015) is a statistical method developed at Carnegie Mellon by, amongst others, A. Datta. See https://www.cs.cmu.edu/~mtschant/ife/. See: (Datta, Tschantz, & Datta, 2015). "AdFisher, received attention earlier this year after showing that fake Web users thought to be male job seekers were more likely than female job seekers to be shown ads for executive jobs when later visiting a news site."

[6] *SunLight* (2015) is a tool developed by the same team as *Xray*. It builds on both *Xray* and *AdFisher* (Lecuyer et al., 2015, p. 556). See: https://columbia.github.io/sunlight/ (or: https://github.com/columbia/sunlight) and www.cs.columbia.edu/~djhsu/papers/sunlight.pdf. "Sunlight is distinctive in that it can examine multiple types of inputs simultaneously (e.g., gender, age, browsing activity) to develop hypotheses about which of these inputs impact certain outputs (e.g., ads on Gmail)". (Datta, as quoted by: Martineau, 2015)

[7] ESRC Professorial Fellowship (United Kingdom) project "Value and Values" (ES/K010786/1) conducted between 2013-2016 by Bev Skeggs and Simon Yuill. Online available: https://values.doc.gold.ac.uk/ The main publication describing the methodology: (Skeggs & Yuill, 2016).

transparency tool like DataBait because there is no attempt to 'reverse engineer' a *particular* algorithm. DataBait uses its own algorithms, developed within the USEMP project, and does not say anything about how the algorithms of one profiler (e.g. Facebook) relate to another (e.g. Google). A commercial profiler might claim that it's commercially disadvantageous if competitors can get insights in its particular algorithms through a third party transparency tools, or if its algorithms are 'misrepresented' ('slander') which might result in bad publicity. It is thus less likely that a commercial profiler will use IP rights (copyright, database rights, patents, etc.) or other rights (trade secrets, right to conduct a business) to interfere with the type of transparency provided by a tool like DataBait. If a company would want to use their IP rights to obstruct 'transparency' as provided by DataBait, it could only do so through IP rights it might have on the 'input' (the user data and, possibly, their structure). DataBait's advantageous independence is also its drawback: the advantage of input-output matching over DataBait's approach is that it is way more *specific*. Input-output matching looks at a particular online platform or application (e.g. how do the *Google* ads change if you adjust your profile). DataBait, however, when compared to input-output matching is likely to give more individualized information ("this is what we can infer from *your* data"). Input-output matching often takes an experimental format ('what changes in the output, if we change this input?") from which *general* conclusions follow (e.g., 'if you change your ethnicity from Y to X, you get more advertisements A instead of B'). Finally, it should be noted that both in the case of 'input speculation' (DataBait) and input-output matching the conclusions drawn will be dependent on the variables studied by the researchers. DataBait has a specific focus[8] on (inferred) user information which is classified as sensitive ("special categories of data") by EU data protection law and/or that is likely to be perceived as such by the user.
This leads to the conclusion that DataBait's speculative input-approach and input-output matching approaches are complementary: each in their own way they are valuable transparency tools that can be provided by independent third parties.

When comparing the profiling insights provided by DataBait with the information provided by Facebook, we again see that they complement each other. As noted above, the information provided by DataBait can be said to be *speculative*: it shows what can be inferred given the state-of-the-art in machine learning – not what Facebook actually infers. However, compared to some of the insights given by DataBait, Facebook's information is also *speculative* (though in a very different sense!) as it often only gives *possible* (*"there may be other reasons you saw this ad"*) and rather *general* (e.g.,"*you have this preference because we think it may be relevant to you based on what you do on Facebook*") indications of why certain interests are inferred. In contrast, in the section "My disclosures" DataBait allows the user to trace an inferred interest (e.g., "pizza") or categorization (e.g., "drunkard") back to the actual data (see figures 5 and 6).

In "My disclosures" DataBait allows the user to trace an inferred interest (e.g.,"pizza") or categorization (e.g., "drunkard") back to the actual data.

[8] This is reflected in the DataBait "privacy score", which is based on information relating to the following categories: health, hobbies, psychology, sexuality, politic, demographics, religion, employment and relationships.

Figure 5. In the "My disclosures" section DataBait offers the possibility to go back to the data (in this case: photos) that underlie why DataBait attributes a certain interest or categorization to a user. Here an example of the ten pictures in a user profile which underlie the categorization "drunkard". (N.B. in the actual version of DataBait faces are not blurred). Pictures with a red frame around it are categorized as "probably sensitive" (recommendation to remove them). Pictures with a green frame are categorized as "probably less sensitive". In order to make this categorization more accurate DataBait invites users to correct the given categorizations if necessary (and thus to create more training data on users perceptions of sensitive and less sensitive pictures).

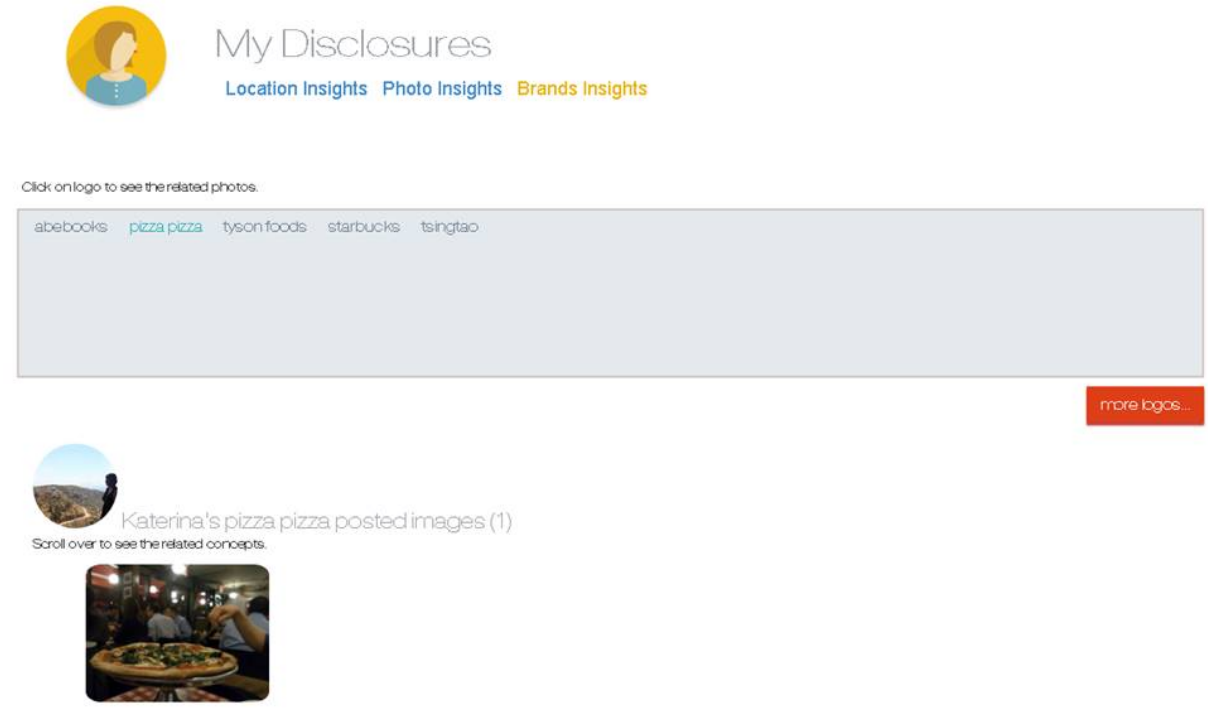

Figure 6. In the "My disclosures" section DataBait offers the possibility to go back to the data (in this case: photos posted by the user on Facebook) that underlie why DataBait attributes a certain interest or categorization to a user. Here an example of the photo in a user profile which underlies the brand interest "pizza pizza".

However, it should be noted that also DataBait is not always able to provide a link to an individual piece of data. In the section “your privacy score”, where the inferences are based on DataBait’s “privacy score”-model (which takes together a whole set of factors), DataBait does refer the user to review their profile in general as it is unable to provide the link to all the underlying individual pieces of data (figure 7).

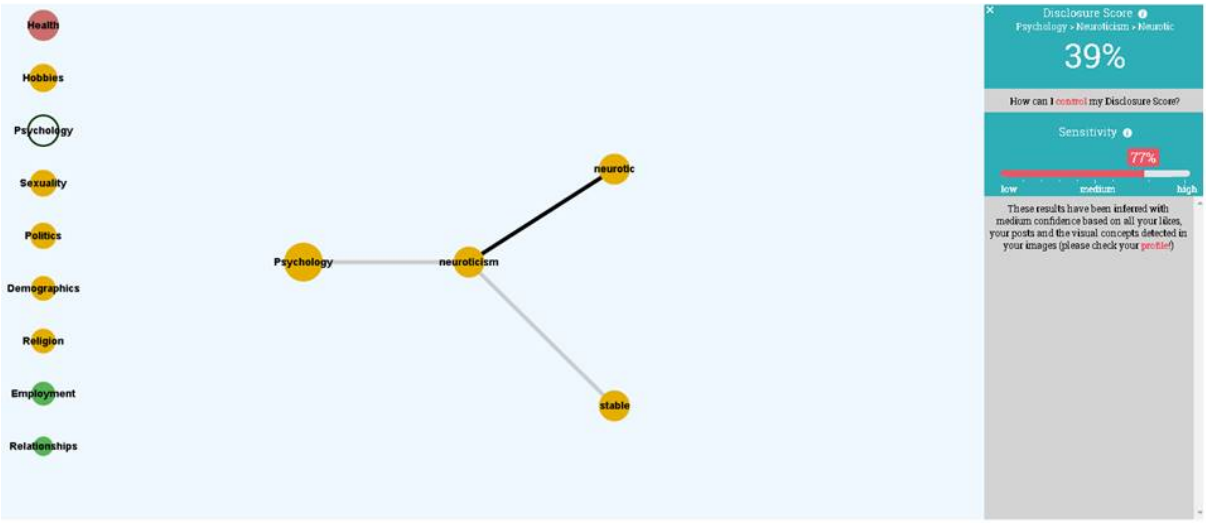

Figure 7. An example from DataBait’s section “Your disclosure scoring”. The disclosure score for the psychological trait “neuroticism” of this user is 39%, which means that the exposure and risk for this trait is rather low. The score is not linked back to individual pieces of user data: “These results have been inferred with high confidence based on all your likes, your posts and the visual concepts detected in your images (please check your profile!)”. The disclosure score takes into account three factors: a) DataBait’s confidence that the predicted value (in this case: “neuroticism”) applies to the user, b) the visibility of the associated content to other social network users (for instance, public posts are more visible compared to posts shared with user’s friends only) and c) the sensitivity of different pieces of information. The first two factors are automatically computed by DataBait, whereas the third factor is initialized with some default values that have resulted from DataBait’s user studies, but can be adapted according to the user’s preferences.

1.3. DataBait: fair and lawful profile transparency

Creating the *DataBait* tool is not only an experiment in creating a profile transparency tool supporting the exercise of rights following from the data protection framework (that is, *user empowerment*). It is also a way of experimenting with optimal forms to *comply* with the

Despite the seemingly extensive definition of 'Data Protection by Design' in Art. 23(1) of the GDPR, an exact understanding of this notion is still heavily debated

requirements of (profile) transparency and fairness of data processing ("Data Protection by Design" or DPbD) when creating a transparency tool. Art 23(1) of the GDPR ("*Data Protection by Design and by Default")* reads:

> "Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject."

Despite the seemingly extensive definition of *Data Protection by Design* in Art. 23(1) an exact understanding of this notion is still heavily debated. Article 23(2) obliges the data controller to implement mechanisms to ensure *Data Protection by Default*, which is a certain form of *Data Protection by Design* based on the idea "that privacy intrusive features of a certain product or service are initially limited to what is necessary for the simple use of it" (European Data Protection Supervisor 2012, 7 March, p. 29-30). However, as the European Data Protection Supervisor (EPDS) argued in its Opinion on the GDPR, Article 23(2) does not give "any clear substance" to "data protection by default":

> "The first sentence does not add much to the general principles of data processing in Article 5, and the data minimisation principle in Article 5(c) in particular, except from the confirmation that such principles should also be embedded in the design of relevant systems." (European Data Protection Supervisor 2012, 7 March, p. 29).

The DataBait tool can act as an example of how the right to profile transparency could be transposed into the technological and organizational design of systems and practices which profile end-users

When we try to imagine how the right to profile transparency could be transposed into the technological and organizational design of systems and practices which profile end-users, tools like the one developed in the USEMP project (the *DataBait* tool) could be the

answer. When the GDPR comes into force, and DPbD becomes an enforceable legal requirement, the DataBait tools can be a good example of how profile transparency could be built into otherwise opaque automated profiling systems. In this section we list the various ways in which the DataBait tool aims to comply with data protection law in the best possible way.

To begin with, *DataBait* users are expected to sign a contract before using this profile transparency tool. This contract, the so-called *Data Licensing Agreement*, is the legal ground for any data processing performed by the USEMP in relation to the data gathered by the *DataBait* tool. The contract supports transparency by avoiding any unnecessary 'legalese' and specifying the purposes and the process of the data processing in a very comprehensive way. In comparison to data processing based on user consent, using contract as a legal ground for the processing creates a more equal footing between the data subject and the data processor. Chapter 4 of this deliverable is devoted to explaining this way of DPbD through the contract.

Another way in which compliance with Data Protection law is realized in the current preliminary version of *DataBait* is the clear user interface where one can request data deletion and withdraw consent for the processing of one's sensitive data (see figure 8).

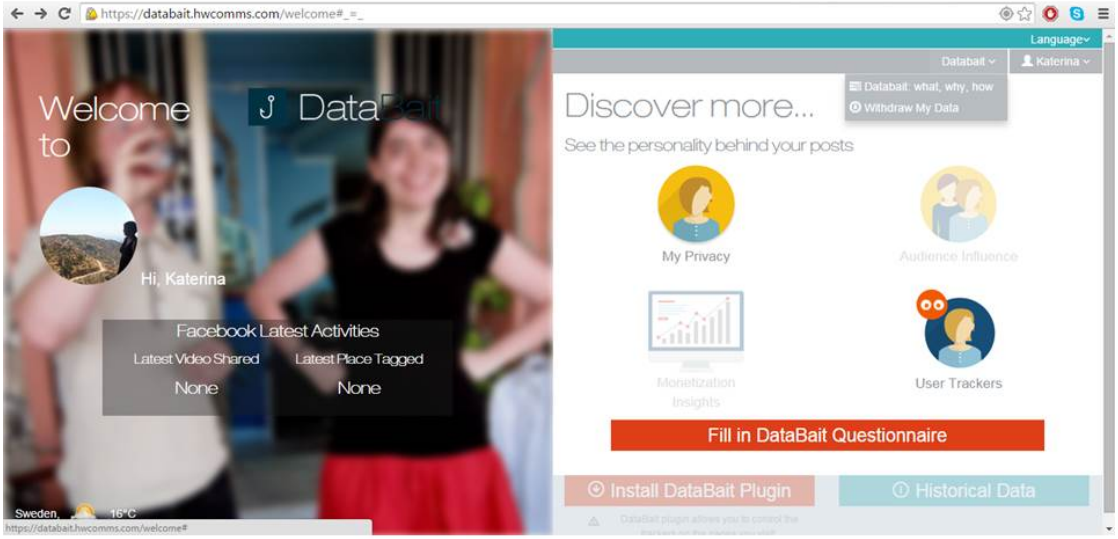

Figure 8. The 'Withdraw My Data'-button in the preliminary version of DataBait (August 2016) can be found in the upper right corner.

While all the information that the data controller is required to provide to the data subject is in principle included in the contract (the 'Data Licensing Agreement' or DLA) signed by each user of the *DataBait* tool, the USEMP consortium also provides additional information to further enhance the transparency and fairness of the processing in the '*DataBait: how, what and why?*'-section (see figure 9). When drafting this section we made a list of items that should be included in this section:

(1) The contract signed by each user (the 'Data Licensing Agreement', abbreviated as DLA) and the contract which all USEMP partners have signed amongst each other with regard to the processing of personal data (the 'Personal Data Processing

Agreement', abbreviated as PDPA) which also incorporates the DLA and binds each USEMP partner.

(2) Some very practical info, including the identity of the data controllers in the USEMP project, an email address for each USEMP partner that processes personal data (to make further inquiries), information about the existence of the right to request rectification or erasure of the data concerning the data subject and of the right to object to the processing, and the right to lodge a complaint to the supervisory authority and the contact details of the supervisory authority.

(3) Text, graphs and/or an animation providing insight in the general logic of the processing and a precise description of operations performed. This includes references to the databases used for training and testing the USEMP analytic algorithms (used to derive additional information from the raw data of the user) and a list with precise descriptions of what categories/types of data are collected/processed by each USEMP partner and how they are processed (this list is also presented in clause E of the PDPA).

(4) Text, graphs and/or an animation clarifying the purpose for which the data are processed, for what estimated period, which recipients receive the data (no data sharing to third parties!), and what might be the consequences of such processing.

(5) Provision of which data are actually processed [corresponding to the data listed in D3.4 and D3.9]. In a post-USEMP version of DataBait one might consider adding a button which allows users to download all their data in the '*Which of your personal data do we process?*'-section (in the current version this was deemed technologically difficult to realize).

(6) Complementary information with regard to data protection rights EU citizens have with regard to, for example, OSNs and browsers processing their personal data in an additional tab entitled '*Your digital data protection rights*'. (under construction)

These five requirements have been translated into four tabs in the '*DataBait: how, what and why?*'-section (see figures 9 till 12), entitled '*DataBait at a Glance*' (containing flow-charts, explanatory text, and an explanatory video-animation giving an overview of the processing actions performed on the data gathered by the *DataBait* tool, the purpose of the processing and the relevant responsible actors), '*Which of your personal data do we process?*' (containing lists of collected data types), '*Practical info'* (containing all practical contact details for the exercise of the right of access and rectification) and '*DataBait Contract: Terms of Service'* (containing the DLA and PDPA).

The content and the format of the information in the '*DataBait: how, what and why?*'-section is not radically new in itself: it is mostly information which each data controller bound by EU law has to provide (explanation of the processing through text, graphs, and animations; lists of processed data types; the possibility to download your data; contact info; information about legal rights; terms of service and data policy). Yet, while many data controllers are bound by a double bind, namely the need to comply with data protection law as well as the need not to scare users away with too much insight in what is happening with user data, the USEMP project does not have such an ambiguous position. For example, when a user signs up for *DataBait*, the user cannot simply click 'consent' to the DLA contract as a whole, but has to click through every clause (twelve screens). A commercial data controller would probably refrain from choosing such a format, being afraid that the sign-up procedure will become too tedious and gives the user 'too much' insight in the data processing. However, the USEMP project is an excellent occasion to check and experiment

with how users react to such format – do they indeed dislike it because it takes longer? Do they become better informed? Etc. During the pilot in August 2016 such questions where explored (see WP 4 and 8).

USEMP uses a layered way in providing information to the *DataBait* users. The explanatory text contains many hyperlinks where the interested user is able to find more detailed information. For example, the text explaining how the USEMP-DataBait algorithms were construed contains links to the databases used to train and test the algorithms. In providing information to users we had to find a middle ground between oversimplification and buffer-overload by providing the user with too much technical details. There is a fine line between making a complex situation understandable and oversimplification. Moreover, there is no 'free lunch' in communicating security or privacy risks in a heuristic way (Asgharpour, Liu, & Camp, 2007; Camp, 2006): the "cost" of a heuristic presentation is that it will always contain a bias in some direction. Finding optimal ways of making *DataBait* compliant with EU Data Protection law is in this sense also an opportunity to find the best possible mental models in communicating the risks and implications related to data processing, and particularly profiling. Thus, using hyperlinks allows for a layered approach where a user has the option to choose between different layers of detaill when informing herself about the data processing to which she is subjected.

