Kortesniemi, Yki; Kremer, Jens

Recommendations and Automation in the Consenting Process

Published: 12/12/2018

Please cite the original version:
Kortesniemi, Y., & Kremer, J. (2018). *Recommendations and Automation in the Consenting Process: Designing GDPR compliant consents*. Paper presented at Legal Design as Academic Discipline: Foundations, Methodology, Applications, Groningen, Netherlands.

Recommendations and Automation in the Consenting Process

Designing GDPR Compliant Consents

Yki Kortesniemi
Department of Computer Science,
Aalto University, Finland
Yki.Kortesniemi@aalto.fi

Jens Kremer
Faculty of Law,
University of Helsinki, Finland
Jens.Kremer@helsinki.fi

Giving consent to the processing of personal information can be complex. Under the GDPR, to be valid, a consent has to present a 'freely given, specific, informed and unambiguous indication of the data subject's wishes' -- requirements, which can be difficult for the controller to meet. But choice and consent can also be burdensome for data subjects as, for instance, being truly informed of personal data processing operations and their consequence may require serious efforts and deep understanding of technical and societal processes. This paper looks at using recommendations and automation to provide a better consenting process under the GDPR. In particular, the paper analyses four scenarios of increasing automation, and finds that while recommendations are an acceptable way for improving the consent process, fully automated consenting is difficult to implement under the GDPR.

I. Introduction

Consent has long been held in many legislations as one of the legal bases for processing personal information, and rests on the idea that individuals, whose personal information is being processed, is thereby able to control their personal information. Though theoretically highly empowering for the individual, in practice consenting comes with a variety of fallacies[1] due to the way the consenting process is implemented, and does not always empower the individual quite as much as the ideal suggests. This situation is also reflected in new regulations on data protection: the General Data Protection Regulation (GDPR) reworks the European consent framework and therewith attempts to guarantee truly free choices, tackles power imbalances and sets strict requirements for transparency.[2] The GDPR does provide five other legal bases for processing personal data, which in many cases can be more appropriate than consent, but when consent is chosen as the basis, it should be implemented so that the ideals of the law are realised as much as possible without undue burden to the individual.

The difficulty of consenting stems from eight obstacles, which can be ranked in three groups based on their hardness: *solvable*, *challenging*, and *insuperable*.[3] The first of the *solvable* obstacles, *timing & duration,* refers to the fact that consent to the use of data is given when processing begins, while the harms and

[1] Tuukka Lehtiniemi and Yki Kortesniemi, 'Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach, Big Data & Society (2017)

[2] 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), OJ L 119, 4.5.2016, p. 1–88.; Arts 6,7.

[3] Tuukka Lehtiniemi and Yki Kortesniemi, 'Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach, Big Data & Society (2017)

benefits of processing accumulate over time[4] and may be the result of data analysis techniques,[5] some of which may not even exist at the time of consenting. The second solvable obstacle, *non-negotiability,* describes the fact that individuals are often not free to negotiate the consent details but have to accept the terms of the service as defined by the controller[6] or not use the service at all - an issue the GDPR is addressing. The third solvable obstacles, *scale,* refers to the large number of decisions and the amount of effort behind each decision. As an example, McDonald and Cranor estimate that it would take 80-300 hours for the the average individual just to read the privacy policies of the websites they visit in a year,[7] let alone all the other services used in everyday life. These three obstacles are *solvable* because they are not fundamentally insurmountable but rather the result of how consenting has been implemented.[8] Legal regulation, setting stricter requirements for valid consent, as well as better tools and user interfaces, can help make these obstacles manageable.

The next three obstacles are classified as challenging. They can be partially solved with better tools, but also contain elements that are insurmountable. Firstly, the *aggregation* obstacle refers to a data subject's difficulty to assess the effects of data processing operation. Complex processing may, for instance, aggregate data from multiple sources unknown to the data subject (something the GDPR is addressing), or data analytics[9] may reveal more detailed information from existing data sets, both of which can significantly affect a data subject's' potential cost-benefit analysis behind the consenting decisions.[10] The second obstacle in this group are the *downstream uses* of data. This refers to the effect that the consented processing of data expands without further consent. This happens e.g. when the authorised data processor transfers information to third parties[11] or when a malicious actor gains unauthorised access. Data subjects would not know or foresee all such downstream uses, and can therefore not consider them when giving consent to processing. The third challenging obstacle, *cognitive* demands refer to conceptual problems of humans as rational decision makers.[12] Due to limitations in information, cognitive capabilities, and the available time, data subject may act only boundedly rational,[13] showing the fallacies of consent and choice theories.