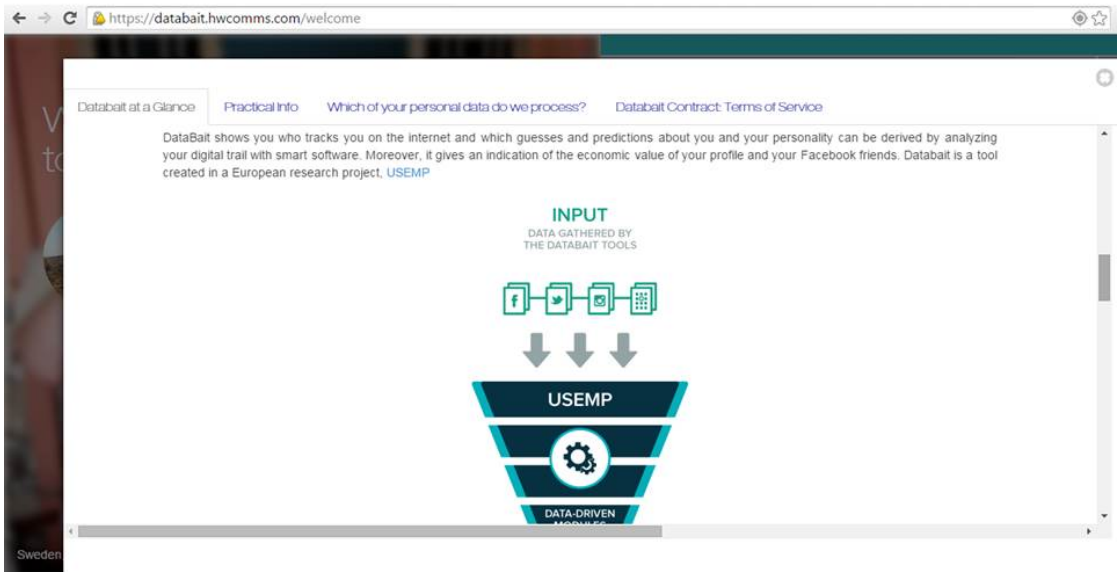

Figure 9. The 'Databait: what, why, how'-section in the preliminary version of DataBait (August 2016) contains four subsections: the first one is 'DataBait at a Glance'.

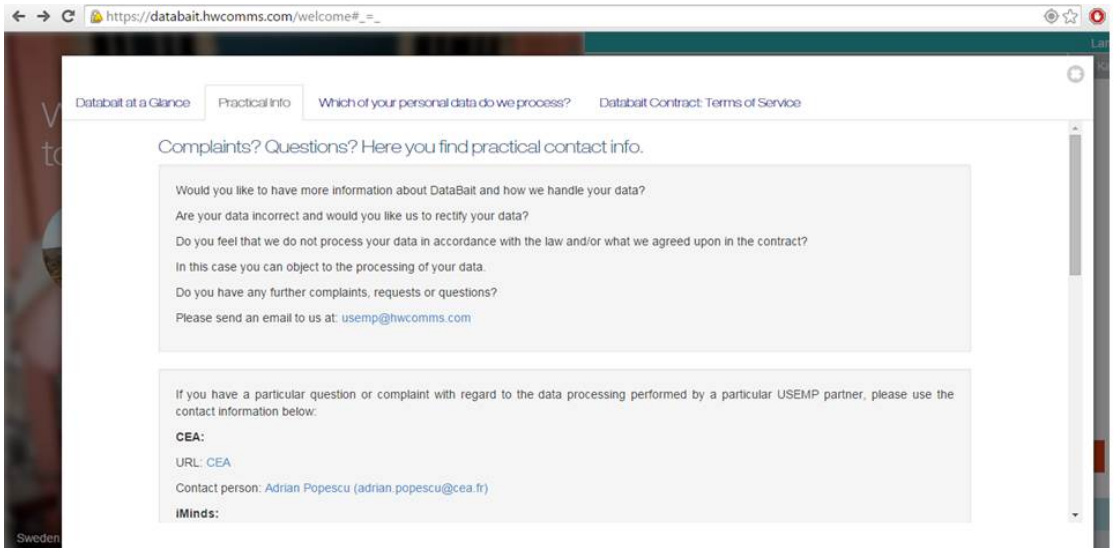

Figure 10. The 'Databait: what, why, how'-section in the preliminary version of DataBait (August 2016) contains four subsections: the second one is 'Practical info'.

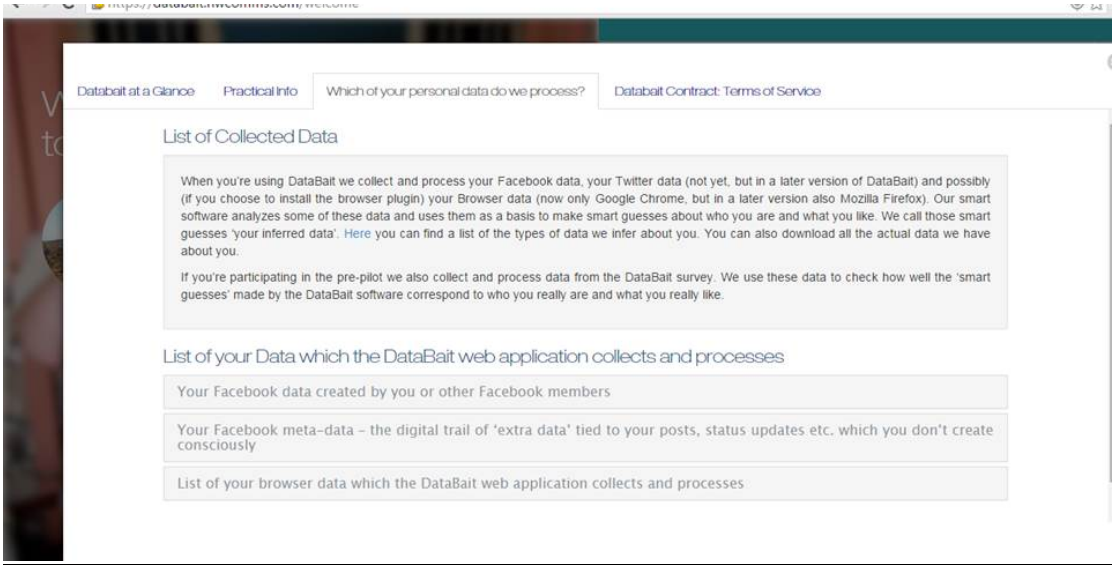

Figure 11. The 'Databait: what, why, how'-section in the preliminary version of DataBait (August 2016) contains four subsections: the third one is 'Which of your personal data do we process?'

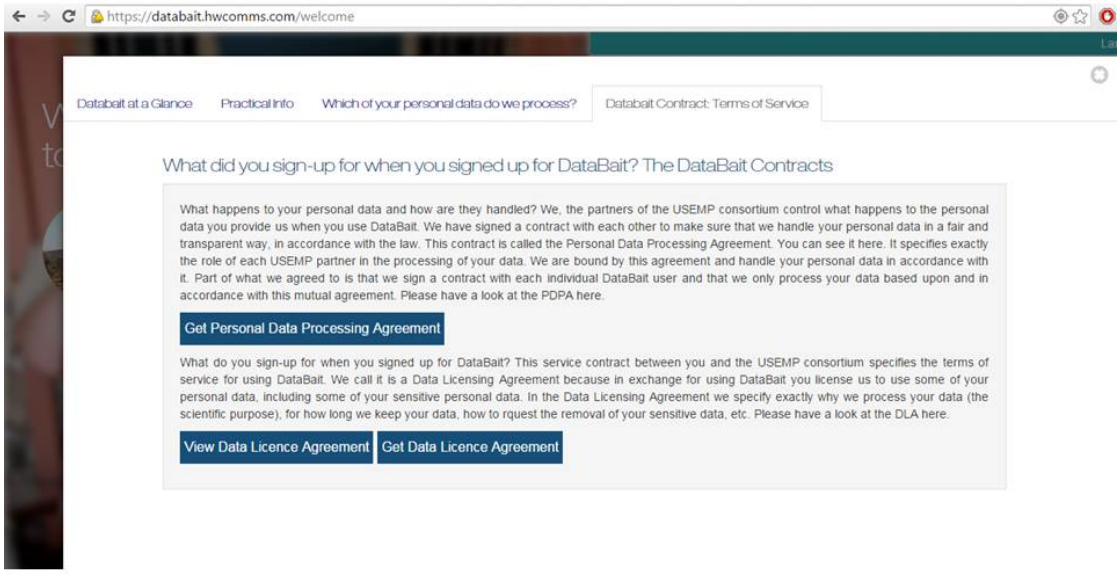

Figure 12. The 'Databait: what, why, how'-section in the preliminary version of DataBait (August 2016) contains four subsections: the last one is 'DataBait Contract: Terms of Service'.

2. Can third party profile transparency tools be combined with PDM solutions?

Can personal data management (PDM) solutions be combined with third party profile transparency tools such as DataBait? PDM providers (such as Mydex[9], IRMA[10], Synergetics[11], Qiy[12], etc.) are intermediaries between users and those who want to access user data. PDM providers keep user data in a virtual safe box and provide access based on a permissions system[13]. The exact conditions can vary but the general idea is that access is only given if this is legally necessary (the fulfillment of legal obligations, e.g. following from a contract to which the user is a party, or a legal requirement) or if a users have given explicit consent. The benefit of using a PDM provider as an intermediary is that your data are kept safe and that no more data than strictly necessary are shared.

Personal data management (PDM) providers are intermediaries between users and those who want to access user data. The benefit of using a PDM provider as an intermediary is that your data are kept safe and that no more data than strictly necessary are shared

For example, if you want to buy alcohol, the seller should have access to information shoing that you are old enough to be legally allowed to buy alcohol. The seller does not need to know your name, adress, religion, etc. for such a transaction. A PDM provider can ensure that only necessary information is shared. The idea of combining profile transparency tools with PDM solutions is that, firstly, a user could define who can access which data *based on* the insights derived from the profile transparency tool, and secondly, the PDM system could ensure that any third party re-user will sign an adequate DLA (adjusted to the specific data transfer) with the user that includes profile transparency in exchange for the data.

The idea of combining profile transparency tools with PDM solutions is that, firstly, a user could define who can access which data based on the insights derived from the profile transparency tool, and secondly, the PDM system could ensure that any third party re-user will sign an adequate DLA (adjusted to the specific data transfer) with the user that includes profile transparency in exchange for the data.

[9] https://mydex.org/
[10] https://www.irmacard.org/irma/
[11] http://synergetics.be/
[12] https://www.qiyfoundation.org/
[13] There are many cryptographic possibilities. For example, one such possibility is the use of Attribute-based Credentials (ABC). See: https://abc4trust.eu/ and (Koning, Korenhof, & Alpár, 2014)

Before exploring whether a transparency tool like DataBait could be integrated with a PDM like solution we need to look at the principle of purpose limitation. As we will see this principle is crucial to the functioning of such combined PDM-transparency service.

2.1. The limits of purpose limitation?

The European legal framework for data protection enables the processing of personal data within the EU whilst making sure that this happens in a way which is lawful, fair and transparent. One of the *fairness and transparency* requirements is that any processing has to be justified *by a specified, explicit and legitimate purpose* and that further processing for other incompatible purposes is not permitted (the so-called purpose specification and limitation principle, art. 6(1)b GDPR and Art. 5(1)b DPD[14]). Parts of industry have been lobbying to make re-use of personal data easier by relinquishing the purpose limitation principle in the new GDPR. Fortunately this did not happen: it would have emptied EU data protection from one of its core ideas, namely preventing personal data from circulating around for other purposes than the one for which they were initially collected. Data being re-used for purposes which no one foresaw at the time of collection, or even worse: data being transferred from one data controller to another as if they were simple goods that can be used for whatever purpose their 'owner' deems right, is in absolute opposition to the purpose specification and limitation principle.

So how to decide which re-use is

Key Points from the legal framework to keep in mind when discussing data re-use:

- Processing of personal data has to be based on a legal ground. Only processing of data based on one of the legal grounds listed in Art. 6.1 GDPR is lawful. This list includes, for example, consent given by the data subject (Art. 6.1(a)) and a legitimate interest of the data controller (Art. 6.1(f)).
- Next to the requirement that processing has to be based on one of the grounds listed in Art. 6.1 GDPR, processing of personal data is limited by the purpose limitation principle (art. 5.1(b) GDPR). This means that it is prohibited to re-use data for purposes that are incompatible with the purposes for which the data was initially collected.
- A strict understanding of purpose limitation is that even consent to re-use for a incompatible purpose is not enough to allow for such re-use; data will have to be deleted and recollected for the new purpose.
- The strict understanding of purpose limitation is not very common. The more common understanding (to which we adhere as well) is that re-use is allowed as long as the data controller specifies the new purpose and gets consent.
- When the ground for the re-use of the data is not consent but, for example, a legitimate interest of the data controller (Art. 6.1(f)), the data controller will still have to inform the user of the new purpose.

[14] 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 , 23/11/1995 P. 0031 – 0050.

still compatible with the original purpose and which is incompatible? One way is to compare the *context* of the collection and of the re-use (Custers & Uršič, 2016; Uršič & Custers, 2016). However, the notion of "context" is quite tricky. One could argue that data collected in a hospital to monitor your health during your treatment and the re-use of these data by a pharmaceutics company stays within the "same" context (the "medical" one). However, because the type of data processor (the 'actor') changes from a health professional to a commercial business aiming for profit, it is still unlikely that this would qualify as a compatible purpose. Probably the best way to decide whether a new purpose is compatible is to simply compare *purposes*: is the purpose "medical treatment" still compatible with "generating profit from a new drug"?

A very strict interpretation (see e.g. WP 29, Opinion on Purpose Limitation, 2013; Koning, 2014) of the principle of purpose limitation holds that even if the data subject explicitly consents to re-use of data for a purpose which is incompatible with the one for which the data was originally collected, this would infringe on the purpose limitation principle and thus be unlawful under the current legal regime. However, the more common interpretation is that, as long as the new purpose is specified properly and a new legal ground for the processing is available (for example explicit consent[15] or because processing is necessary for the purposes of the legitimate interests pursued by the controller; Art. 6(1) GDPR), data can be re-used. In the case of Facebook one could, for example, argue that the processing of data for targeted advertisements belongs to the business model of Facebook and as such is processing for the sake of Facebook's legitimate interests (see for a comparible line of reasoning: CJEU 13 May 2014, C‑131/12, Google Spain v Costeja Gonzalez). It should be noted that if the legal ground is the "legitimate interests of the data processor", this does not imply that the data processor can keep the new purpose and the new legal ground to herself. She still has the duty to *inform* the user (Art. 13 and 14 GDPR).

The purpose is specified by the data controller at the moment of data collection. As such it is a *one-sided* decision of the actor carrying the responsibility for the lawfulness, transparency and fairness of the processing.

Wouldn't everyone benefit from a transparent handling of data where there is mutual agreement with regard to the context for further processing as well as the type of data controllers with whom the data may be shared, and where it is clear to all actors how and for what purposes a piece of personal data can be processed?

However, wouldn't everyone benefit from a transparent handling of data where there is *mutual* agreement with regard to the context for further processing as well as the type of

[15] The risk here is that a data subject could be nudged ("Please consent to these new terms of service – don't bother reading them, just click 'yes'") or forced ("Please consent to these new terms of service – otherwise we'll deny you access to this service") to agree with further processing. This could be avoided by prohibiting contractual clauses that deny continuation of service in case the data subject does not consent, and by requiring the consent to be explicit and informed.

data controllers with whom the data may be shared, and where it is clear to *all* actors how and for what purposes a piece of personal data can be processed? Neither internet users, nor industry benefit from a situation where industry operate in a grey legal zone (see D3.5). Not only does this entail for the industry that they are unsure if their data processing actions are within the boundaries of law, but the opaque situation also is more likely to result in personal data of unknown quality and origin. Ideally, a user would be aware of the fact that she has a profile which categorizes her as someone who, for example, enjoys good wines and loves books, and could adjust her information (e.g., '*No, I'm not interested in books about gardening and I don't like Chardonnay, but I do like Merlot wines and Italian twentieth century literature*'), and specify in which ways this information can be used (e.g., *'I do like to receive offers for Bordeaux wines, but I don't want the data about my drinking habits to be available to health insurers'*). While such a transparent and voluntarist system could decrease the quantity of data available to certain parts of industry (e.g., because many users might choose to prohibit the use of their data for price differentiations for services such as insurances), it would increase the reliability of the data and provide legal certainty about the purposes for which these data can be processed. As discussed above, in section 1.1 ("First party profile transparency"), Facebook already includes the option to adjust one's "interests". Clearly, Facebook and users benefit if data is as correct as possible: users are more likely to see adverts that they actually like (though it should be noted that this can also lead to a self-confirming circle or "filter bubble") and Facebook can serve advertisers better tailored audiences. Facebook does not include the option for users to select the types of advertisers that might contact them.

If the current data protection regime is so strict, how is this compatible with the situation where users are tracked and targeted with personalized ads despite the fact that they move from one website to another? We will now discuss three legal 'loopholes' which can sometimes be used in an intermingled way: a vague and broad description of the processing purposes at the stage of getting user consent (in the general terms and conditions) undermining the rationale of purpose specification, a loose interpretation of what counts as a "compatible purpose" for the processing of personal data, and the possibility for the data controller (who has stated this as a processing purpose) to offer a multiplicity of actors the possibility to 'address' an end-user based on her profile (targeted ads), without disclosing or transferring any actual data to these actors.

Why are internet users tracked and targeted through different websites and contexts despite the purpose limitation principle?

(1) a vague and broad description of the processing purposes at the stage of getting user consent (in the general terms and conditions) undermining the rationale of purpose specification,

(2) a loose interpretation of what counts as a "compatible purpose" for the processing of personal data, and

(3) the possibility for the data controller (who has stated this as a processing purpose) to offer a multiplicity of actors the possibility to 'address' an end-user based on her profile (targeted ads), without disclosing or transferring any actual data to these actors.

Before discussing the details of each of these three loopholes, we first need to take a closer look at the exact formulation of the principle of purpose limitation in Art. 5(1)(b) GDPR and Art. 6(1)(b) DPD 95/46:

> "personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall […] not be considered to be incompatible with the initial purposes;"

The first sentence of Art. 5(1)(b) consists of two parts. The first half ("*personal data must be collected for specified, explicit and legitimate purposes…*") expresses the "principle of purpose specification". Each of the three elements (the *specificity* of the purpose, its *explicit* communication to the data subject and its *legitimacy*) are important and non-negotiable requirements. The second half of the first sentence of Art. 5(1)(b) articulates the "compatibility clause" *("…and not further processed in a way incompatible with those purposes*"). Taken together the purpose specification principle and the compatibility clause constitute the principle of purpose limitation. The principle of purpose limitation expresses the basic idea that the processing of personal data should stay within the boundaries of the initial purpose defined by the data controller (the person or body who determines the purposes and means of the processing of personal data) so that the data subject (the person identifiably related to the personal data) knows what to expect and who to address with queries or complaints. This creates foreseeability based on legitimate expectations and prevents data processing getting out of bounds[16].

The first 'legal loophole' employed by the industry is the open texture of purpose specification, following from the fact that the term 'specified and explicit purpose' has not been tested in a court of law yet. Users of internet services, such as browsers or OSNs, often are asked to consent to the processing of their data for a long list of vaguely defined purposes. This renders void the prescription that purposes should be specified and explicit. When the compatibility clause is combined with an initial specification of purposes which is broad and vague, it might almost seem that everything is possible. Thus, while "collecting personal data for a specific commercial transaction with a customer, and later on deciding to export the data to another firm for the purposes of direct marketing is unlawful" (European Commission, 2012), this transfer would be lawful if the transfer were included in the initial purpose specification. How far can this provision be stretched? Working Party 29 (WP29) writes in its Opinion on purpose limitation:

> "Vague or general purposes such as 'improving users' experience', 'marketing', 'IT-security' or 'future research' will - without more detail - usually not meet the criteria of being 'specific'. However, the degree of detail in which a purpose should be specified depends on the particular context in which the data are collected and the personal data involved." (Article 29 Data Protection Working Party 29, 2013, p. 52)

[16] "Purpose specification and the concept of compatible use contribute to transparency, legal certainty and predictability; they aim to protect the data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing. The limitation should, for example, prevent the use of individuals' personal data in a way (or for further purposes) that they might find unexpected, inappropriate or otherwise objectionable. At the same time, the notion of compatible use also offers some degree of flexibility for data controllers". (Article 29 Data Protection Working Party 29, 2013, p. 11)

The boundary between 'too vague' and 'specific enough' is not always easy to draw. Is a long list of specific purposes (a company might decide to 'play it safe' and include as many purposes as possible) in accordance with the principle of purpose specification? It seems doubtful that such an overly inclusive list would be considered legitimate and fair in the sense of Arts. 6(a) and (b) DPD 95/46 (see also below, section 5.1.2) if tested in Court; however – much will depend on the particular context. Let's explore a more concrete example: is it legitimate for a company to state that the purpose of the processing includes transferring data to "corporate affiliates and affiliates' services" and selling your personal data in case of a bankruptcy or merger?[17] All major online sites such as Facebook, Twitter, Google and LinkedIn include very similar transfer clauses[18] in their terms of service. For example, Twitter states:

> "Business Transfers and Affiliates: In the event that Twitter is involved in a bankruptcy, merger, acquisition, reorganization or sale of assets, your information may be sold or transferred as part of that transaction. This Privacy Policy will apply to your information as transferred to the new entity. We may also disclose information about you to our corporate affiliates in order to help provide, understand, and improve our Services and our affiliates' services, including the delivery of ads."[19]

Such a clause may hold up in a court of law to the extent that the purpose remains the same or is found to be compatible, and insofar the Privacy Policy is indeed applied. However, in practice such transfers of data as a kind of 'assets' from one company to another will render the foreseeability of how the next company will handle the data more difficult and this may be said to go against the purpose of purpose limitation. This could be resolved by requiring a notification to the relevant data subjects, combined with a right to withdraw one's data if provided on the legal grounds of consent or the legitimate interest of the data controller. We strongly oppose a lenient approach in such cases as it renders effective protection illusionary. Instead, we argue for clear and precise rules on how to proceed when personal data are transferred as part of a package deal in the case of bankruptcy, mergers, acquisitions and reoganization or sale of assets.[20]

This brings us to the second legal 'loophole', which consists in a loose interpretation of the "compatible purposes" clause (*"…and not further processed in a way incompatible with those purposes*"), extending the legal uncertainty of the purpose limitation principle following from vaguely formulated purposes even further. If the principle of purpose specification were not complemented by the "compatibility clause", re-use of personal data (whether by the same of another data controller) would become very much constraint. Especially if the one determining the purpose changes, the purpose will easily change. Since the goal of purpose limitation is not to prohibit reuse and transfer of data but to safeguard the legitimate expectation of the data subject, the 'compatibility clause' should ensure that this expectation is not violated. A transparent relationship between data subject and data controller requires

[17] https://support.twitter.com/articles/20172501
[18] http://www.nytimes.com/interactive/2015/06/28/technology/Firesale-Listy.html?; http://www.nytimes.com/2015/06/29/technology/when-a-company-goes-up-for-sale-in-many-cases-so-does-your-personal-data.html?
[19] https://twitter.com/privacy
[20] Speaking of 'clear and precise rules' refers to the legal requirement for justification of an infringement of the fundamental rights to privacy and data protection, as stipulated by the CJEU, following the case law of the ECHR. Cf. e.g. par. 54 in CJEU, 18 April 2014, C-C-293/12 and C-594/12 (*Digital Rights Ireland v Irelan*d).

that the controller remains the only one who is in control over the data and that the processing is limited to the initial purposes.

So how is it possible that personal data seem to be transferred between different actors all the time? Why do data seem to circulate so easily on the internet? This is mainly[21] due to a broad interpretation of the aforementioned "compatible purposes" clause which states that further processing is allowed as long as the purpose is not *incompatible* with the original purpose. Further processing of data for historical, statistical or scientific purposes shall be considered as compatible with the original purpose. Here we end up in a matter of definition: for example, can market research be qualified as a scientific or statistical purpose?

> "What 'compatible' means, however, is not defined and is left open to interpretation on a case-by-case basis." (European Union Agency for Fundamental Rights, 2014, p. 69)

Clearly, industry prefers to give a broad interpretation that gives the data controller quite some freedom to process data for other purposes than the initial one (as long as these purposes are 'compatible'). The "compatibility clause" also allows for transfers between private entities as long as the purpose of the transfer is compatible with the one for which the data were initially collected and processed. We may, however, expect that once data protection legislation is appropriately enforced, data controllers will have to be more specific about reuse, turning the loophole into a safeguard instead of a vulnerability. Such enforcement is to be expected once the GDPR comes into force, but even at this moment there seems to be a momentum for holding data controllers responsible for their stewardship of personal data. This is clear from the case law of both European Courts and the case law within the Member States of the EU, notably when based on tort law, while various types of class actions have been highly successful in challenging the unfettered sovereignty that some data controllers exercize over personal data.[22]

The third 'loophole' is strictly speaking not a loophole – because it does not result in the circulation of personal data. Yet, it does result in the *semblance* of data circulating around the web, intransparency and some possibly negative effects similar to when data would actually circulate. To use an analogy: imagine that you tell your mailman not to tell

[21] All transfers for incompatible purposes are prohibited *unless* required by legislation of the Member State to which the controller is subject; for example if the processing of the personal data is necessary for carrying out a task in the public interest. This means that a provider of an online service such as Facebook or Twitter can, and sometimes even has to, transfer data to authorities or public bodies (e.g. the police or social services) for incompatible purposes if this is required by national law. Art. 13 DPD 95/46 lists that exemptions to the purpose limitation of Art 6(1) can be made in national legislation if such exemption safeguards one of the following interests: (a) national security; (b) defence; (c) public security;(d) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;(e) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters; (f) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (c), (d) and (e);(g) the protection of the data subject or of the rights and freedoms of others.

[22] See art. 73-79b GDPR, including substantial fines, tort liability and the right to be represented by a non-profit association; e.g. CJEU 18 April 2014, C-293/12 and C-594/12 (Digital Rights Ireland) and CJEU 13 May 2014, C-131/12, (Google Spain v Costeja Gonzalez), Court of Appeal of England and Wales, 27 March 2015 Google Inc v Vidal-Hall & Ors [2015] EWCA Civ 311 (confirming a privacy tort for the violation of data protection rights), available at <http://www.bailii.org/cgi-bin/markup.cgi?doc=/ew/cases/EWCA/Civ/2015/311.html> and the draft legislation pubished February 2015 by the German Government to enable class action for the violation of Data Protection rights (*Entwurf eines Gesetzes zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts*, available at <http://www.cr-online.de/36818.htm>. On the role of the ECHR in the protection of personal data in the private sector, e.g. F. Boehm, Information Sharing and Data Protection in the Area of Freedom Security and Justice (Springer 2012), 75-76.

anyone where you live and who you are. Still, you receive an abundance of letters which seem to be very specifically tailored to address you (e.g. a single mother with a low income and an interest in cars). You reproach your mailman that he has told everyone about but he cunningly replies: "*No, I did not – I just told everyone that if they wanted to sent mail to a single mother with a low income and an interest in cars, that I would gladly pass the message on*". The third 'loophole', which this analogy illustrates, is that in targeted advertising it's often not the actual data which are being sold but the *possibility to target customers with a certain profile*.[23] User profiles and data are to an OSN service like the chicken laying golden eggs: selling the data would be as silly as slaughtering the chicken. This means that the personal data of a user of an OSN service are not transferred but that ads are routed towards certain profiles without revealing the actual identity of the owners of these profiles. Thus, what is sold is targeted advertising space and not personal data. It is attractive for an OSN to buy additional data from data brokers to complement their profiles; but selling data would economically be counterproductive. Calling the business model of selling targeted advertisement space a 'loophole' might be considered controversial as it does not involve a loose or broad interpretation of a data protection requirement (as with the two other 'loopholes'). An OSN who has "targeted advertising" as one of the purposes of its processing can stay the sole data controller; and yet an end-user is addressed by ads of all kind of actors, giving the impression that her personal data are transferred. However what circulates is not the user data but a user 'profile'. We would argue that the user would benefit from more transparency regarding such business practices and that more attention could be devoted (which is partly the case in some versions of the pGDPR) to the regulation of possible adverse, discriminatory, effects of targeted ads and personalization of settings. While the business practice of companies acting through intermediaries, without access or control over the actual personal data, is clearly preferable over a practice where the actual data are transferred, this set-up might also make it more difficult for the data subject to know whom is liable for what and whom to address with complaints or questions.

[23] For example, a commercial company selling particular type of clothing might want to target pregnant women, who are older than 35 and live in Paris, Lyon and Marseille. The only information this company would get is the amount of women targeted and feedback (e.g. do women in Paris click the ad more often than the ones in Lyon?). The commercial company never gets the access to the personal data; it is the OSN who stays in control.

2.2. PDM and transparency tools

So let us now return to the question whether personal data management (PDM) solutions can be combined with third party profile transparency tools such as DataBait. It should be noted that this analysis, regarding the possibilities to combine third party transparency with PDM solutions, does *not* impact directly on the design of DataBait. The DataBait tool as developped by the USEMP project does not aim to combine the functionality of a transparency tool with a PDM solution. DataBait is "merely" a third party transparency tool – not a PDM provider.

DataBait is "merely" a third party transparency tool – not a PDM provider.

The insights provided by DataBait can make a user reconsider certain postings (by either deleting them or restricting their accessability) or block certain trackers. Such decisions might affect who knows what about the user, and thus, *indirectly*, influence the relationship between OSN and OSN user. However, DataBait does not function as a PDM intermediary between an OSN user and an OSN or other actors interested in obtaining the OSN user data. One could imagine that certain users would like the combination of a transparency tool and a PDM solution. The idea would be that subscribing to such a service would then enable users to *granulary* license their data in exchange for profile transparency mediated through a

Users might like the combination of a transparency tool and a PDM solution if this tool could (1) provide for an easy way to translate transparency insights in actions with regard to user permissions, and ensure (2) that user data can only be accessed according to the user permissions ('granular licensing'), and (3) that any transfer happens under the same conditions as the ones guiding the relationship between the user and the PDM/transparency tool provider: any further use of user data would only be allowed in exchange for profile transparency.

third party transparency tool provider. Thus, the PDM/transparency tool provider would have to provide, firstly, for an easy way to translate transparency insights in actions with regard to user permissions (e.g., "*If information about my sexual preference can be inferred from this holiday picture, it is not allowed to use it for insurance purposes*[24]"), secondly, ensure that user data could only be accessed according to the user permissions and, secondly, under the same conditions (this would involve a tranferrable clause) as the ones guiding the

[24] It should be noted that using Facebook data for to decide for insurance purposes is not allowed by Art. 3(15) of Facebook's Platform policy. Also see: https://www.theguardian.com/money/2016/nov/02/facebook-admiral-car-insurance-privacy-data (last accessed 2 November 2016).

relationship between the user and the PDM/transparency tool provider: any further use of user data would only be allowed in exchange for profile transparency. For example, a user could specify that *nobody is allowed to use her data about religion; however, her health data can be used for cancer research – but definitely not for insurance purposes.* The transparency function of the service would show which (seemingly innocuous data, such as posts or photos) could actually be relabeled as containing health or religion related information. The PDM function of the service could then be that a research institute doing cancer research could be given access to the user data under the condition that they would sign a new DLA with the user (stating that in exchange for the use of the data, first party as well as third party profile transparency will be provided).

However, a PDM/transparency solution is legally highly problematic as the purpose limitation principle prohibits any blank checks with regard to how data may be used. Moreover, it would put the independent position of DataBait at risk. The empowering strength of DataBait lies exactly in its position as an independent provider of transparency, not as a mediator between users and businesses/organisations looking for user data. Finally, why would users trust a minor actor with their data? And what incentive would they have to share data beyond what they already share with the OSN and OSN applications?

However, such a PDM/transparency solution is highly problematic in terms of the purpose specification and limitation principle as this principle prohibits any blank checks – even limited blank checks! – with regard to how data may be used. A granular 'license' would merely function as a marker for any data controller wishing to process data: "This individual is probably (not) interested in processing of data types X, Y, Z for purposes A, B, C". The data controller still would need to specify the purpose of the processing and ask for user consent, or at least inform the user (if the ground for the processing is not consent but, e.g., a contract or the legitimate interest of the controller). An individual cannot be bound to consent based on a granular license.

Moreover, in terms of a viable role within the business niche PDM/transparency solution would also be very problematic as it would put the independent position of DataBait at risk. The empowering strength of DataBait currently lies exactly in its position as an independent provider of transparency, not as a mediator between users and businesses/organisations looking for user data. It is also hard to imagine what the incentive for organisations and users would be to use a mediating transparency provider and why this provider would want to take on the large responsibility for preserving the data secure and provide transparency. Also, it is difficult to imagine why a user would like to share data *beyond* what is already shared with the OSN, DataBait and applications running on the OSN platform. Sharing data with an OSN is for most users a necessary evil: you give access to data that are necessary for the service to function and in addition you also "pay" with your

data (allow for their commercial exploitation) for the OSN service you want to use. The same goes for many apps even though Facebook tends to reject applications that ask for unnecessary permissions[25], especially after public indignation in 2010 about the amount of collected information by many apps[26]. Sharing data with the DataBait provider is a clear *quid pro quo*: the user provides her data (the *quid*) and gets third-party profile transparency about what an OSN could know about her (the *pro quo*) in return. We do not see a similar clear motivation *why* DataBait users would like to share their data with any other parties than the OSN, DataBait and the other apps running on the OSN which they have installed. Of course there might be DataBait users who want to be "data altruists" (« *Use my data for cancer research, to make the world a better place* ») and who combine this desire with a distrustfulness of direct data transfers or transfers mediated only through the Facebook Platform (*« I would like to use my PDM intermediary for this altruistic donation of data ; the intermediary will help me ensure that I sign a DLA with the research institute to whom I provide my data ; this DLA will state that they provide me with profile transparency in exchange for the use of my data ; I consider such a contractual clause to be more solid than the profile transparency a data processor has to provide me based on Data Protection law*»).

However, given the drawbacks (*Is the security of the data not better guaranteed by Facebook than an independent, third party PDM provider ? What is the gain in sharing more data through the PDM provider?*) it seems to us that this 'niche' of users is likely to be rather small. Nevertheless the idea of granular licensing should not be discarded completely. Some OSNs might embrace[27] the idea to allow some form of permission management to give the users a sense of control and get better data. However, this would probably not include the particular *quid pro quo* on which our granular licensing model is based: access to data in exchange for contractually specified profile transparency. Such *quid pro quo* granular licensing might work in a specific context (for example in a medical environment, where the patient is given the power to set limits on to which medical professional has access to which data) but not in the current way DataBait is created (aiming to empower users who make use of the services of large OSNs or browsers).
Thus, in the remainder of this section we explore how a contractual *granular licensing system* could be a form of DPbD with regard to the requirements of purpose specification and transparency with regard to the processing. By offering a set of default forms of permitted uses of personal data from which the data subject can choose –a concise, pre-set, and transparent 'menu' of options- the purpose of the processing would no longer be a singular offer made by a data controller for the data subject to consent to or reject.

[25] https://developers.facebook.com/docs/apps/review#selectitems (last accessed 1 Augustus 2016)
[26] http://arstechnica.com/tech-policy/2010/10/many-faceook-apps-found-to-be-collecting-selling-user-info/ last accessed 1 Augustus 2016)
[27] For example, Facebook already allows users to adjust advertisement interests. Permission management fits in this way of approaching users. A user who corrects her data and actively states which advertisers are allowed to contact her is a valuable asset in terms of advertisement.

OSNs might embrace the idea to allow some form of permission management to give the users a sense of control. However, this would probably not include the particular* quid pro quo *on which our granular licensing model is based: access to data in exchange for contractually specified profile transparency. Such quid pro quo granular licensing might work in a medical environment, where the patient is given the power to set limits on to which medical professional has access to which data

2.3. Granular licensing

As noted above, when applied in an OSN setting, third party tools that combine a PDM and transparency functionality are problematic both from a legal (the purpose limitation principle does not allow for data licenses that function as blank checks) and from a business perspective (it is unclear to which "need" such a tool would be the answer). However, we believe that in some situations tools that combine a PDM and transparency functionality could actually be useful and stay within the limits of the purpose limitation principle. Imagine, for example, a hospital wanting to re-use data of patients for purposes that differ from the ones for which they were initially collected: such as the monitoring health, improving the quality of care, development of better treatments and pharmaceutical drugs, etc. One could think here of data gathered in the hospital (blood pressure, temperature, etc.) that are used outside the treatment setting (e.g. for the development of a drug or treatment by a pharmaceiutical company) or data gathered outside the hospital (browsing data, OSN data, fitness apps etc.) that the user would like to share with the hospital under very particular circumstances (e.g., when a patients ends up in a sudden coma; knowing what the user was doing in the days before could sometimes help a diagnosis). Here a user might granulary license.

In such a setting a PDM/transparency tool would combine two functionalities:

Granular licensing of personal data consists of two aspects:

(1) A particular **permission system** in which the user can express preferences as to the types of data and data processing;

(2) Contractual data licensing in exchange for (contractually defined) profile transparency – all of this mediated through an independent third party.

(1) *Permission management:* data controllers (in this case: medical professionals) could refine the processing purpose in mutual agreement with their end-users (not through "consent" to a standard, and not through individually negotiated contracts but, for example, through a mutual agreement in which the end-user would have several options of licensing her data for particular options for sharing and targeting) and in a more standardized and transparent way (e.g. "You license us to use your data according to standardized license X"); this "permission system" would not contain any "blank checks" but indidications of the types of processing purposes permitted by the data subject (the patient);

(2) *Contractual data licensing in exchange for (contractually defined) profile transparency:* the licensed data would be provided by the user in exchange for contractually defined profile transparency (*a quid pro quo*). The transaction could takes place through an independent third party PDM/transparency provider. Users could adjust their licensing settings based on information about what happens to their data, who accessed it and about what can be inferred from their data.

Co-involving data subjects through a permission system and licensing data in exchange for profile transparency could also help in channeling the ways in which the aforementioned legal 'loopholes' (section 2.1) are used to be in better accordance with the original rationale of the purpose limitation principle. This could also be beneficial for data controllers: data

subjects who are co-involved in deciding on the purpose of the processing through a granual licensing system are likely to be more motivated to ensure that their data are accurate. An empowered data subject, who is a party to a mutal agreement with regard to how her data is used and who has active knowledge of the processing of her data, will feel a bigger involvement in the processing of her data than a data subject who has consented in a take-it-or-leave-it manner and is kept in the dark about the personal data "economy" taking place "through the looking glass". If data subjects were more actively engaged in caring for the quality of their data, data controllers would be able to base their marketing, targeting, personalization and risk assessment decisions on more accurate and up-to-date information. A granular licensing system would thus benefit both data subjects and controllers.

In section 2.3.3 we clarify the contractual *quid pro quo* part of our proposed granular licensing system: profile transparency in exchange for data. In section 2.3.1 and 2.3.2 we clarify what kind of “permission system” we envision by drawing two analogies. The first analogy is with the way in which WP29 (Article 29 Data Protection Working Party, 2012) proposes to understand the requirement of the cookie consent following Art. 5(3) from e-Privacy Directive 2002/58/EC. The second analogy is with the way *Creative Commons* licenses[28] for copyright protected works function.

2.3.1. Lessons from cookie consent.

Since the EU adopted new cookie legislation in the form of Art. 5(3) of the e-Privacy Directive (Directive 2009/136, amending Directive 2002/58/EC), making it mandatory for websites to request the prior consent before placing cookies on a users’ computer or reading them back, internet users who want to access a website often have had to make the empty gesture of accepting cookies as a precondition for accessing the website. As WP29 has shown (Article 29 Data Protection Working Party, 2012) such a binary request for cookie consent ("either you accept all cookies, or access is denied to you") twarths the rationale of Art. 5(3) of the e-Privacy Directive, which builds on a distinction between functional cookies (for which no prior consent is required) and non-functional cookies (for which prior consent should be requested).

> "Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user." (Art. 5(3) of the e-Privacy Directive 2002/58/EC)

Art. 5(3) of the e-Privacy Directive does not intend to create an unnecessary extra hurdle for internet users, but sets out to give internet users a real choice in refusing cookies which are not necessary for the performance of the service requested by the internet user (such as

[28] https://creativecommons.org/licenses/?lang=eng

tracking cookies for a service which does not have tracking as its core functionality). There are between two types of functional cookies:

1. technical cookies that have "the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network
2. functional service cookies that are "strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".

The distinction between functional and non-functional cookies could be used in an analogous way to make a distinguish between "functional" processing of data, i.e. necessary for the processing purpose of a service, and additional processing, i.e. beyond the strict processing purpose (e.g. any sharing of data with other parties or offering third parties the possibility to target users based on their profile, in as far as this does not strictly contribute to the service requested by the user).

A granular license clause with regard to personal data could offer the data subject an option to “negotiate” or “choose”, within the limits of the law and the broader boundaries of the purpose as defined by the data controller, how and for what purposes her data can be used. It should be underlined that the outer boundaries of this choice will always be delineated by the specific, explicit and legitimate purpose set out by the data controller. It would make no sense if an medical professional, would state a processing purpose (e.g. “*Monitoring health progress of the patient; access is given to all directly involved nurses*”) and the data subject could go *beyond* these limits (e.g. “*I would like my data to be processed for the purpose of achieving peace in the Middle East*”). However, within the boundaries of a specific, explicit and legitimate purpose there might be room for “choice” or “negotiation”, which could benefit both the data subject (end-user) and the data controller (service provider).

A granular license clause with regard to personal data could offer the data subject an option to “negotiate” or “choose”, within the limits of the law and the broader boundaries of the purpose as defined by the data controller, how and for what purposes her data can be used. It should be underlined that the outer boundaries of this choice will always be delineated by the specific, explicit and legitimate purpose set out by the data controller.

When a data controller defines her purpose, there is, firstly, the processing purpose as strictly necessary for the performance of the service requested by the user. Here there is no room for negotiation or choice for the data subject; it is the data controller defining the use of the data. However, the controller can also define additional purposes, not strictly necessary for the performance of the service requested by the user, which involves *sharing* user data with third parties (e.g. a pharmaceutics company, a research institute or a marketing company) or allowing the data controller and/or third parties to *target* users with a certain profile (e.g., patient with a history of breast cancer). It is in these three latter categories (i.e., sharing data with third parties, targeting by data controller, targeting by third

parties) that we believe there is room for 'choice' and 'negotiation'; and, consequently for the granular licensing of personal data which we propose in this chapter.