The final group of obstacles relate to the social aspects of humans. They are considered *insuperable* because an individual-focused privacy self-management model simply cannot fully address them. Firstly, the obstacle of *social norms* refers to social conventions that force people to behave differently than they otherwise would,[14] e.g. sometimes reveal more of themselves because social networking services are now regarded as an integral part of modern life.[15] Secondly, the *social nature* of personal data refers to the fact that some personal data reveals information about other people, e.g. when a cooperation with others also

[4] Daniel J. Solove, 'Privacy self-management and the consent dilemma', Harvard Law Review (2013)

[5] Bart Custers, 'Click here to consent forever: Expiry dates for informed consent', Big Data & Society (2016)

[6] Bart Custers, 'Click here to consent forever: Expiry dates for informed consent', Big Data & Society (2016)

[7] Aleecia McDonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies', I/S: A Journal of Law and Policy for the Information Society (2008)

[8] Tuukka Lehtiniemi and Yki Kortesniemi, 'Can the obstacles to privacy self-management be overcome? Exploring the consent intermediary approach, Big Data & Society (2017)

[9] Jens-Erik Mai, 'Big data privacy: The datafication of personal information', The Information Society (2016)

[10] Daniel J. Solove, 'Privacy self-management and the consent dilemma', Harvard Law Review (2013)

[11] Gary Anthes, 'Data brokers are watching you', Communications of the ACM (2015)

[12] Daniel J. Solove, 'Privacy self-management and the consent dilemma', Harvard Law Review (2013)

[13] Gerd Gigerenzer and Reinhard Selten, 'Bounded Rationality, The Adaptive Toolbox' (2001)

[14] Alessandro Acquisti, 'The economics of personal data and the economics of privacy', 2010

[15] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization', Journal of Information Technology (2015)

reveals information about the other parties. Hence, revealing information about oneself can reveal information about others, which can have a harmful effect on them - and vice versa.

This article utilises legal design to improve the consenting process for the individual by exploring the existing approaches of recommendations and automation in the context of consenting and by evaluating to which extent they can be utilised within a GDPR-compliant legal framework. The article approaches this through four different scenarios (as shown in Figure 1) chosen to represent progressively more automated/delegated consenting processes, which can, therefore, be used to gauge roughly how far automation/delegation can be taken. Scenario 1 represents the current situation, where the individual personally finds any additional information necessary to make the consenting decision and then manually adjusts the settings to achieve the desired consent. Scenario 2 utilises specific recommendations from a source of the individual's choosing to reduce complexity. In scenario 3, the recommendations have been automatically input into the consenting system and the individual only makes a higher level decision. Finally, in scenario 4, a personal privacy assistant system automatically takes care of all consenting based on which systems the individual chooses to use or stop using. For each of the scenarios, the paper analyses how well it addresses the obstacles and the main legal requirements and limitations of that solution. The key finding is that under the GDPR, Scenarios 1-3 could be a feasible scenario for compliance, while Scenario 4 may be difficult to build in line with the GDPR.

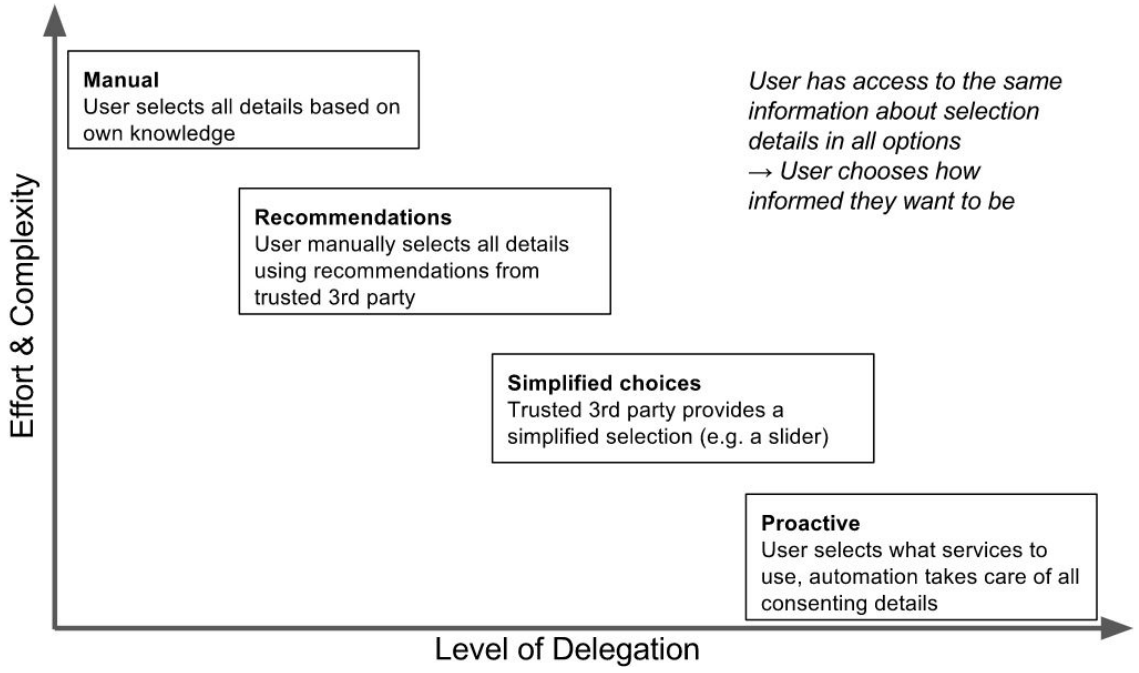

Figure 1: The four consenting scenarios

The rest of the paper is organised as follows: Sections II-V go over the four scenarios and Section VI discusses the findings.

II. Scenario 1: Baseline, Manual Consenting

Using consent for justifying data processing requires on one hand communicating the data processing operations to the individual, and on the other hand justifying and recording the use of consent before a public control entity in order to demonstrate compliance and accountability.[16] Here, the way of presenting

[16] The GDPR not only sets requirements for how to substantially acquire consent, but also obliges controllers to be

the options to consent is important, because user interfaces have the potential to manipulate, deceive or push for certain choices, while they could in fact be used to give real choices to data subjects.

The baseline Scenario 1 refers to a consenting interface similar (though perhaps better organised) as currently seen in many services. The interfaces provide the information the data controller deems necessary and the data subject manually chooses all relevant options to indicate, to what they want to consent. Whatever additional information the data subject feels they need to truly understand the consenting options the data subject has to find themselves as there are no third party recommendations available to help them decide nor is there any automation to reduce the number of (repetitive) decisions they have to make for similar services.

The above described obstacles highlight the need to grant individuals real and detailed choices while at the same time maximizing simplicity and comprehensiveness in order to avoid problems related to the scale of information. Presenting large amounts of options, explanations and selection to a data subject may certainly grant real choices to individuals, but at the same time it may hinder clear, informed and unambiguous consent in practice. One way of approaching this is to separate data processing purposes from the data types and require actively consenting to both: the reason for personal data processing as well as to the required types of personal data processed. And if some data type is vital for a particular purpose, that data type should not be deselectable by the data subject, though the purpose itself should then be optional. Figure 2 shows an example, where for the purpose of creating graphical statistics of latest sports activities, the data controller needs recorded activity data from a movement sensor, but not necessarily the time of the workouts, so the latter data type should be optional. The data controller can also provide other optional processing, e.g. sharing the activity data for scientific data or more advanced analytics to get further insight to the effects of sports activities.