Building on the analogy with the differentiation between functional and non-functional cookies, one of the choices offered to the data subject could be to exclude any processing which is not strictly necessary for the service, or to offer an even more fine-grained system in which the user can exclude some of the not strictly necessary processing actions while preserving others.

To get even more of a sense of how a system of standardized licensing options could be realized we turn in the next section to our second analogy, namely with Creative Commons licenses.

2.3.2. Lessons from Creative Commons licensing.

The word 'licensing' is strongly associated with intellectual property, such as licensing copyright protected content. However, the majority of personal data does not qualify as copyright protected content. The subject matter protected under copyright is not uniformly defined[29], but one can broadly say that in order to be a copyrightable, the subject matter should be "original" or the author's own "intellectual creation"[30] and reflect the author's personality[31]. More specifically, this is the case if the author was able to express her creative abilities in the production of the work by making free and creative choices[32]. An author can give a license that allows for the reproduction or publication of this IP content.

However, it is important to underline that the licensing system we propose would not only cover IP content ('IP licensing') but the licensing of any personal data. To 'license' basically just means "to give permission to"; it means "granting (a person) a licence or authoritative permission to hold a certain status or to do certain things"[33]. Consequently, the granular Personal Data Licensing (gPDL) approach, which is inspired by Creative Commons licenses (which are IP licenses, not licenses with regard to other information), does itself not have anything to do with IP licensing or copyright protection as such[34].

The granular Personal Data Licensing (gPDL) approach we propose would not only cover IP content ('IP licensing') related to an identifiable person, but the licensing of any personal data.

[29] Copyright is granted at the national level and is regulated in national laws but many harmonisation efforts have been made at the international and European levels.
[30] Judgment in *Infopaq International A/S v Danske Dagblades Forening*, C-5/08, ECLI:EU:C:2009:465, para. 37.
[31] Recital 17 in the preamble to "Council Directive 93/98/EEC of 29 October 1993 harmonizing the term of protection of copyright and certain related rights" , *O.J. L 290 , 24/11/1993 P. 0009 – 0013 ;*
[32] Judgment in *Eva-Maria Painer v Standard VerlagsGmbH and Others*, C-145/10, ECLI:EU:C:2011:798, para. 89.
[33] See Oxford English Dictionary, http://www.oed.com/
[34] Moreover, it should be noted that CC licenses work worldwide, because copyright relies on old international treaties, which have harmonised important parts of copyright protection worldwide; this is translated in CC licences that are reviewed and adapted per national legal order. Because data protection is not as universally harmonized, the gPDL approach will be especially useful when the processing is limited to the EU. However, as a "good practice" it could also spread beyond the EU.

What we take from the Creative Commons licensing system and what we transfer to our granular licensing system of personal data is (a) the non-dogmatic, problem-oriented and pragmatic approach in creating licenses, (b) a comprehensive, standardized and transparent set of licenses specifying how a piece of data can be used, (c) using a layered format for the licences (a layer specifying the legal intricacies, a layer which can be easily grasped by a lay person and a machine readable layer). Let us elaborate on these three aspects.

1.

A first aspect we adopt in our granular personal data licensing (gPDL) system is the non-dogmatic, problem-oriented and pragmatic approach of the Creative Commons movement. Creative Commons (CC) licenses where not developed as from an ivory tower but in direct response to a concrete (societal) *problem*, namely how to stimulate the free circulation of content while preserving the system of copyright protection, and the need to come up with a solution to this problem. The six CC license types which currently exist have been created over time, in a bottom-up way. These CC licenses have resulted in a growing "pool of content that can be copied, distributed, edited, remixed, and built upon, all within the boundaries of copyright law"[35], thus stimulating the dissemination of knowledge and creativity. Thus, if we use with Creative Commons as an analogy, the first step towards developing a gPDL system has to be based in defining the concrete need or problem we are trying to address. However, an important *problem* which gPDL tries to solve is rather opposite in nature to CC: how to restrict the uncontrolled and opaque diffusion of personal data. In this sense the goal is to come to what we can tentatively call a "personal anti-commons" (PAC). This does not mean that gPDL opposes all circulation of data (after all, it is very well possible that the data subject wants her data to be re-used in a particular way); but it does oppose *opaque* circulation of data (where the data subject does not know who has access to her data and what happens to them). In the light of the failure of the purpose limitation principle in this regard, one way to address this problem is to create a system where the way in which personal data are used is a matter of mutual agreement between data controller and data subject, and less of an idiosyncratic, one-sided offer – to which the data subject can merely consent or not. The lack of such a situation is the *need* which our gPDL addresses.

Granular Personal Data Licensing does not oppose all circulation of data, but it does oppose* opaque *circulation of data data (where the data subject does not know who has access to her data and what happens to them).

2.

A second aspect we adopt in our gPDL system is a comprehensive, standardized and transparent set of licenses specifying how a piece of personal data can be used. After all, it is not realistic to expect data subjects in their dealings with a large hospital to enter into

[35] https://creativecommons.org/licenses/?lang=eng

individual negotiations. A large institution is unlikely to have the resources to negotiate terms with users on an individual basis – it would merely create an enormous work load. Moreover, most individual users (patients) will lack motivation or knowledge to negotiate individual terms.

However, if a limited set of standardized and openly scrutinized personal data licenses existed, users (gaining empowerment and transparency about what happens to their data) and the institution/business (gaining transparency about what is allowed with data and possibly more accurate data due through user engagement) might be interested in using them. Public institutions and industry could try to "seduce" the user to grant them a very permissive license (e.g. by offering additional services), but at least the standardization of the licenses would offer the user more transparency about the "cost" of this deal in terms of personal data usage and lead to better informed decisions. Even more safeguards for transparency could be offered if these licenses would be provided by an independent platform, informing users of the "costs" in terms of privacy and data protection of providing very broad licenses.

If a limited set of standardized and openly scrutinized personal data licenses existed, users (gaining empowerment and transparency about what happens to their data) and the institution/business (gaining transparency about what is allowed with data and possibly more accurate data due through user engagement) might be interested in using them.

So what kind of standardized licenses would be useful? When we have a look at the CC approach to licensing, we see that the solutions to IP problems are reduced to a few basic conditions, which we can call the "license atoms", and the combinations of these. Currently there are six CC license types, which build on three basic distinctions. The first two distinctions are commercial versus non-commercial and derivative versus non-derivative (i.e. no modification of the original work) use. These two distinctions have even been integrated in Google image search where you can filter your results according to the following five 'usage rights' types: (a) not filtered by license, (b) labeled for reuse, (c) labeled for commercial reuse, (d) labeled for reuse with modification, (e) labeled for commercial reuse with modification. The third distinction underlying CC licenses is whether or not derivative works, based on works licensed under a CC license, have to be licensed under the same licensing conditions as the original work. This is called "share alike". Furthermore, each of the six CC licenses has the basic condition of attribution ("CC BY"), which means that you mention the author of the original creation. This results in the following six licenses[36], ordered from the most accommodating license (the "*CC BY*" license: "lets others distribute, remix, tweak, and build upon your work, even commercially, as long as they credit you [the author] for the original creation") to the most restrictive one (the "*CC BY-NC-ND*": "only allowing others to download your works and share them with others as long as they credit you [the author], but they can't change them in any way or use them commercially"):

[36] License images reproduced from: https://creativecommons.org/licenses/?lang=eng

Attribution
CC BY

Attribution-ShareAlike
CC BY-SA

Attribution-NoDerivs
CC BY-ND

Attribution-NonCommercial
CC BY-NC

Attribution-NonCommercial-ShareAlike
CC BY-NC-SA

Attribution-NonCommercial-NoDerivs
CC BY-NC-ND

What kind of default licenses (i.e, pre-set licensing settings) would make sense for mutual agreements with regard to re-use or sharing of personal data, based on the initially specified purpose or one that is compatible? Before proposing a set of gPDLstandardized licenses it is good to note that the CC licenses have been created over time, in a bottom-up way. Our proposal should therefore also be seen as a first step in a long debate. A second caveat is that the licensing would have to stay within the limits of the purpose set out by the data controller and of EU data protection law. For example, it would not be possible for a data controller and data subject to come to the agreement that the data subject will give an open license allowing data use for an unspecified set of purposes, because this would be at odds with the purpose limitation principle (Art. 5 GDPR).

The data subject should have the possibility to exclude any processing which is not strictly necessary, and to exclude the use of any inferred data (that are not strictly necessary).

We think that the data subject should have the possibility to exclude any processing which is not strictly necessary for the requested or necessary service (most likely: a

particular treatment). In section 2.3.1 we distinguished: sharing data with third parties, targeting by data controller, targeting by third parties. Moreover, we think it would be good if users have the possibility to exclude the use of any data that were "derived" or "inferred" (unless they are necessary for the performance of the requested or necessary service).

3.

A third aspect we propose in our gPDL system is a layered format for the licences: a layer specifying the legal intricacies, a layer which can be easily grasped by a layperson and a machine readable layer. This is what would make the license *granular* in a second sense[37], that is, operating on three levels of details and with three different 'audiences' in mind. When we enumerated the six CC licenses (see above) we only reproduced the human readable layer: an iconic depiction and a set of abbreviations.

The gPDL system would look very much like the CC licensing system. Like in the CC licensing system, each license would consist of a layer of "legal code", of human readable icons and text and machine-readable tags.

Like in the CC licensing system, in a gPDL system each license would consist of a layer of "legal code", of human readable icons and text and machine-readable tags.

The layer of « legal code » is pretty straightforward – it is the traditional legal formulation of a license. The human and machine readable layers require more creative thinking. The human readable layer is the "common sense" layer, consisting of a user friendly interface of human understandable *text* and *icons* (which could actually be considered as two sublayers). Here legal options are translated and communicated to the user in an understandable way. This also correlates with a series of transparency obligations introduced in the new GDPR, on the data controller for providing transparent information and communication and for effective procedures and mechanisms. First, the controller needs to offer "transparent and easily accessible policies" for the exercise of the data subject's rights, and for the processing of personal data in general. Furthermore any information and communication with regard to the processing of personal data has to be provided "in an intelligible form, using clear and plain language, adapted to the data subject, in particular for any information addressed specifically to a child' (article 11.1-2 GDPR).[38] Here social sciences like media studies can be very relevant giving shape to this "accessibility" and "intelligibility" of these communications.[39]

Then there is the machine readable layer[40] : this is the technological layer. Wouldn't it be great if sets of personal data or individual pieces of personal data would be tagged in

[37] The first granularity is the break-down in different options for data handling by the data controller, instead of 'all-or-nothing' consent.

[38] See the discussion in Heyman, R., van Dijk, N., Who can Afford Users as Targets? Interfaces, Transparency and the Commodification of Relations in Online Social Networks, Report on differences between user and legal perspectives on privacy and profiling (D3.3.1). EMSOC Project. 2013, at: http://emsoc.be/wp-content/uploads/2013/11/D322-SMIT-and-LSTS.pdf

[39] One possibility is to experiment with the idea of *mental models* of privacy and data protection in this case. See Camp, L. J., (2009) Mental Models of Privacy and Security, IEEE Technology and Society Magazine.

[40] See also the W3C work done in the past as part of P3P initiative http://www.w3.org/P3P/

such a way that one could easily filter personal data according to the kind of permitted uses ? In the case of content licensed with a CC license there is a kind of digital marking of copyrightable works with the content usage policy, travelling with it. This could also be done with regard to personal information, though the tagging would probably be easier at the level of a set of data than tagging each individual data piece. The data controller (the hospital) would have to implement this or facilitate the creation of such tags.

2.3.3. gPDL's *quid pro quo*: access to data in exchange for profile transparency.

In the two previous subsections we presented our gPDL system as a sort of permission management system: a user sets limits as to the context in which data can be used. Although we used a hospital setting as an example for such a permission system, permission systems as such an be applied in many settings. As noted earlier in this chapter, OSNs are likely to create some form of user settings control panel and/or permission management with regard to their profiling processes, because this can give the users a sense of control and help the OSN in obtaining better data. The permissions could be part of the service contracts between data controllers (aka service providers) and data subjects (aka end users of a service). This means that a data subject who chooses very restrictive permissions might simply be denied to use a service. The purpose and ways of the processing personal data are determined by the data controller; a permission system could make the controller negotiate with the user, but the licensing of personal data cannot be a one-sided affair of the subject of those data (the data subject).

However, the inclusion of user permission settings in a contract between OSN and OSN user does not suffice to call it a gPDL system. It can only be called a gPDL system if it also includes the particular *quid pro quo* on which our particular granular licensing model is based: access to data in exchange for contractually specified profile transparency. Such *quid pro quo* granular licensing might work in a specific context (for example the aforementioned medical environment, where the patient is given the power to set limits on to which medical professional has access to which data). Here the granular personal data licences could be mediated through an independent PDM/transparency tool provider (for example, a third-party commercial provider, an NGO, a private nonprofit organization with a public goal, or a scientific consortium). In this particular context an independent third party, acting like an intermediary or very special type of 'data broker' (whose purpose is to support EU end-users in the exercise of the data protection rights), could leverage the field between large health service providers and end-users[41] by ensuring that no more data than strictly necessary are provided and that the data subject gets contractually stipulated profile transparency in return.

[41] In previous work from W3C (P3P) the user agent (browser) would enforce a policy dictated by the the user by filtering out data but this was meant for web browsing data; not data explicily shared via OSNs or in a medical setting. See: P3P initiative http://wwww3.org/P3P/

An independent third party, acting like an intermediary or very special type of 'data broker' (whose purpose is to support EU end-users in the exercise of the data protection rights), could leverage the field between large health service providers and end-users by ensuring that no more data than strictly necessary are provided and that the data subject gets contractually stipulated profile transparency in return

3. 'Sensitive personal data' and 'anonymisation'

The third strand of research in this deliverable gives *a legal clarification* of which data should be considered *'sensitive'* in the sense of Art. 8 DPD 95/46[42] (or Art. 9 GPDR[43]), and which data can be considered *anonymous* (i.e., not personal data and therefore outside the scope of DPD 95/46) and shows how our clarification of these two contentious legal notions would translate into DPbD requirements.

What makes both notions ambiguous in their practical application is that they both contain an element of *possibility* or, almost Aristotelian, *potentiality*. In the same sense as Aristotle would say that an acorn should be understood as a potential oak and the boy as a potential man –they just have to realize their potential nature – some data could be classified as sensitive or personal, not because this is what they are now, but because of their potential of becoming such. Thus, in order to decide whether a piece of data should be qualified as *sensitive* personal data (and thus be treated with additional care, compared to 'ordinary' personal data) or whether a piece of data should be qualified as *anonymous* (and thus not be handled in accordance with data protection requirements which only relate to personal data) it is not enough to look at them at their face value. In order to assess whether a piece of data is personal or not, one has to assess whether there is a potential for a piece of anonymous data to be de-anonymized (turning it into personal data).

In the same sense as Aristotle would say that an acorn should be understood as a potential oak and the boy as a potential man –they just have to realize their potential nature – some data could be classified as sensitive or personal, not because this is what they are now, but because of their potential of becoming such.

3.1. Anonymous data?

In its Opinion on anonymization techniques (Article 29 Data Protection Working Party, 2014) Working Party 29 describes randomization and generalization as the anonymisation techniques which are applied most widely. The Opinion assesses the robustness of each technique based on three criteria:

(i) Is it still possible to single out an individual ? Singling out is the possibility to isolate some or all records which identify an individual in the dataset.

[42] Art. 8 (1) of DPD 95/46: "Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life."
[43] Art. 9 (1) of the pGDPR: "The processing of personal data, revealing: race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited."

(ii) Is it still possible to link together multiple records related to an individual ? Data are considered 'linkable' when it is possible to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases).

(iii) Can information be inferred concerning an individual? Inference is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.

Thus in assessing whether data are anonymous, it is not enough that data are not directly related to an identified or identifiable person, because the possibility of singling out, re-linking and inferring information should be taken in to account.

In assessing whether data are anonymous, it is not enough that data are not directly related to an identified or identifiable person, because the possibility of singling out, re-linking and inferring information should be taken in to account.

We follow the opinion of Working Party 29 (Article 29 Data Protection Working Party, 2014), and conclude that only data which, taking into account *all the means likely reasonably to be used*[44], cannot be de-anonymized can be qualified as anonymous. The standard of '*all the means likely reasonably to be used'* is a very high one (Article 29 Data Protection Working Party, 2014), meaning that data which have any reasonable potential of being de-anonymized should not be considered anonymous but as pseudonymous[45] personal data, that is, as data with a "potential identifiability" (p. 8) and as such fall within the scope of Data Protection law.

> "Data controllers often assume that removing or replacing one or more attributes is enough to make the dataset anonymous. Many examples have shown that this is not the case; simply altering the ID does not prevent someone from identifying a data subject if quasi-identifiers remain in the dataset, or if the values of other attributes are still capable of identifying an individual. In many cases it can be as easy to identify an individual in a pseudonymised dataset as with the original data. Extra steps should be taken in order to consider the dataset as anonymised, including removing and generalising attributes or deleting the original data or at least bringing them to a highly aggregated level" (Article 29 Data Protection Working Party, 2014, p. 21)

Full anonymization will often be not easy, because the technological possibilities for de-anonymization abound and are constantly increasing. The Working Party stresses that no anonymization technique is devoid of shortcomings per se. Thus, the rule of thumb in

[44] Recital 23 of DPD 95/46 states: "..to determine whether a person is identifiable, account should be taken of *all the means likely reasonably to be used either by the controller or by any other person* to identify the said person" (*italics ours*) See similarly Recital 26 of the pGDPR.

[45] "'pseudonymous data' means personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution", Art. 4(2a) pGPDR.

assessing whether data are anonymous is straightforward: *any* reasonable[46] potential for de-anonymization disqualifies data from being labelled as anonymous and brings them within the scope of data protection law[47]. The difficulties in the qualifying whether data is anonymous do not lie in the qualification rule as such (*every* potential for de-anonymization disqualifies the qualification of anonymity), but in the almost impossible task of having an overview of all the technological possibilities for de-anonymization and of all other existing data-sets which could be combined in such ways that de-anonymization becomes possible[48].

The analysis of Working Party 29 leads to the conclusion that many of the widely used techniques actually result in pseudonymization[49] instead of anonymization because some re-identification might still be possible. Real anonymization is only possible if "the prerequisites (context) and the objective(s) of the anonymisation process [are] clearly set out in order to achieve the targeted anonymisation […]. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, […].

Finally, data controllers should consider that an anonymised dataset can still present residual risks to data subjects. Indeed, on the one hand, anonymisation and re-identification are active fields of research and new discoveries are regularly published, and on the other hand even anonymised data, like statistics, may be used to enrich existing profiles of individuals, thus creating new data protection issues. Thus, anonymisation should not be regarded as a one-off exercise and the attending risks should be reassessed regularly by data controllers."

The USEMP project will not anonymize the data at the end of the project, but simply delete them (see details in table 1). By deleting the data, difficult questions about the potential for reidentification can be avoided. However, one could imagine other, similar projects, in which it turns out that the value of the data gathered makes it important to preserve the data in anonymized form. The deletion of the USEMP data will be performed in accordance with the implications following from the *Rijkeboer* decision of the EU Court of Justice[50], that is, deletion or anonymization of data should not interfere[51] with the data

[46] In assessing what is to be a reasonably likely potentiality, "[i]mportance should be attached to contextual elements: account must be taken of "all" the means "likely reasonably" to be used for identification by the controller and third parties, paying special attention to what has lately become, in the current state of technology, "likely reasonably" (given the increase in computational power and tools available)."" (Article 29 Data Protection Working Party, 2014, p. 6) For an empirical example of how seemingly anonymized data have been de-anonymized, see for example work on Netflix: (Narayanan & Shmatikov, 2008).

[47] The extent to which pseudonymous person data should be protected with a 'lighter' regime of data protection than 'ordinary' (non-pseudonymous) personal data, is still a topic that is fiercely debated.

[48] See also: (Ohm, 2010).

[49] The European Parliament's version of the proposed General Data Protection Regulation introduces this notion of pseudonymous data, which it defines as "personal data that cannot be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and subject to technical and organisational measures to ensure non-attribution." (art. 4.2a GDPR)

[50] CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, 7 May 2009. Online available at: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7

[51] Working Party 29 writes in this regard: "It should also be emphasized that anonymisation has to be held in compliance with the legal constraints recalled by the European Court of Justice in its decision on case C-553/07 (College van burgemeester en wethouders van Rotterdam v M.E.E. Rijkeboer), relating to the need to retain the data in an identifiable format to enable, for instance, the exercise of access rights by data subjects. The ECJ ruled that "*Article 12(a) of the [95/46] Directive requires Member States to ensure a right of access to information on the recipients or categories of recipient of personal data and on the content of the data disclosed not only in respect of the present but also in respect of the past. It is for Member States to fix a time-limit for storage of that information and to provide for access to that information which constitutes a fair balance between, on the one hand, the interest of the data subject in protecting his privacy, in particular by way of his rights to object and to bring legal proceedings and, on the other, the burden which the obligation to store that information represents for the controller*." (Article 29 Data Protection Working Party, 2014, p. 8)

subject's right to access of her data following from Art. 12(a) DPD 95/46. It seems to us that the implications of the *Rijkeboer* decision[52] for the anonymisation and deletion of the USEMP data do not seem to interfere with deletion within three months after the end of the project (as stipulated in the DLA) : after all, all the historical DataBait data are merely copies of the user's Facebook (and possibly browser) data, and the inferred DataBait data are not used for any real life decisions.

According to the* Rijkeboer *decision of the EU Court of Justice deletion or anonymization of data should not interfere with the data subject's right to access of her data.

Similarly, the upcoming Directive on Digital Content[53] (which regulates digital content provided in exchange for a price or for a non-monetary counter-performance, such as the provision of not strictly necessary personal data; art. 3(1)) stipulates that

> "the supplier shall provide the consumer with technical means to retrieve all content provided by the consumer and any other data produced or generated through the consumer's use of the digital content to the extent that data has been retained by the supplier. The consumer shall be entitled to retrieve the content free of charge, without significant inconvenience, in reasonable time and in a commonly used data format;" (Art. 13(2))

However, the Directive is not applicable to DataBait because all data processed by the USEMP consortium are "strictly necessary for the performance" of the DLA "and the supplier does not further process them in a way incompatible with this purpose" (Art. 3(4)). As such the requirements of Art. 13 (2) sub b and c, Art. 15(2) sub b, and Art. 16(4) a and b do not apply and need not to be taken in consideration when deleting user data.

[52] See for a recent application of the *Rijkeboer* decision by the Dutch court of The Hague (1 September 2015, case number 200.162.134/01, online available at: http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:GHDHA:2015:2332), in which telecom provider KPN was held liable for infringing on the right to access and had to pay damages for deleting a history of text messages of one of their customers, as these data constituted crucial evidence which would probably have allowed this customer to win a court case which he lost due to the lack of these data. From April 2010 onwards the customer had requested KPN access to these data on several occasions. The most recent request of the customer was dated 10 April 2014. However, KPN did not respond to any of these requests and deleted the data in May/June 2014. See for a commentary (in Dutch) of this case: http://dirkzwagerieit.nl/2015/10/02/kpn-draait-op-voor-schade-wegens-onrechtmatig-verwijderen-persoonsgegevens/

[53] *Proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content* COM/2015/0634 final - 2015/0287 (COD).

The Directive on Digital Content is not applicable to DataBait because all data processed by the USEMP consortium are "strictly necessary for the performance" of the DLA. Consequently, the requirements regarding the deletion of user data stipulated in this upcoming Directive do not apply.

One other important point to keep in mind is that when a consortium like USEMP shares any anonymised data with other (scientific) interested parties, these data cannot be considered anonymised if the consortium still has the identifying information. This means that any sharing of anonymized data was not be possible during the project (while USEMP still had identifying information). Theoretically data could be shared anonymously after the project has ended and the consortium itself has deleted all identifying information and has only has preserved anonymised data. However, given that all data are deleted this theoretical scenario will not be realized.

Personal data processed in the USEMP project, ordered according to source:	**Premise**	**Deletion/anonymization/pseudonymization? (if, when)**
A. Personal data collected with the DataBait OSN app	*All personal data processed in the USEMP project are stored at HWC; next to that some small, pseudonymized subsets are stored at CERTH, VELTI and iMinds.*	*All personal data processed in the USEMP project will be deleted at the end of the project. During the project no anonymization/pseudonymization techniques are applied, apart from the pseudonymization of the subsets provided to CERTH and VELTI.*
B. Personal data collected with the DataBait browser plugin		

C. Personal data collected in the DataBait surveys in the pre-pilot. D. Personal data *inferred* from a subset of the data collected through the OSN app [A] and the browser plugin [B] E. Personal data in training and testing sets, used to train and test classifiers	*Additional clarification:* 1. All data are stored at HWC. 2. HWC will, however, provide CERTH[54], VELTI[55] and iMinds[56] with a set[57] of pseudonymized[58] data from the pre-pre-pilot for temporary usage at their own premises. 3. CERTH and VELTI have remote access to backend servers for integration which gives indirect access to imagery data stored on the system, as well as indirect access to the social media stores. 4. CEA has remote access to the backend server, which also allows indirect access to social media data and imagery data.	*Additional clarification:* 1. At the end of the USEMP project HWC deletes all data - outside the project they have no use for such data, and even with anonymisation or pseudo-anonymisation there still would be a risk in holding such data. 2. During the project there are no plans to anonymise or pseudonymise the data kept at HWC, though much of the data is stored in a segregated state - e.g. imagery data is kept separate from user profile data, and without the profile data, the information they provide is simply the image itself. Similarly, survey data is segregated from profile data and OSN data although the survey and OSN data of course have personally identifying data within them. 3. HWC will, however, provide CERTH and VELTI with pseudonymized data from the pre-pre-pilot for temporary usage at their

[54] Pseudonymized data from the pre-prepilot requested by CERTH are:
- User likes for all the users. Likes should not be hashed.
- Posts / status updates
- Extracted visual concepts and logos.
- List of friends of each user
- Survey responses

Data will be used for the development of the likes-based inference module and validation of the results that it produces

[55] Pseudonymized data from the pre-prepilot requested by Velti are:
- User likes for all the users.
- Survey responses

[56] Pseudonymized data from the pre-prepilot requested by iMinds are:
- Facebook Data.
- Survey responses

Data will be used to investigate if there exists contradictions between what people have claimed that is available online (survey) and what actually could be found.

[57] This data set from the pre-prepilot contains all the survey data ("surveyAnswers"), apart from any identifying information such as email, address, etc.contained in the section “Contact Information”, and the following Facebook data: "relationshipStatus", "religion", "website", "birthday", "timezone", "verified", "gender", "political", "locale", "updatedTime", "currency", "interestedIn", "meetingFor", "education","sports", "favoriteTeams", "favoriteAthletes", "languages", "birthdayAsDate", and "likes". The data set does not contain any images. In order to pseudonymize the Facebook and survey data the “id” has been *discarded and converted to a non-tracable guid*. Moreover, the following Facebook data have been *discarded*: "metadata", "type", "name", "firstName", "middleName", "lastName", "link", "bio", "quotes", "about", "email", "username", "picture", "hometown", "location", "significantOther", "thirdPartyId", "tokenForBusiness","work", and "hometownName".

[58] Facebook id, username, phone number and email numbers are hashed.

		own premises. 4. CERTH and VELTI have remote access to backend servers for integration which gives indirect access to imagery data stored on the system, as well as indirect access to the social media stores. 5. CEA has remote access to the backend server, which also allows indirect access to social media data and imagery data.

Table 1. Where the DataBait data are kept and if/when are they deleted/anonymized/pseudonimized?

3.2. Explicit consent for the processing of sensitive personal data

Some personal data can be defined as 'sensitive' or 'special' and need to be handled with extra care. We follow the list of sensitive categories of data mentioned in Art. 9 (1) of the GDPR (which gives a slightly more extensive list than Art.8(1) DPD 95/46):

> "The processing of personal data, revealing: race or ethnic origin, political opinions, religion or beliefs, trade-union membership, and the processing of genetic data or data concerning health or sex life or criminal convictions or related security measures shall be prohibited."

The rationale why the processing of data from this 'special' category deserves extra caution is explained by Working Party 29:

> "In its advice paper from 2011 to the European Commission the Working Party has explained the rationale behind this stricter legal regime. It stems from the presumption that misuse of these data in general, is likely to have more severe consequences for the individual's fundamental rights, such as the right to privacy and non-discrimination, than misuse of other, "less sensitive" types of personal data." (Article 29 Data Protection Working Party, 2015a, p. 1)

The strict regime for the handling of sensitive personal data entails that processing of such data is prohibited - *unless* an exception applies. The most important exception is *consent*, which has to be given specifically for the processing of this sensitive data. Moreover, the consent for the processing of sensitive needs to be *explicit* (Art. 8.2(a), Directive 95/46 and Art. 9.2(a) GDPR).

The strict regime for the handling of sensitive personal data entails that processing of such data is prohibited - unless an exception applies. The most important exception is* explicit consent*, which has to be given specifically for the processing of this sensitive data.

This is a higher standard than consent for other (i.e, non-sensitive) personal data (which, under the current DPD 95/46, could sometimes also be "inferred" or "implicit", i.e. that the actions of the data subject imply consent). Working Party 29 (Opinion 15/2011 on the definition of consent) clarifies:

> "In legal terms "explicit consent" is understood as having the same meaning as express consent. It encompasses all situations where individuals are presented with a proposal to agree or disagree to a particular use or disclosure of their personal information and they respond actively to the question, orally or in writing. Usually, explicit or express consent is given in writing with a hand-written signature. For example, explicit consent will be given when data subjects sign a consent form that clearly outlines why a data controller wishes to collect and further process personal data.[…] The requirement for explicit consent means that consent that is inferred will

not normally meet the requirement of Art 8(2). In this regard, it is worth recalling the Article 29 Working Party opinion on electronic health records stating that "*In contrast to the provisions of Article 7 of the Directive, consent in the case of sensitive personal data and therefore in an EHR must be* ***explicit****. Opt-out solutions will not meet the requirement of being 'explicit'.....*". (p. 25)

In transposing Directive 95/46 into national legislation, Member States have taken different approaches with regard to what is exactly required for legally valid consent (both in case the processing of sensitive and non-sensitive personal data)[59]. The USEMP consortium does not have the resources to check the national laws of all member states, nor does that seem necessary from a legal perspective: sticking to the strictest interpretation of the DPD 95/46 should suffice[60]. However, for the sake of completeness we take a quick look at Belgian and Swedish law in this regard: we pick these examples because those are Member States where two of the USEMP partners are based and where the first cohorts of DataBait users are recruited. The requirement of *explicitness* is repeated Swedish law.[61] In Belgian law[62] the only requirement is that the consent for the processing of sensitive data has to be *written*[63]. Thus, the way DataBait requests consent for the processing of sensitive data (through a separate screen in the DLA) is in line with both Belgian and Swedish law.

Under the GPDR, that is, the new legal data protection regime, the requirement for consent for the processing of sensitive data is still that is has to be *explicit* (Art. 9.2(a) GDPR). In this respect things have stayed unchanged. However, what is relevant in the

[59] For example, Spain has set set additional requirements for consent with regard to the processing of sensitive data. Article 7.2 of the Spanish Organic Law of Personal Data Protection (LOPD) 15/1999, 13th of December, requires consent for the processing of information relating to ideology, religion, beliefs and trade union membership to be "express" (i.e. explicit) and in writing. Article 7.3 requires that consent for processing of other sensitive personal data is "express" but does not require that it is in writing.
See <http://www.twobirds.com/en/news/articles/2006/use-of-consent-in-data-protection> (last accessed 12 February 2016) for a concise overview of how consent has been interpreted in some of the EU member states.

[60] Under current law (Arts. 4(1)(a) and 4(1)(c) Directive 95/46/EC) it is the *location of the establishment* of the data controller which determines applicable national law. The USEMP consortium is the joint controller of the processed DataBait data. Because USEMP is not a legal entity, there is not a single place of establishment. That means that the law of each Member State in which an USEMP partner is based (Belgium, the Netherlands, France, UK, Sweden and Greece) applies. Does this mean that the legal iCIS team has to check the national data protection laws of each of these member states? No. From a dogmatic point of view following the strictest interpretation of the DPD 95/46/EC should ensure DataBait is also compliant with national data protection laws. As clarified by the Court of Justice in Luxemburg in joined Cases C-468/10 and C-469/10, *Asociacion Nacional de Establecimientos Financieros de Credito (ASNEF)* and *Federacion de Comercio Electronico y Marketing Directo (FECEMD) v. Administracion del Estado*, 24 November 2011 (online available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0468>), DPD 95/46 brings along a *full harmonization* which implies that Member States do not have the discretion to offer a lower protection or add additional requirements. This means that, if we follow the strictest interpretation of DPD 95/46, we don't have to check every national legislation of each of the aforementioned Member States.

[61] See the Swedish Data Protection Authority on consent ("samtycke") in the case of sensitive data (http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/samtycke/) and Art. 13 (sensitive data) and 15 (consent for the processing of sensitive data) of the Swedish Data Protection law (https://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Personuppgiftslag-1998204_sfs-1998-204/), requiring *explicit* consent ("sitt *uttryckliga* samtycke")

[62] See the Belgian Data Protection Authority on consent ("toestemming") in the case of sensitive data (https://www.privacycommission.be/nl/gevoelige-gegevens) and Art. 6.2(a)(consent for the processing of sensitive data) of the Belgian Data Protection law (https://www.privacycommission.be/nl/node/3788), requiring *written* consent ("schriftelijke toestemming")

[63] If "written" is interpretated is in line with EU legislation on electronic commerce and digital signatures, it is likely to include "handwritten" consent on paper as well as (some) electronic forms of consent. See WP 29, Opinion Opinion 15/2011 on the definition of consent (adopted on 13 July 2011), p. 26.

GDPR is that the standard for consent in general has been made stricter. Consent will have to be “unambiguous” (Art.4(8)):

> 'the data subject's consent' means any freely given, specific, informed and unambiguous indication of his or her wishes by which the data subject, either by a statement or by a clear affirmative action, signifies agreement to personal data relating to them being processed’;

In order for consent to be considered as “freely” given, “utmost account shall be taken of the fact whether, among others, the performance of a contract, including the provision of a service, is made conditional on the consent to the processing of data that is not necessary for the performance of this contract” (Art. 7(4) GDPR). This additional test does not pose any problems for the consent of DataBait users: the processing of sensitive data (and informing users about it) is the core business of DataBait and thus clearly necessary for the performance of the contract between the DataBait user and the USEMP consortium.

A new requirement in the GPDR is that a written request for consent for the processing of any personal data must be presented in a manner which is “clearly distinguishable” from the rest of the written context in which it is presented (Art. 7(2) GDPR):

> “If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent must be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of the declaration which constitutes an infringement of this. Regulation that the data subject has given consent to shall not be binding.”

We present the DLA in the form of separate screens (each article of the DLA is a separate screen – including the one on sensitive data) in order to fulfill the requirement of Art. 7(2) GDPR (i.e., to present the request for consent “in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language”).

A new requirement in the GPDR is that a written request for consent for the processing of any personal data must be presented in a manner which is “clearly distinguishable” from the rest of the written context in which it is presented (Art. 7(2) GDPR). DataBait’s DLA is presented in the form of separate screens and thus fulfills this requirement.

We do not ‘hide’ the request for consent in some general terms of service: the whole DLA concerns the fulfilment of data protection requirements and offering transparency about it. Whether our current presentation could be even further enhanced is something which we will discuss with the other partners. One could for example consider giving the screen with the consent for sensitive data another color. However, it would be also unnecessary to “overdo” it and scare users away from a tool that is precisely empowering in terms of data protection.

3.3. The grey zone of what qualifies as sensitive

There are data which are obvious cases of sensitive data. For example, a medical record in a hospital is an obvious instance of health data (pertaining to the health status of the data subject) and a municipality record stating that a person is Roma, Jew, etc. is an obvious instance of data revealing race or ethnic origin. There are also data which are seemingly innocuous. For example, think of a data subject who has uploaded a holiday picture on Facebook where she is standing in a bar with a sigarette and a glass of wine or a data subject who regularly uploads the data of her running app (stating where she runs,how fast, her heart rate, how many calories she has burned, etc.). These data are in some way related to health, but are they health data (and thus sensitive)? And does the fact that one's skin color is visible in a picture make it racial data? In establishing whether personal data are sensitive or not, it is not enough to take raw data at their face value – also their *potential* sensitivity in case of inferences or combination with other data should be taken into account. With regard to establishing whether such data 'from the grey zone' is sensitive, the difficulty lays both in establishing the technical possibilities (*what can be extracted from the data? which software possibilities exist? what can be extracted from the data in combination with other data sets an which data sets are available for such combinations?*) and in the fuzziness of the qualification rule (*some* possibilities to extract sensitive information from a piece of data make it sensitive in the sense of Art. 8 DPD 95/46 and *some* don't). In order to clarify which potentialities are relevant we follow the line set out by Working Party 29 with regard to health data (Article 29 Data Protection Working Party, 2015a, 2015b) and apply their analysis in an analogous way with regard to other types of sensitive data.

The bottom-line is that it would be unsustainable to consider every potentiality as a ground for qualifying data as sensitive. For example, photos and videos containing images of people can be a source of all kind of sensitive information: smart analytic software could extract racial (e.g. based on skin colour) and religious features (e.g. based on whether someone is wearing certain religious garments or jewelry), health or biometric data (e.g. based on gait, body shape, activity pattern, skin colour, behavioral analysis etc.). However, requiring that any photo or video containing a face or body of an identifiable person should be qualified as sensitive and thus be subjected to the extra strict regime of handling sensitive personal data would put an unreasonable burden on data controllers operating on the internet. Working Party 29 has given two possible situations when a piece of data which is not a clear-cut[64] case of health data (e.g. medical data) nevertheless qualifies as health data:

[64] "There remain some types of processing, where it is not obvious at first sight whether or not the processing of these data should qualify as the processing of health data. This is especially the case where the data are processed for additional purposes and/or combined with other data or transferred to third parties. These types of data processing may create risks, including the risk of unfair treatment based on data about a person's assumed or actual health status. Clearly, these types of data processing deserve significant attention. If data are health data, but mistakenly treated as 'ordinary' personal data, there is a risk that the high level of protection deemed necessary by the European legislator is undermined. If seemingly innocuous raw data are tracked over a period of time, combined with other data, or transferred to other parties who have access to additional complementary datasets, it may well be that even the seemingly most innocuous data, combined with other data sources, and used for other purposes, will come within the definition of 'health data'.This risk specifically applies to further processing of such data for profiling and marketing purposes, given that the key business model of most apps is based on advertising." (Article 29 Data Protection Working Party, 2015a, p. 3)

It would be unsustainable to consider every potentiality as a ground for qualifying data as sensitive. For example, photos and videos containing images of people can be a source of all kind of sensitive information: smart analytic software could extract racial and religious features, health or biometric data. However, requiring that any photo or video containing a face or body of an identifiable person should be qualified as sensitive and thus be subjected to the extra strict regime of handling sensitive personal data would put an unreasonable burden on data controllers operating on the internet.

1. The data are raw sensor data that can be used in itself or in combination with other data to draw a conclusion about the actual health status or health risk of a person: i.e., there has to be a demonstrable relationship between the raw data set and the capacity to determine a health aspect of a person,

2. Conclusions are drawn about a person's health status or health risk (irrespective of whether these conclusions are accurate or inaccurate, legitimate or illegitimate, or otherwise adequate or inadequate)

How to transpose this as a guideline in deciding whether any non-obviously sensitive data qualifies as sensitive? We think that following the lines set out here by WP29 for health data, two general guidelines could be proposed for the assessment of any data which are neither obviously non-sensitive nor a clear-cut instance of sensitive data. Firstly, that it does not matter whether an inference is correct: if it is likely that a company will use smart software which wrongly classifies all people with dark hair as “Asians”, this is nevertheless processing of sensitive (racial) data. Secondly, we propose that what is important in non-obvious cases is that there needs to be a realistic possibility and a significant chance that sensitive information will be extracted and used as such. We would like to propose that “intended use” (Article 29 Data Protection Working Party, 2015a, p. 4) of the data, that is, the concrete context in which data are likely to be used, could be a very useful criterion in deciding whether data qualifies as sensitive in non-obvious cases. Both “a demonstrable relationship” (Article 29 Data Protection Working Party, 2015a, p. 4) between raw data and sensitive information and the question whether it is likely that conclusions with regard to sensitive matters will be drawn from the data, show that the qualification of data from the ‘grey area’

Qualification of data from the ‘grey area’ as sensitive or not, should not be an abstract exercise in theoretical possibilities and potentialities but look at concrete possibilities and intended uses.

(where it is not immediately obvious whether data should be qualified as sensitive or not) should not be an abstract exercise in theoretical possibilities and potentialities but look at concrete possibilities and intended uses (e.g. *What is the business model of the data controller processing these data? Does the data controller have access to other data bases that allow combinations of data that make it possible to infer information regarding health*

status?). The notion of 'intended use' as we propose it should be distinguished from the specified purpose of the processing. The latter is a legal requirement for processing, while intended use is a factual criterion for establishing whether non-obvious cases qualify as sensitive data. Purpose specification and intended use can be related (e.g. when a data processor explicitely specifies that she will combine weight data with opinion data to assess the mental health of the data subject) but do not necessarily coincide (i.e. if a data controller does *not* state it as a processing purpose to establish the health status, religion, race, etc. from a certain type of data, this does not exclude the possibility that the concrete context can nevertheless make it likely that the data controller *could and would* extract this sensitive information). Let's take a closer look at how the Working Party arrives at its recommendation for qualifying health data through the lens of the notion of 'intended use'.

'Purpose specification' and 'intended use' can be related but do not necessarily coincide. For example, if a data controller does not state it as a processing purpose to establish the health status, religion, race, etc. from a certain type of data, this does not exclude the possibility that the concrete context can nevertheless make it likely that the data controller* could *and* would *extract this sensitive information.

The Working Party begins by observing that health data is a broad notion, covering anything from direct medical data, stating that a person has a certain disease, to more indirect data (e.g. data about buying certain medical devices, being a member of a support group or association like Weight Watchers or Alcoholics Anonymous, etc.), to 'light' medical information (e.g. wearing contact lenses or allergy information), to "data about a person's intellectual and emotional capacity (such as IQ), information about smoking and drinking habits" (Article 29 Data Protection Working Party, 2015a, p. 2), or data indicating a good (instead of ill) health. Also lifestyle data which might contribute to the establishment of disease risks can be health data.

> "According to the Working Party, health data therefore also include information about a person's obesity, high or low blood pressure, hereditary or genetic predisposition, excessive alcohol consumption, tobacco consumption or drug use or any other information where there is a scientifically proven or commonly perceived risk of disease in the future." (Article 29 Data Protection Working Party, 2015a, p. 2)

However, the Working Party also underlines that it assumes that :

> "…there is a category of personal data generated by lifestyle apps and devices that is, in general, not to be regarded as health data within the meaning of Article 8. This concerns data from which no conclusions can be reasonably drawn about the health status of a data subject. Not all raw data collected through an app (measurements) qualify as information (from which meaning can be derived) about the health of a person. For example, if an app would only count the number of steps during a single walk, without being able to combine those data with other data from and about the

> same data subject, and in the absence of specific medical context in which the app data are to be used, the collected data are not likely to have a significant impact on the privacy of the data subject and do not require the extra protection of the special category of health data. They are just raw (relatively low impact lifestyle) personal data (provided, the app does not process location data), not information from which knowledge about that persons health can be inferred." (Article 29 Data Protection Working Party, 2015a, p. 3)

We would thus add that whether such data are in the 'grey area' much depends on the *intended use* of the data. If an individual piece does not constitute health data as such (e.g. the amount of steps someone made during a day), it should be checked whether there is an intended plan to combine it with other data to use it in a health related way.

> "There has to be a demonstrable relationship between the raw data set and the capacity to determine a health aspect of a person, based on the raw data itself or on the data in combination with data from other sources. For example, if a diet app only counts the calories as calculated from input provided by the data subject, and the information about the specific foods eaten would not be stored, it would be unlikely that any meaningful conclusions can be drawn with regard to the health of that person (unless the daily intake of calories is excessive in absolute terms). But if data from a diet app, or heart rate monitor or sleep diary app are combined with information provided by the data subject (directly or indirectly, for example based on information collected from that person's social networking profile), conclusions (whether accurate or inaccurate) may be drawn about that person's health condition, such as medical risk or diabetics. In these cases it is likely that health data can be inferred from the combined data." (Article 29 Data Protection Working Party, 2015a, p. 4)

The Working Party states that data following from opinion or mood analysis conducted on texts posted in social media *could* constitute health data depending on the actual context and the purpose of the processing :

> " An example […] is analysis conducted on social media to detect whether people may suffer from a depression. Even though 'sad' messages sent by users, in general, do not have to be treated as health data by (generalist) social networks, the systematic analysis of such messages for the purpose of diagnosis/health risk prevention or medical research certainly qualifies as the processing of health data." (Article 29 Data Protection Working Party, 2015a, p. 3)

In summary, we think that in difficult, non-obvious, cases, in order to establish whether a piece of data should be qualified as sensitive data, it is important to look at the intended use of the data. It is not enough to look at a piece of data in isolation : if the intended use entails that the data will be combined with other data in such a way that what can be inferred from the data becomes more health related, this should be taken into account. We propose this rule of thumb : whether a *potential* to derive sensitive information from 'innocuous' (i.e. non-sensitive) raw personal data should result in the qualification of these data as 'sensitive' depends on their *intended use* (realistic possibility and significant chance that sensitive information will be extracted and used, given the concrete circumstances). Thus, a picture depicting faces of a particular skin color does not necessarily constitute sensitive data about race and ethnic origin – it depends on the intended use.

We propose this rule of thumb : whether a* potential *to derive sensitive information from 'innocuous' (i.e. non-sensitive) raw personal data should result in the qualification of these data as 'sensitive' depends on their* intended use *(realistic possibility and significant chance that sensitive information will be extracted and used, given the concrete circumstances).

What does this imply for the derived data in the USEMP project and the raw data from which they are derived? The DataBait tool will inform the user about the possible information which can be extracted from her data. Thus, we will inform the user that data about race, health, religion etc. could be extracted from a certain picture, and that this could mean that the picture should be treated as sensitive data, but that this will depend on the actual intended use of the picture. The DataBait user will be given realistic examples of the intended uses for which the informaton could be used.

In table 2 we list the qualifications of the various derived data types. The DataBait user will be informed about which raw data could potentially be qualified as sensitive based on the potentially sensitive data which could be derived from it.

	'Privacy dimensions (i.e., categories into which the derived data are organised: see D6.1)	**Derived attributes**	**Legal qualification in terms of EU data protection (DP) law and EU anti-anti-discrimination (AD) law.** **SPD: sensitive personal data;** **PD: personal data**
	Demographics	1. Age	DP: PD AD: Protected ground in the field of employment
		2. Gender	DP: PD AD: Protected ground in the field of (1) employment, (2) access to goods and services
		3. Nationality	DP: PD AD: Protected ground but many exceptions (i.e. particular areas where differentiation based on nationality is allowed)
		4. Racial origin	DP: SPD AD: Protected ground in the field of (1) employment, (2) access to goods and services, (3) education, (4) social advantages, (5) social protection
		5. Ethnicity	DP: SPD AD: Protected ground in the field of (1) employment, (2) access to goods and services, (3) education, (4) social advantages, (5) social protection

		6. Literacy level	DP: PD
		7. Employment status	DP: PD
		8. Income level	DP: PD
		9. Family status .	DP: PD, could be SPD if it reveals information about one's sex life (or according to the pGPDR: sexual orientation or gender identity)AD: if the data reveals sexual orientation- this is a protected ground in the field of employment law
	Psychological Traits	1. Emotional stability	DP: PD; possibly SPD (if characterized as health data)
		2. Agreeableness	DP: PD; possibly SPD (if characterized as health data)
		3. Extraversion	DP: PD; possibly SPD (if characterized as health data)
		4. Conscientiousness	DP: PD; possibly SPD (if characterized as health data)
		5. Openness	DP: PD; possibly SPD (if characterized as health data)
	Sexual Profile	1. Sexual preference	DP: SPD AD: if the data reveals sexual orientation- this is a protected ground in the field of employment law
	Political Attitudes	1. Parties (Part of list for Belgium: CD&V; Groen!; N-VA; Open VLD /Part of list for Sweden: Centerpartiet; Vansterpartiet; Folkpartiet liberalerna)	DP: SPD
		2. Political ideology (Communist; Socialist; Green; Liberal; Christian democratic; Conservative; Right-wing extremist)	DP: SPD
	Religious Beliefs	Supported Religion (Atheist, Agnostic, Christian, Muslim, Hinduist, Buddhist, Other, etc.)	DP: SPD AD: religious belief is a protected ground in the field of employment law

	Health Factors & Condition	1. Smoking	DP: PD; possibly SPD (if characterized as health data)
		2. Drinking (alcohol)	DP: PD; possibly SPD (if characterized as health data)
		3. Drug use	DP: PD; possibly SPD (if characterized as health data)
		4. Chronic diseases	DP: PD; possibly SPD (if characterized as health data)
		5. Disabilities	DP: PD; possibly SPD (if characterized as health data) AD: Disability is a protected ground in the field of employment law
		6. Other health factors (e.g.: Exercise (yes / no); Late night shifts (yes / no); Staying up late)	DP: PD; possibly SPD (if characterized as health data)
	Location	1. Home	DP: PD
		2. Work	DP: PD
		3. Favourite places	DP: PD
		4. Visited places	DP: PD
	Consumer Profile	1. Brand attitude	DP: PD
		2. Hobbies	DP: PD; possibly SPD if the hobby reveals one's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, or information with regard to one'shealth or sex life.
		3. Devices	DP: PD
	n.a.	Detection of faces in images (number and location)	DP: PD
	n.a.	Detection of opinion	DP: PD

		(positive/negative/ neutral) from textual posts and status updates	
	n.a.	Disclosure score (How sensitive, uncontrollable and visible are your data?)	DP: PD
	n.a.	Personal data value score (what kind of audience do you have on your OSN and to whom could reaching such an audience be valuable?)	DP: PD

Table 2. How should the data derived from the raw DataBait data be qualified in terms of Data Protection (DP) law and Anti-Discrimination (AD) law? In terms of DP law data can be either non-sensitive personal data (PD) or sensitive personal data (SPD)

3.4. 'Intended use': Sensitive data and anti-discrimination law.

Compared to the legal instruments of the EU, the rights derived from the European Convention on Human Rights (ECHR) often provide a broader but also a fuzzier protection. Not only because the primary goal of the ECHR is to protect the individual citizen against the State (and not against Facebook, Google or a databroker), but also because the route to the Court in Strasbourg (a measure of last resort) is longer than the route with regard to EU legislation (or the national implementation thereof). National courts can raise preliminary questions with the Court of Justice of the European Union (CJEU) in Luxemburg about the interpretation of EU law. Nevertheless it is also precisely the broad formulation of ECHR rights which can sometimes provide protection where the more specific provisions of the EU fail to do so. This is particularly clear in the field of anti-discrimination law. As shown in figure 2, the anti-discriminatory law of the EU offers protection with regard to a very specific set of protected grounds (listed in Art. 13 of the *Treaty Establishing the European Community*[65] [TEC, 1997; entry into force in 1999]: sex, racial or ethnic origin, religion or belief, disability, age or sexual orientation) and areas of life. The largest protection is offered with regard to race, and in the field of employment.

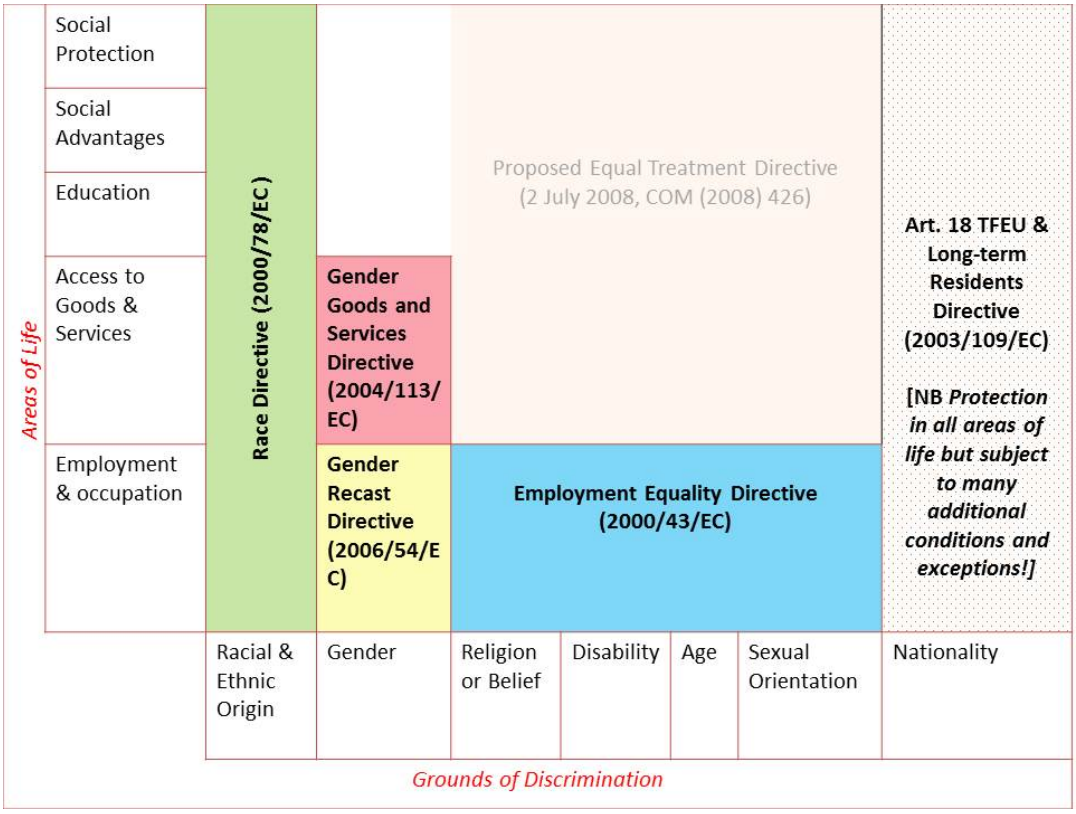

Figure 13: Protected grounds and areas of life in secondary EU anti-discrimination law

[65] Now replaced by Article 19 of the *Treaty on the Functioning of the Union* (TFEU, 2008). The content of Art. 19 TFEU and Art. 13 TEC is identical.

When comparing the anti-discriminatory provisions from EU data protection law with those from EU anti-discrimination law, there are some interesting overlaps as well as differences to be pointed out (see table 2).

Data Protection	Art. 9 (1) of the proposed General Data Protection Regulation (GDPR)	The processing of personal data, revealing: **race or ethnic origin, political opinions, religion or beliefs**, trade-union membership, and the processing of ***genetic data*** or data concerning *health or sex life* or criminal convictions or related security measures shall be prohibited.
	Art. 20 (3) of the proposed General Data Protection Regulation (GDPR)	Profiling that has the effect of discriminating against individuals on the basis of **race or ethnic origin, political opinions, religion or beliefs**, trade union membership, *sexual orientation or gender identity*, or that results in measures which have such effect, shall be prohibited. The controller shall implement effective protection against possible discrimination resulting from profiling. Profiling shall not be based solely on the special categories of personal data referred to in Article 9
Anti-Discrimination	Art. 21 Charter of fundamental rights of the European Union (CFREU)	(1) Any discrimination based on any ground such as: sex, **race**, colour, **ethnic** or social **origin, *genetic features***, language, **religion or belief, political or any other opinion**, membership of a national minority, property, birth, *disability*, age or *sexual orientation* shall be prohibited. (2) Within the scope of application of the Treaty […] any discrimination on grounds of nationality shall be prohibited.
	Art. 13 Treaty Establishing the European Community (TEC)	…take appropriate action to combat discrimination based on sex, **racial or ethnic origin, religion or belief**, *disability*, age or *sexual orientation*

Table 3: Discrepancies and overlaps between (1) the data categories classified as sensitive or discriminatory in EU data protection law and (2) the prohibited grounds in EU discrimination law. In this table the bold categories are the ones that overlap, the italic ones partly overlap, and the underlined ones are new additions to the list of sensitive data in Art. 9 (1) of the GDPR (in comparison to the ones mentioned in Art 8(1) of the current DPD 95/46. This table is an updated and adjusted version of the table in: (Gellert, de Vries et al. 2012)

One way to explain these overlaps and differences is that data protection is more oriented on the *process* of data processing, while the anti-discrimination provisions look at discriminatory *effects*. Thus, data such as sex, age, and nationality (which is the kind of basic

information which one is required to provide frequently in OSNs) are not considered to be sensitive data from a data protection perspective, but as soon as one begins to take discriminatory measures based on them, for example in the area of employment, they become “toxic”.

Data such as sex, age, and nationality (which is the kind of basic information which one is required to provide frequently in OSNs) are not considered to be sensitive data from a data protection perspective, but as soon as one begins to take discriminatory measures based on them, for example in the area of employment, they become “toxic”.

While the processing of *sensitive* data -for example, data which reveal racial origin or political opinions- requires additional safeguards in comparison to the processing of “ordinary” personal data (even when no actual discrimination results from it), data such as sex, age, and nationality are not considered to be sensitive *as such*.

However, when the sensitivity of data is to be judged in terms of their ‘intended use’ (see above), it becomes clear that the prohibition to process sensitive data (unless an exception such as explicit consent applies) comes closer in rationale to the ‘effect’-oriented provisions from anti-discrimination law. The provisions are increasingly merging into a partly overlapping continuum. Therefore we propose that the *DataBait* should inform users both of the protection with regard to sensitive data and the anti-discrimination provisions which might apply.

In designing the DataBait tool the notion of ‘intended use’ should be incorporated in the information provided to the user, when informing her that her data can be categorized as (potentially) belonging to the specific categories of data in EU anti-discrimination law (protected grounds) and EU data protection law (sensitive data and the protected grounds mentioned in Art. 20(3) GDPR). The question which needs to be posed is whether these categories of data are (likely to be) processed by commercial profilers. Additional questions to be explored are how the user should be informed of the relevant legal provisions with regard to these particular kinds of data and whether users feel that the sensitive data and protected grounds deserve a higher level of protection than other data (e.g. income, log-in patterns, educational level, etc.)?

4. Data Licensing Agreement

4.1. A DLA: legal ground and legitimate purpose

Lawful processing of personal data always has to be based on a legal ground legitimizing the processing and have a legitimate, specified and explicit purpose by which the allowed usages of the data are limited. Both conditions have to be fulfilled to make the processing lawful. With regard to the first requirement the GDPR enumerates six legal grounds in Art. 6(1):

Processing shall be lawful only if and to the extent that at least one of the following applies:

The threefold aim of the Data Licensing Agreement (DLA) for the end-users of DataBait platform has been:

(1) To provide a legitimate legal ground for the processing of personal data, notably also sensitive data and for using/downloading the USEMP DataBait tools;

(2) To engage the end-user (data subject) by asking her to enter into an obligatory agreement with the USEMP partners (joint data controllers), clarifying mutual rights and obligations;

(3) To present the end-user (data subject) with a clear, concise transparent agreement that is legible for lay people and covers all the relevant issues of compliance on the side of the USEMP service providers (joint controllers)

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The first, and most well-known, legal ground is *consent*. The other five concern *necessity* in relation to (b) a contract, (c) a legal obligation, (d) the vital interests of the data subject, (e) the public interest or (f) the legitimate interests of the data controller (if these

interests are not overruled by the fundamental rights of the data subject).” (Hildebrandt, 2014, p. 24)

The second requirement, which is a combination of purpose specification and use limitation, is described in Art. 5(1)b GDPR (see also our discussion in chapter 2):

> “Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”.

Both the requirement of a legal ground and purpose specification/use limitation need to be fulfilled, which means that:

> “…one *cannot* consent purpose limitation away; a valid new legal ground does not imply that historical data can now be used for an incompatible purpose in relation to the one for which they were originally processed. Purpose binding thus ties whoever processes personal data to the explicit legitimate purpose as it was specified upfront, when the data were first collected. It chains that entity to its own stated – and necessarily legitimate - purpose.” (Hildebrandt, 2014, p. 24)

The purpose of the processing is determined by the data controller.[66] Because the USEMP consortium has jointly determined what the purpose and means of the processing of personal data will be, and should thus be qualified as a joint data controller[67]. As the USEMP consortium does not possess legal personality, it was important to create an internal agreement between the partners (the PDPA, see below) in which partners commit to implementing relevant data protection law when processing the personal data of USEMP end-users, while each partner exonerates the others from liability for data processing which is not under the actual control of these other partners.

It was important to create an internal agreement between the USEMP partners (the PDPA) in which partners commit to implementing relevant data protection law when processing the personal data of DataBait end-users, while each partner exonerates the others from liability for data processing which is not under the actual control of these other partners.

The USEMP consortium has chosen to take the ground from Art. 6.1(b) GDPR as the legal ground for all the processing: a data licensing agreement (DLA) between the USEMP consortium (the joint data controller) and the end-user of the USEMP tools is the legal

[66] “**'controller'** shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data”, Art. 2(d) DPD 95/46.

[67] “Joint controllers. Where several controllers jointly determines the purposes and means of the processing of personal data, the joint controllers shall determine their respective responsibilities for compliance with the obligations under this Regulation, in particular as regards the procedures and mechanisms for exercising the rights of the data subject, by means of an arrangement between them. The arrangement shall duly reflect the joint controllers‘ respective effective roles and relationships vis-à-vis data subjects, and the essence of the arrangement shall be made available for the data subject. In case of unclarity of the responsibility, the controllers shall be jointly and severally liable” (Art 24 of the pGDPR)

ground for the data processing in USEMP. It should be noted that this DLA is *not* merely a service license agreement (SLA) or Terms of Service agreement (ToS) in which the part about data processing is only an appendix – i.e., a consent form attached to the main service agreement – but that this contract actually focuses on the *purpose* of data processing within the USEMP project and the mutual obligations between the USEMP consortium partners (the joint data controllers) and the end-user of the USEMP tools. These obligations are created in order to fulfil that purpose.

A data licensing agreement (DLA) between the USEMP consortium (the joint data controller) and the end-user of the USEMP tools is the legal ground (Art. 6.1(b) GDPR) for the data processing in USEMP. It should be noted that this DLA is not merely a service license agreement (SLA) or Terms of Service agreement (ToS) in which the part about data processing is only an appendix – i.e., a consent form attached to the main service agreement – but that this contract actually focuses on the purpose of data processing.

Opting for a DLA, rather than the usual combination of a SLA (or ToS) combined with a privacy policy, user consent and lengthy terms and conditions, also aligns with the USEMP proposal to enable the licensing of the use of personal data by data subjects, as described in the USEMP Description of Work (DOW). Another way in which the DLA embodies the objective of user empowerment, is that it keeps matters as straightforward as possible and puts them in plain language: the DLA avoids any unnecessary “legalese”. The DLA is implemented in the USEMP graphic user interface (GUI) and is part of the sign-up procedure. It is impossible to sign-up or use the DataBait tools without first signing the DLA. Each article of the DLA is presented as a separate screen. All the text fits easily on one screen, making it unnecessary for the user to scroll down.

Building the DLA and the internal agreement into the DataBait GUI can also be considered as a way in which USEMP realizes Data Protection by Design (Art. 23 GDPR) with regard to Art. 6(1) GPDR (legal ground) and the requirement of *data minimization* (Art. 5 GPDR), which is an umbrella term for the requirement of *purpose specification* (that data must be collected for specified, explicit and legitimate purposes and that they must be adequate, relevant and not excessive in relation to the purposes for which they are collected), *use limitation* (that data should not be further processed in a way incompatible with those purposes), that data have to be *accurate and complete*, and that they are deleted or anonymised as soon as they are no longer needed for the purpose that led to their collection.

An important counter argument with regard to the use of a DLA could be that such an agreement could be used to replace privacy policies, thus disabling data subjects from easily withdrawing their data. Such a DLA could integrate the usual complex and intransparent language, meant to lure data subjects into signing away the control over how their personal data is used. The USEMP DLA not only provides for, but also depends on the profile transparency that is a precondition for informed consent regarding the use of one’s personal

data. Our argument is not based on the idea that any type of DLA necessarily offers more protection than consent or processing based on the f-ground. On the contrary, the USEMP DLA is based on the fact that the b-ground allows to process only those personal data necessary for the performance of the DLA, meaning that a clear and enforceable description must be provided of the mutual obligations generated by the DLA. Further protection derives from paying keen attention to a number of private law and consumer law provisions that protect the weaker party against unreasonable clauses in contracts concluded between consumers and businesses. Finally, we argue that the USEMP DLA is highly relevant for all business models that are based on providing a so-called 'free service', by clarifying in clear and enforceable terms how the processing of the user's volunteered, observed and inferred data may affect the way she can be targeted by the service provider, third parties and government authorities.

Thus, to summarize, the threefold aim of the Data Licensing Agreement (DLA) for the end-users of DataBait platform has been::

1. To provide a legitimate legal ground for the processing of personal data, notably also sensitive data and for using/downloading the USEMP DataBait tools;
2. To engage the end-user (data subject) by asking her to enter into an obligatory agreement with the USEMP partners (joint data controllers), clarifying mutual rights and obligations;
3. To present the end-user (data subject) with a clear, concise transparent agreement that is legible for lay people and covers all the relevant issues of compliance on the side of the USEMP service providers (joint controllers)

Below we present the DLA and the underlying personal data processing agreement (PDPA) that has been concluded between the USEMP Consortium Partners (as joint controllers), thus binding the partners to provide some form of profile transparency in exchange for a specified license to process the user's (data subject's) personal data. We will explain the relationship between the DLA and the consent requirement for processing sensitive data (art. 8 DPD) and between the DLA and the consent requirement for storing tracking mechanisms on the user's (subscriber's) device (art. 5.3 ePrivacy Directive).

The idea of employing a data licensing agreement is new and hopes to provide for a new way of addressing the power imbalances between users and providers of OSNs[68]. It is based

[68] The fact that the service of an OSN is rendered at no cost does not justify a weak position of the user in terms of consumer and data protection. Moreover, the notion of "service at no cost" must be nuanced. See e.g. Wauters e.a. 2014, p. 10: "*Since most SNS do not require an actual payment of a fee, we wonder if SNS can fall under the scope of the Consumer Rights Directive. […] However, it is often stated that personal data is the new currency of the Internet. A SNS offers its service to users and in exchange, they gather (explicitly through registration forms or 'secretly' via cookies) personal data of their users. Because of this personal data, they are able to offer personal advertisements in order to make a profit. Another indication may be found in the definition of information society services under the e-Commerce Directive (above), which includes service which are financed by advertising."* Following Wauters it might be argued that based on the Consumer Rights Directive the license granted by the users to Facebook is too broad and not legally valid. The PDPA which is signed between the USEMP consortium and the users of the DataBait tool is a first step to a more balanced approach, and which can form the basis for a more granular licensing approach. This entails that a later, modular version of the DLA should include licensing of copyrighted material posted on the OSN.

on the fact that data subjects have a bundle of rights with regard to the processing of their personal data. This allows them to contract about such processing to the extent that processing is not e.g. mandatory for reasons of public security or necessary for the legitimate interest of the data controller.

4.2. The USEMP DLA

As indicated, the data licensing agreement (DLA) will be concluded between the USEMP Consortium Partners (as joint data controllers) and the end-users of the USEMP tools. It clearly defines the mutual legal obligations, taking the end-users seriously as participants in the research that is conducted. It is also the legitimizing ground for the data processing in USEMP (“contract” as decribed in Art. 7b of Data Protection Directive 95/46).

The DLA is implemented in the USEMP graphic user interface (GUI) and is part of the sign-up procedure. Each article of the DLA will be presented as a separate screen. The

underlying Personal Data Processing Agreement (PDPA, see below) can be seen as an offer made by all each of the USEMP Consortium Partners to conclude the DLA; when the end-user clicks accepts this offer by clicking the button at the end, each USEMP Consortium Partner is bound by the DLA.

Later on in this chapter we present a modular version of the DLA, enabling data usage licensing via DataBait tools for profile transparency, with other service providers that may have a commercial interest in providing the tools. This entails that the purpose is extended or adapted.

Screen 1:

USEMP Data License Agreement

The parties:

(1) [……You……], user of the USEMP platform and services, from hereon called '**You**' and

(2) [CEA-France / iMinds-Belgium/ CERTH-Greece / HWC-UK/ LTU-Sweden /VELTI-Greece/ SKU Radboud University-the Netherlands], provider of the USEMP platform and services, joint data controllers, from hereon called '**USEMP consortium partners**'

Hereby agree:

Screen 2:

(A) After registration, You may use **DataBait-Facebook app**. The DataBait-Facebook app will be used by the USEMP consortium partners to collect data that You share on Facebook. After registering to the DataBait You can, if You choose to, also install the **DataBait web browser plug-in**. The DataBait web browser plug-in will be used by the USEMP consortium partners to collect Your browsing data and allows You to control the trackers on the pages You visit. Together the app and the plug-in form the '**DataBait application**'. The data collected by the DataBait application can be data You posted (volunteered data), or online behavioural data reflecting what You did on Facebook and – if You install the DataBait browser plug-in – what You did on the internet (observed data).

This article defines the obligation to install the DataBait tools, which is pertinent for participation in the USEMP research. It clarifies upfront that both volunteered (declared) data will be processed and observed (behavioural) data. In a later, modular version of the DLA, not necessarily focused on scientific research, the same article can be used.

Screen 3:

B) You license the use of Your volunteered, behavioural and observed personal data by the USEMP consortium partners, as gathered by the DataBait-Facebook app and the DataBait web browser plug-in for the sole purpose of scientific research and – within that

context – to provide You with information about what third parties might infer based on Your sharing of information, and on Your online behaviour. The said data may be combined with publicly available personal data gained from other sources to infer more information about Your habits and preferences (inferred data).

This article, first, makes clear that this is a *quid pro quo* agreement, creating legal obligations on the side of the user (data subject) in the form of licensing the use of the data that will be processed by the USEMP consortium, and on the side of the service provider (data controller) in the form of providing a form of profile transparency. Second, it determines the specific purpose of processing. In the modular version of the DLA, not necessarily focused on scientific research, part of this article *("…for the sole purpose of scientific research and – within that context – to provide You through the DataBait graphic user interface (GUI) with information about what third parties might infer based on Your sharing of information")* will have to be adapted

Screen 4:

C) The data we gather through the DataBait-application may contain creations (such as images, photos, text, video) protected under copyright or neighbouring rights. These protected creations will be copied and stored on our servers and adapted for the purposes of our research (in particular for inferring additional information from Your data, for the scientific purpose described in clause B, by using automated data analytic tools). We will not commercialise Your creations or distribute these to third parties. We will not communicate Your creations to the public: Your creations will only be made available to You (when You access the Databait application via the web interface) and to our research teams (for the purposes of our research).

You agree with this use of Your creations covering the worldwide territory, for the duration of our research project. You will not receive any remuneration but You will have access to our research results.

As explained in D3.11 this Article allows for the reproduction of copyright protected content for USEMP's profiling purposes. The coverage of the "worldwide territory" refers to the fact that USEMP is licensed to use such content independent of the question in which region of the world the user is located when she uploads content to her OSN or logs in to DataBait.

Screen 5:

D) This license agreement confirms Your explicit consent to store the DataBait application on Your devices.

This article provides the consent required on the basis of art. 5.3 ePrivacy Directive for all and any tracking mechanisms to be stored on the user's (data subject's) device. That such tools contain tracking mechanisms is clarified in the previous articles A and B – the consent thus includes any cookies that are stored on the device, which are – in this case – necessary to fulfil the functionality of the service that is provided. This means that consent may not be required, since – according to the art. 29 WP consent is not required for functional cookies. To be on the safe side we have included this consent. We advise that this article is part of the modular versions of the DLA discussed in section 4.5.

Screen 6:

(E) The USEMP consortium partners will do scientific research to predict what kind of information Facebook or other third parties with access to Your postings and online behavioural data could or might infer from the said data. These inferences will be shared with You in an intuitive manner through the DataBait web interface, thus providing You with an online presence awareness tool.

This article further explains the obligation on the side of the service provider and the purpose of processing, highlighting that the profile transparency provided is based on statistical inferences by others than OSN providers, meaning that the user is made aware of the fact that the USEMP Consortium partners are not reverse engineering software code of the OSN provider and cannot in any way provide certainty about how one may be targeted. This article also ensures that the transparency is provided in a user-friendly manner. This article is crucial in any DLA for DataBait tools. However, the term 'scientific research' might have to be adapted in some of the modular versions of the DLA (see below).

Screen 7:

(F) You agree to participate in surveys and/or focus groups, to enable the consortium to gain insights in how users engage with social networking sites and how they evaluate (1) various scenarios regarding the use of their personal data and targeted profiles and (2) the effectiveness, usability and utility of the DataBait application.

This article clarifies that the user will participate in the research that enables to correlate their declared preferences or personality traits with the inferences drawn from behavioural data or the mining of multi-media content. This article may be part of the modular version of the DLA (see below), depending on the particularities of the transparency tool and the services accompanying it. Any reference to USEMP will of course have to be removed in the modular version.

Screen 8:

(G) You hereby grant Your consent to process Your sensitive personal data, notably those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and those concerning health or sex life.

Since consent is required for processing art. 9 GPDR types of data, this article stipulates such consent. It highlights the intrusive nature of the processing of such data. It is part of the modular version of the DLA (see below).

Screen 9:

(H) The USEMP consortium partners will treat all Your personal data, especially Your sensitive data, with care and delete or anonymize them as soon as possible. Because one of the main goals of the USEMP project is to create awareness about the possibility to infer

sensitive data from trivial data trails, it is important to alert You to such inferences and thus to process them.

See commentary below the next Article.

Screen 10:

(I) The USEMP consortium partners will process Your personal data in a secure way and not keep them any longer than necessary for the purpose of the USEMP study. In order to provide You with access to Your personal data and the inferences drawn from them, the data may be kept until the end of the project. Within 3 months of the ending of the research project all personal data will be either deleted, anonymized or processed for related scientific research. In the latter case the relevant USEMP consortium partner will ask You for Your consent.

Articles H and I confirm the legal obligation for the USEMP partners (joint controllers) that the relevant data will be processed in accordance with the data minimisation principle, stipulating deletion or anonymisation as soon as possible (including a clear deadline) and security by design, while also explaining that to provide profile transparency the processing of both personal and sensitive personal data is necessary. These articles are part of the modular version of the DLA (see below) considering that this is a confirmation and reminder of the legal obligations of the service provider (data controller).

Screen 11:

(J) The USEMP consortium partners will not provide Your personal data to any third party.

This article is pivotal to ensure that in the context of USEMP data are not processed beyond the explicitly specified purpose, by the parties to the contract, simply prohibiting any transfer to third parties. The article can be modulated depending on the specifics of the modular version of the DLA, for instance allowing to share data with specified third parties and/or specified types of third parties.

Screen 12:

(H) The national law of Your country of residence (at the moment of registration) is applicable to this contract, assuming you are a resident of the EU.

By clicking the box below You become a party to this agreement:

To prevent any confusion about the applicable national law, and to accommodate the natural person whose personal data are being processed we confirm that the national law of the end-user (data subject) of the USEMP platform is applicable. Under current EU Data Protection Law this seems the most apt, also for the modular version of the DLA (section 4.5). This may change when the General Data Protection Regulation (GDPR) comes into force in April 2018.

4.3. The USEMP PDPA

The USEMP DLA is included in an internal agreement between the USEMP Consortium Partners. This internal agreement, which we call the USEMP Personal Data Processing Agreement (PDPA), specifies which partner will do what kind of processing of personal data, and determines that and how the Consortium Partners are legally bound to treat the personal data they are processing. It also includes a clause which binds each partner to the DLA. We note:

- The USEMP partners act as joint data controllers because they have jointly determined the purpose of the processing of personal data within the USEMP project, namely scientific research as explicated in the DOW, the DLA and the PDPA.

- The DLA is part and parcel of this contract; the PDPA is an irrevocable offer to DataBait end-users to conclude the DLA contract. A link will be placed in the DLA to the DPDA contract.
- The PDPD contains strict obligations in terms of the appropriate security measures regarding the capture, storage and transmission of personal data, based on a risk assessment performed by each partner.
- The PDPA thus clarifies to the end-users of the USEMP tools which partner does what kind of processing of data and, finally exonerates partners from liability for data processing performed by other partners over which they have no actual control.
- The PDPA also addresses the user-friendly, layered and precise information to which end-users of the USEMP platform (data subjects) are entitled by stipulating that two buttons will be visible and operational on the platform's website: (1) to obtain more detailed information about the way USEMP Consortium Partners are bound to deliver on the contract, by showing the PDPA contract and by adding a table which shows in even more detail what data are processed how and for what reasons in the design of the USEMP architecture; and (2) to obtain from the USEMP Consortium Partners the erasure of their sensitive data or the removal of the DataBait tools.

Below we reproduce the complete PDPA:

USEMP Personal Data Processing Agreement (PDPA)

The parties:

(1) CEA-France,
(2) iMinds-Belgium
(3) CERTH-Greece
(4) HWC-UK

(5) LTU- Sweden
(6) VELTI-Greece
(7) SKU Radboud University-the Netherlands

having concluded the USEMP Consortium Agreement, being providers of the USEMP platform and the DataBait application and services, and being joint data controllers,

Hereby agree:

(A) Each party will comply with and perform in accordance with the USEMP Data Licensing Agreement (DLA, as attached to this contract) when processing the personal data of DataBait users, who are defined as the USEMP end-users who have signed the DLA with the USEMP Consortium Partners.

(B) Each party will comply with their national and EU data protection law, including notification of their national Data Protection Authority if necessary under their national law, when processing the personal data of DataBait users or any other personal data processed in the context of USEMP.

(C) Each party will provide precise information on what type of personal data they process concerning DataBait users, how it is processed and which data-flows they enable. This information will be available for DataBait users after clicking a specified button that can be accessed through the web interface of the DataBait application, and include an email address for each partner that processes personal data, to make further inquiries. The information will be updated whenever the relevant processing of personal data changes. Each party will also provide an email address to be contacted in case a user wants to withdraw her consent for processing her sensitive data; this is preferably the same email address as the one used to gain further information, but will be available behind a separate button that can be accessed through the web interface of the DataBait application.

(D) All parties shall carry out a personal information assurance risk assessment from their own context concerning their own collection, storage and/or processing of personal data, prior to deployment of the live service when personal data will be collected, and at any point through the operation of the system where there is a relevant change to either hardware installation, software versions, and/or software interfaces. Such a risk assessment shall follow information assurance principles covering, at least, hardware installation, software development processes, software validation and approval, software execution and backup processes. Each partner is liable for inappropriate security at its own premises.

(E) Parties agree that the following processing of personal data will be performed by the following parties:

CEA-France will conduct the following processing of personal data: via image recognition and text mining techniques CEA will infer potential preferences for specific objects, places and brands. No personal data of DataBait Users will be stored at the premises of CEA, that will be authorized to run its algorithms on the data stored at HWC.

iMinds Belgium will conduct the following processing of personal data: together with CERTH and LTU, iMinds will prepare a survey asking registered users of the USEMP platform and the DataBait application to answer a set of questions about their lifestyle preferences, selected health issues and personality traits, religious and political beliefs, sexual orientation, gender, age, place of residence and ethnic background. iMinds will conduct the survey to enable testing of how the inferences drawn from DataBait users' postings, social graphs and behavioural data match their real preferences and background. The outcome of the survey feeds into the database that is stored at HWC. iMinds can access the result of the survey based on secured authorization. The transmission of these sensitive data will be done in a secure way by means of appropriate security protocols. iMinds will also conduct user interviews which contain personal user's information. Interviews will be anonymized, transcribed and stored in an appropriately secured server, only accessible to authorized iMinds personnel.

CERTH-Greece will conduct the following processing of personal data: via image, text mining and behavioural profiling techniques (involving the 'likes' and sharing of Facebook pages and visits to URLs) CERTH will make inferences about undisclosed demographic characteristics (gender, age, origin), place of residence, sexual orientation, personality and health traits, political opinions, religious beliefs, relationship status, living situation as well as potential lifestyle preferences, including those that may interest specific types of brands and enterprises. When developing the DataBait application, a small portion of DataBait user data will be stored at CERTH. In that case appropriate security protocols will be in force, considering the nature of the data. Data will be deleted or fully anonymized once they are no longer necessary for developing the DataBait tools. CERTH will be authorized to run its algorithms on the data stored at HWC.

HWC-UK will conduct the following processing of personal data: all data collected through the DataBait application are directed to and stored at HWC, who will secure the data and provide secure access to the USEMP partners for the sole purpose of scientific research as specified in the DLA contract and the description of work that is part of the Grant Agreement with the EU. During storage at HWC appropriate security protocols will be in force concerning storage and access. Data will be deleted or fully anonymized as soon as the scientific purpose as stated in the DLA agreement is fulfilled.

LTU- Sweden will conduct the following processing of personal data: together with CERTH and iMinds, LTU will prepare a survey asking registered users of the USEMP platform and the DataBait application to answer a set of questions about their lifestyle preferences, selected health issues and personality traits, religious and political beliefs, sexual orientation, gender, age, place of residence and ethnic background. LTU will conduct the survey to enable testing of how the inferences drawn from DataBait users' postings, social graphs and behavioural data match their

real preferences and background. The outcome of the survey feeds into the database that is stored at HWC. LTU can access the result of the survey based on secured authorization. The transmission of these sensitive data will be done in a secure way by means of appropriate security protocols. LTU will also conduct user interviews which contain personal user's information. Interviews will be anonymized, transcribed and stored in an appropriately secured server, only accessible to authorized LTU personnel.

VELTI-Greece will conduct the following processing of personal data: based on the inferences made by CEA and CERTH, VELTI will conduct further processing operations to visualize information on potential inferences to be provided to the DataBait users. Velti will also use additional Facebook data of DataBait users, stored at HWC, for the visualisation of user's demographics and other statistical information. Some of this data may be retrieved from HWC and stored temporarily at VELTI for preliminary testing. In that case appropriate security protocols will be in force, considering the nature of the data. Data will be deleted or fully anonymized as soon as the purpose of such testing is achieved.

SKU Radboud University-the Netherlands will not conduct any processing of personal data.

(F) Each party that processes personal data hereby exempts all other parties from liability for any unlawful processing of personal data, and from processing personal data in violation of the USEMP DLA or this PDPA. Thus parties will not be severely liable for violations committed by other parties.

(G) Belgium law will be applicable to this contract.

Signature page USEMP PDPA

	Date	Place	Name/function	Signature
(1) CEA-France				
(2) iMinds-Belgium				

(3) CERTH-Greece

(4) HWC-UK

(5) LTU- Sweden

(6) VELTI-Greece

(7) SKU Radboud University-the Netherlands

4.4. A modular DLA

In this section we present a *modular* version of the DLA, which could be used by different types of providers of profiling transparency tools (modularity 1) and with regard to different OSNs and browsers (modularity 2).

Modularity 1:

Who is the provider of the profile transparency tool?

(a) another scientific consortium (not USEMP)

(b) an OSN (either simulating inference mechanisms or providing insight in the real inference mechanisms)

(c) a third-party commercial provider

(d) an NGO (e.g. a civil society or consumer organization) or aprivate nonprofit organization with a public goal (e.g. a charitable organization).

Modularity 2:

Profile transparency with regard to which OSN/browser?

(a) Facebook

(b) Twitter

(c) Facebook and Twitter

(d) Another OSN (e.g. Instagram)

(e) Chrome

(f) Firefox

(g) Chrome and Firefox

(h) Another browser

With regard to the first modularity we show how the DLA should be modulated if the provider of a transparency tool was (a) another scientific consortium, (b) an OSN, (c) a third-party commercial provider, (d) a NGO (e.g. a civil society or consumer organization) or a private nonprofit organization with a public goal (e.g. a charitable organization). We think that it is most likely that a profile transparency tool would be offered by an independent third party such as a commercial provider, a NGO or a nonprofit organization. If the transparency tool would be provided by an OSN the question would be if the OSN would give insight in the actual inferences made (and how we would know that this information was reliable), or whether it would offer a 'simulation'-tool (showing possible inferences instead of the actual ones) like *DataBait*. While it does not seem very likely that an OSN would provide a transparency tool like *DataBait*, we do not want to exclude the possibility that an OSN could be the provider.

With regard to the second modularity we explore how the DLA would look when the profiling transparency tool would apply to (a) Facebook, (b) Twitter, (c) both Facebook and Twitter, (d) another OSN, (e) a browser like Chrome or Firefox, or (f) another browser. The second modularity ('*Profile transparency with regard to which OSN?*') is relatively easy to incorporate: because the DataBait tool created by the USEMP project relates to data gathered from Facebook, Twitter, and a browser like Chrome or Firefox, this is simply a matter of removing any superfluous wording. The first modularity might require more adjustments to the DLA, notably with regard to the purpose of the processing, which will have to be extended or adapted.

In deliverable D3.11 we further adjust the DLA by adding an extra Article to also cover the licensing of content protected by intellectual property (IP) rights (notably copyright), such as certain types of pictures, videos and status updates. In that deliverable we also show how this particular article will have to be adjusted in the modular version of the DLA, depending on whether the service provider is commercial, non-profit or scientific (in the latter two cases

some exceptions might apply and reproduction could be possible in some cases without infringing on the copyright protection of the content). However, in this deliverable we leave IP licensing aside and purely focus on the licensing of personal data (see above, section 2.3.2,. for an explanation of the difference between IP licensing of copyright protected content and 'ordinary', non-IP, licensing of personal data).

Screen 1:

Data License Agreement

The parties:

(1) [……], user of the _____ platform and services, from hereon called 'You' and

(2) [_____], the data controller(s), from hereon called '_____' .

Hereby agree:

Screen 2:

(A) You will install the following tools, apps, plug-ins and/or graphicuser interfaces:_____ The _____ app and the _____ web browser plug-in will provide access to Your Facebook/Twitter/other OSN profile and Your browsing behaviour on Your device(s). These tools will be used by '_____' [*name of the the service provider-data controller*] to collect data that You share on Facebook/Twitter/other OSN as well as data collected by the web browser. This data can be data You posted (volunteered data), or data captured by the _____ tools (observed data). The latter concerns online behavioural data (storing what You did on the Internet and on Facebook/Twitter/other OSN).

This article defines the obligation to install the DataBait tools, which is pertinent for using any profile transparency tool of this type. It can be used in all modular versions.

Screen 3:

C) The data we gather through the _____-application may contain creations (such as images, photos, text, video) protected under copyright or neighbouring rights. These protected creations will be copied and stored on our servers and adapted for the purposes of our research (_____). We will not commercialise Your creations or distribute these to third parties. We will not communicate Your creations to the public: Your creations will only be made available to You (when You access the _____ application via the web interface) and to _____You agree with this use of Your creations covering the worldwide territory, for the duration of our research project. You will not receive any remuneration but You will have access to our research results.

This Article allows for the reproduction of copyright protected content for profiling purposes. It needs to be adapted to the particulars of the transparency tool. This is important because, in distinction from the 'blank check'-copyright licenses found in the terms of service of many large internet companies (which could potentially turn out to be not legally valid because of their unspecified nature), we think it is important that any copyright clause is very specific.

Screen 4:

(D) You license the use of Your volunteered and observed personal data by the '_____' [*name of the service provider-data controller*] , as gathered by the the _____ app and the _____web browser plug-in for the purpose of _____ and – within that context – to provide You through the _____graphic user interface (GUI) with information about what third parties might infer based on Your sharing of information, and on Your online behaviour. The said data may be combined with publicly available personal data gained from other sources to infer more information about Your habits and preferences (inferred data).

This article, first, makes clear that this is a *quid pro quo* agreement, creating legal obligations on the side of the user (data subject) in the form of licensing the use of the data that will be processed by the data controller, and on the side of the service provider (data controller) in the form of providing a form of profile transparency. This can *quid pro quo* form (performance on both sides) can be used in all modular versions. However the specific purpose of processing will depend on the type of service provider and the rationale/business plan behind the service.

Screen 5:

(E) This license agreement confirms Your explicit consent to store the_____ tools on Your devices.

This article provides the consent required on the basis of art. 5.3 ePrivacy Directive for all and any tracking mechanisms to be stored on the user's (data subject's) device. This article can be part of all the modular versions of the DLA.

Screen 6:

(F) The '_____' [name of the the service provider-data controller] will use analytic software/do research [*cross out what is not applicable*] to predict what kind of information Facebook/Twitter or other third parties with access to Your postings and online behavioural data could or might infer from the said data. These inferences will be shared with You in an intuitive manner, thus providing an online presence awareness tool, embedded in the "_____GUI".

This article further explains the obligation on the side of the service provider, and the purpose of processing, highlighting that the profile transparency which will be provided is based on statistical inferences by others than OSN providers, meaning that the user is made aware of the fact that the data controller are not reverse engineering software code of the

OSN provider and cannot in any way provide certainty about how one may be targeted. This article also ensures that the transparency is provided in a user-friendly manner. This article is crucial in every modular DLA for a profile transparency tool. However, the precise content of this article will have to be adapted according to the particularities of the service provided. Not every service provider of a transparency tool will have (scientific or commercial) research purposes. This will also have to be adapted according to the particularities of the service and the provided tool.

Screen 7:

(G) You agree to participate in surveys and/or focus groups, to enable '_____' [*name of the service provider-data controller*] to gain insights in how users engage with social networking sites and how they evaluate (1) various scenarios regarding the use of their personal data and targeted profiles and (2) the effectiveness, usability and utility of the provided tools.

This article may be part of the modular version of the DLA depending on the particularities of the transparency tool and the services accompanying it.

Screen 8:

(H) You hereby grant Your consent to process Your sensitive personal data, notably those revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and those concerning health or sex life.

Since consent is required for processing art. 9 GDPR types of data, this article stipulates such consent. It highlights the intrusive nature of the processing of such data. It is part of every modular version of the DLA.

Screen 9:

(I) '_____' [*name of the service provider-data controller*] will treat all Your personal data, especially Your sensitive data, with care and delete or anonymize them as soon as possible.

See commentary below the next Article.

Screen 10:

(J) '_____' [*name of the service provider-data controller*] will process Your personal data in a secure way and not keep them any longer than necessary for the purposes described in Article D. In order to provide You with access to Your personal data and the inferences drawn from them, the data may be kept until the end of the project. Within ____ months of the ending of the project all personal data will be either deleted, anonymised or processed for related scientific research. In the latter case '_____' [*name of the service provider-data controller*] will ask You for Your consent.

Articles I and J confirm the legal obligation for the service provider-data controller that the relevant data will be processed in accordance with the data minimisation principle, stipulating deletion or anonymisation as soon as possible (including a clear deadline) and security by design, while also explaining that to provide profile transparency the processing

of both personal and sensitive personal data is necessary. These articles are part of all the modular versions of the DLA considering that this is a confirmation and reminder of the legal obligations of the service provider (data controller).

Screen 11:

(K) '_____' [*name of the service provider-data controller*] will not provide Your personal data to any third party other than _____. The transfer of the data will happen in a secure way and only in as far as strictly necessary for the purposes decribed in Article D.

This article is pivotal to ensure that data are not processed beyond the explicitly specified purpose. The article can be modulated depending on the specifics of the modular version of the DLA, for instance allowing to share data with specified third parties and/or specified types of third parties.

Screen 12:

(L) The national law of Your country of residence (at the moment of registration) is applicable to this contract, assuming you are a resident of the EU. By clicking the box below You become a party to this agreement:

To prevent any confusion about the applicable national law, and to accommodate the natural person whose personal data are being processed each modular version of the DLA has to confirm that the national law of the user (data subject) of the provided profile transparency tool is applicable. Under current EU Data Protection Law this seems the most apt, also for any of the modular versions of the DLA. This may change under the proposed General Data Protection Regulation (GDPR). Moreover, if the service would also be provided to non-EU residents, this clause would have to be adjusted.

What if data subject and controller could reach a mutual agreement on the re-use and on the sharing of the personal data? In this chapter we explore how *granular* licensing of personal data use could stimulate transparency and put the data subject and controller on more equal footing. The licenses we propose are granular in a double sense. Firstly, the licenses are granular because they offer an alternative to the 'all-or-nothing' consent ('Either you agree with this set of data processing modalities or you cannot use this service') which is often required when using services on today's internet. Granular licensing could be a way of offering data subjects a break down in different options of choice. Secondly, the licenses are granular because they have a layered format: a layer specifying the legal intricacies, a layer which can be easily grasped by a lay person and a machine readable layer.

5. Conclusion

In this deliverable we followed four research strands.

The first research strands looked at how the DataBait tool incorporates (“Data Protection by Design”) profile transparency. According to EU data protection law any data controller who processes data in order to profile data subjects has to provide them with profile transparency, that is, “meaningful information about the logic involved” and about the “significance and the envisaged consequences” of the profiling. Such profile transparency, provided by the data controller in order to comply with EU data protection law, is first party transparency. Next to this, there also can be independent, third party providers of profile transparency that aim to give additional empowerment to users in their relation towards other data controllers. Such tools support the user in exercising her informational rights by providing her insight in the data she shares with other data controllers. It aims to answer pressing questions such as: What information do I share? What can be derived from it? Who is tracking me?)

DataBait is both a first party provider of actual profile transparency (giving users insight in how the USEMP consortium processes the data of DataBait users) as well as an independent, third party provider of speculative profile "transparency" (showing what could be extracted) with regard to the processing performed by large Online Social Networks (OSNs) such as Facebook.

In terms of first party transparency this deliverable checked how DataBait's compliance with EU data protection law (which includes the provision of profile transparency) could be realized to the fullest and most optimal extent. This resulted in a set of design requirements, which include the Data Licensing Agreement (DLA) and the information provided in the "DataBait: How, what, why?"-section within the DataBait tool.

In terms of third party transparency we analysed in this deliverable how DataBait relates to other tools providing such transparency. Many third party providers of profile transparency function by matching input to output: which changes in a profile (input) result in which changes in the advertisements, newsfeeds, etc. one is served (output)? DataBait stands out in relation to other third party providers of profile transparency by only looking at the input. By analyzing the input with its own algorithms DataBait shows what is possible to infer from user data given the state of the art, instead of trying to reverse engineer what happens in a profiling blackbox by matching input and output. DataBait's "input speculation" and the "input-output matching" of other third party providers of profile transparency are complementary approaches that each have their own benefits and drawbacks. In future research it would be important to explore how both approaches can be combined.

The second strand of research in this deliverable looked at potentials to combine transparency tools with personal data management (PDM) systems. DataBait is "merely" a third party transparency tool – not a PDM provider. However, in thinking ahead about future applications of third party transparency tools like DataBait, we explored the combination of a transparency tool and a PDM solution because this sounds, at first sight, very attractive. Such a tool could (1) provide for an easy way to translate transparency insights in actions with regard to user permissions, and ensure (2) that user data can only be accessed according to the user permissions ('granular licensing'), and (3) that any transfer happens under the same conditions as the ones guiding the relationship between the user and the PDM/transparency tool provider: any further use of user data would only be allowed in exchange for profile transparency. As such a PDM/transparency tool allowing for such granular licensing could hold the promise to enable use and re-use of data under truly fair and transparent conditions – one of the Holy Grails in the current EU ecology of data processing. However, based on the results of our research these high hopes cannot be fully realized – at least not in the context of OSN data. We noted that in the case of transparency tools like DataBait (aimed at OSNs and browsers) such a combination is problematic in terms of the purpose limitation principle as this principle prohibits any blank checks – even limited blank checks! – with regard to how data may be used. Moreover, it would put the independent position of DataBait at risk. The empowering strength of DataBait lies exactly in its position as an independent provider of transparency, not as a mediator between users and businesses/organisations looking for user data. Finally, why would users trust a minor actor with their data? And what incentive would they have to share data beyond what they already share with the OSN and OSN applications?

However, we also noted that a PDM/transparency tool allowing for 'granular licensing of personal data' might be useful in other contexts (such as in the use and re-use of medical

patient data by as hospital). We then explored how the distinction between functional and non-functional cookies and the format and functioning of Creative Commons licenses could inform such contractual granular licensing system. Here more future research is needed.

The third strand of research in this deliverable gave *a legal clarification* of which data should be considered *'sensitive'* in the sense of Art. 8 DPD 95/46, and which data can be considered *anonymous* (i.e., not personal data and therefore outside the scope of DPD 95/46). We concluded that in assessing whether data are truly anonymous their potential for de-anonymization should be taken into account.

In assessing whether data are *anonymous*, it is not enough that data are not directly related to an identified or identifiable person, because the possibility of singling out, re-linking and inferring information should be taken in to account. In our present age, the risk for de-anonimization in general is very large: given the fast technological progress and the fast amounts of available data de-anonymisation by, for example, combining different data sets is difficult to fully exclude. As Working Party 29 states: "Real anonymization is only possible if "the prerequisites (context) and the objective(s) of the anonymisation process [are] clearly set out in order to achieve the targeted anonymisation […]. The optimal solution should be decided on a case-by-case basis, possibly by using a combination of different techniques, […]." In the USEMP project we avoid opening Pandora's box of possibilities for de-anonymization by simply deleting the DataBait data. However, it should be noted that simple guidelines for researchers might be helpful : it would be a pity if valuable data would be simply deleted because researchers do not want to burn their fingers on anonymization issues. On the other hand, simply storing anonymized research data in anticipation of an unknown future in which they might be of some use should not be a goal in itself.

In assessing whether data are to be considered *sensitive*, it is also their potential that should be taken into account: can sensitive data potentially be inferred? We propose that in non-obvious cases the crucial notion in assessing whether this potentiality is relevant for the legal qualification 'sensitive' is the *intended use* (realistic possibility and significant chance that sensitive information will be extracted and used, given the concrete circumstances). Consequently we recommended that the DataBait user should be given realistic examples of the intended uses for which the inferred information could be used. The protected grounds from EU anti-discrimination law and the categories of sensitive data from EU data protection law were used in designing the USEMP privacy model on which the DataBait tool builds. The DataBait tool shows users whether these data categories (in combination with some other data types which users in the DataBait user studies designated as 'sensitive') could be inferred from their raw OSN and/or browser data.

The fourth strand presents the Data Licensing Agreement (DLA), which offers an alternative to the 'take-it-or-leave-it-approach' of consent as a legal ground for processing personal data by engaging the data subject in the process of profiling. Before using DataBait each user should sign the DLA. The DLA creates more of a level playing field between data controller (service provider) and data subject (end user) by means of an obligatory agreement that entails clear and mutual *quid pro quo*, while providing transparency about all the relevant legal issues when using *DataBait*. While in principle each data subject has certain data protection rights (including a right to profile transparency), they are strenghtened if they are backed by a contract.

It is important to underline that the DataBait DLA is not just any "service contract" or "Terms of Service". Firstly, the DLA is centered on the idea that we only process data that

are strictly necessary for the performance of the contract. The distinction between necessary data processing and non-necessary processing is inscribed in an increasing amount of legislation: e.g. Art. 7(4) GDPR, the Art. 5(3) of the e-Privacy Directive 2009/136 (on functional cookies) and several articles in the upcoming Directive on Digital Content COM/2015/0634 final - 2015/0287 (COD). Secondly, the DLA builds on a very particular *quid pro quo*: profile transparency in exchange for data. While every user has a right to profile transparency, this right is strengthened if the data controller is contractually bound to it as well and if the contract specifies what profile transparency will be provided.

6. Bibliography

Article 29 Data Protection Working Party 29. (2013). Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013.

Article 29 Data Protection Working Party. (2012). Opinion 04/2012 on Cookie Consent Exemption.

Article 29 Data Protection Working Party. (2014). Opinion 05/2014 on Anonymisation Techniques (Adopted on 10 April 2014).

Article 29 Data Protection Working Party. (2015a). Annex to the letter (Brussels, 05 February 2015) to the European Commission on health data in apps and devices.

Article 29 Data Protection Working Party. (2015b). Letter (Brussels, 05 February 2015) to the European Commission on health data in apps and devices.

Asgharpour, Farzaneh, Liu, Debin, & Camp, L Jean. (2007). Mental models of security risks *Financial Cryptography and Data Security* (pp. 367-377): Springer.

Camp, L Jean. (2006). Mental models of privacy and security. *Available at SSRN 922735*.

Custers, Bart, & Uršič, Helena. (2016). Big data and data reuse: a taxonomy of data reuse for balancing big data benefits and personal data protection. *International Data Privacy Law*. doi: 10.1093/idpl/ipv028

Datta, Amit, Tschantz, Michael Carl, & Datta, Anupam. (2015). Automated experiments on ad privacy settings: A tale of opacity, choice. and discrimination. *Proceedings on Privacy Enhancing Technologies, 2015*(1), 92-112.

European Commission. (2012). FREQUENTLY ASKED QUESTIONS RELATING TO TRANSFERS OF PERSONAL DATA FROM THE EU/EEA TO THIRD COUNTRIES.

European Union Agency for Fundamental Rights, Council of Europe. (2014). *Handbook on European data protection law*. Luxembourg: Publications Office of the European Union.

Hildebrandt, Mireille. (2014). Location Data, Purpose Binding and Contextual Integrity: What's the Message? *Protection of Information and the Right to Privacy-A New Equilibrium?* (pp. 31-62): Springer.

Koning, Merel. (2014). *Purpose Limitation and Fair Re-use*. Paper presented at the Computers Privacy and Data Protection 2014, Brussels.

Koning, Merel, Korenhof, Paulan, & Alpár, Gergely. (2014). *The ABC of ABC. An Analysis of Attribute-Based Credentials in the Light of Data Protection, Privacy and Identity.* Paper presented at the PETS 2014: The 14th Privacy Enhancing Technologies Symposium Amsterdam, Netherlands

Lecuyer, Mathias, Spahn, Riley, Spiliopolous, Yannis, Chaintreau, Augustin, Geambasu, Roxana, & Hsu, Daniel. (2015). *Sunlight: Fine-grained targeting detection at scale with statistical confidence.* Paper presented at the Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security.

Martineau, Kim. (2015). New Tool Expands Tracking of Personal Data on the Web. Columbia Researchers Present "Sunlight" at Computer Security Conference *Data Science Institute, Columbia University*. http://datascience.columbia.edu/new-tool-expands-tracking-personal-data-web

Narayanan, A, & Shmatikov, V. (2008). Robust de-anonymization of large datasets (how to break anonymity of the Netflix prize dataset). 2008. *University of Texas at Austin*.

Ohm, Paul. (2010). Broken promises of privacy: Responding to the surprising failure of anonymization. *UCLA Law Review, 57*, 1701.

Ribeiro, Marco Tulio, Singh, Sameer, & Guestrin, Carlos. (2016). " Why Should I Trust You?": Explaining the Predictions of Any Classifier. *arXiv preprint nr. 1602.04938*. http://arxiv.org/abs/1602.04938

Simonite, Tom. (2015). Probing the Dark Side of Google's Ad-Targeting System. *MIT Technology Review*. https://www.technologyreview.com/s/539021/probing-the-dark-side-of-googles-ad-targeting-system/

Skeggs, Beverley, & Yuill, Simon. (2016). The methodology of a multi-model project examining how facebook infrastructures social relations. *Information, Communication & Society, 19*(10), 1356-1372. doi: 10.1080/1369118X.2015.1091026

Uršič, Helena, & Custers, B. (2016). D2.2 Report on the legal analysis. EuDEco (Modelling the European data economy).