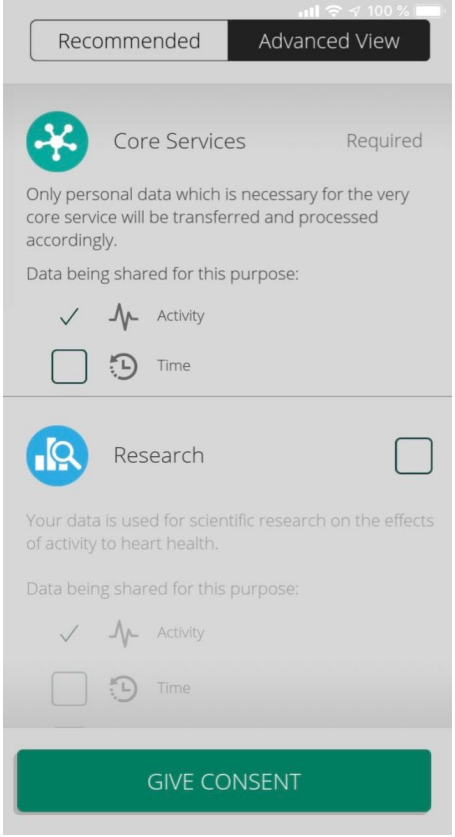

Figure 2: Example UI showing purposes with selectable data types

Regarding the obstacles of consenting, the example above presents a somewhat straightforward solution. The uncontrolled aggregation of personal data as an obstacle for evaluating negative privacy effects or invisible flow to third parties could be tackled with such a consenting interface, as the user would be presented with detailed information on where, how and what kind of personal data is processed for which purposes. The problem of timing and duration could be reduced by limiting the consents to a suitable period or nudging the data subject to re-evaluate the consent eg.g when circumstances change or at suitable intervals. The decisional problem of non-negotiability is addressed by actually enabling the use of a service without the need to grant unfettered consent to all sorts of data processing, and the problem of cognitive limitations and scale can be (partially) tackled with an easily accessible and understandable user interface.

A manual interface as described in the example above therefore goes in line with the object and purpose of

able to demonstrate compliance and record processing activities. Accountability is therefore a core element in the regulation of personal data processing. See Arts 5 (2), 24 (1), 30 GDPR.

the GDPR. Through the consent interface, individuals are given complete information and real choices about the levels of data processing. They are informed about precisely which types of data are processed for each purpose. Depending on the surrounding conditions and particular use of such an interface, an informed and uncoerced choice appears possible. However, the increased complexity of such interfaces may make it difficult and time consuming for the data subject to engage with. Separately listing processing purposes and data types can result in the availability of a vast amount of different choices and options, and pre-selecting data types based on defined processing purposes could result in an impenetrable jungle of choices and options, especially for services that offer a wide array of complex personal data processing operations.

III. Scenario 2: Utilising Recommendations

One of the challenges of consenting is that to make an truly informed decision, the data subject may have to spend significant effort to find enough relevant information (in addition to the information provided by the data controller) relating to the different aspects and consequences of a consent - and some of the information can be hard to obtain, e.g. information relating to the Aggregation and Downstream use obstacles. One solution could be to utilise information from an independent source (a *recommender* the data subject has chosen) to reduce the complexity and required effort. Depending on the trust relation with the recommender and the level of risk/worry involved, the data subject could then simply copy the recommended settings or conduct further evaluations based on the provided information.

In such a system, individuals would have full control over processing operations and can make all possible choices - including the freedom to choose, on which information and recommendations they want to base their consenting decisions. So, as long as the recommendations to consent do not impede a user's decisional freedoms or make false claims, they would not contradict the conditions for consenting in the GDPR. Recommendations could even be used to improve informed consent by providing critical reflections to a data subject. Furthermore, recommendations can significantly simplify the consenting process, which reduces the scale and cognitive obstacles. A more refined form of providing information on consenting consequences and choices would be specific recommendations on how to consent (or not) in a given situation. The challenge with this is that people have very different privacy preferences[17] which can change over time[18], and which depend on the context.[19] Therefore, recommendations on choices in consenting interfaces need to be highly personalised to be of value. The individual's privacy preferences could e.g. be condensed into a *privacy profile* and different recommendations could be made available to match the privacy profiles.

IV. Scenario 3: Simplified Choices

Even with good specific recommendations, a problem may still arise from the complexity and scale of consenting activity as a whole. If a user e.g. actively uses a large variety of data processing services, consenting operations may develop into a burdensome exercise, particularly, if the individual feels that they are answering the same question for each new service. Additional recommendations may therefore not be enough to create a user-friendly consenting environment as utilising them still requires manually copying the recommended settings, which could create a laborious process fraught with possible errors from which

[17] Chris Hoofnagle and Jennifer Urban, 'Alan Westin's Privacy Homo Economicus', Wake Forest Law Review (2014)
[18] Alessandro Acquisti et al., 'Privacy and human behavior in the age of information', Science (2015)
[19] Sami Coll, 'Power, knowledge, and the subjects of privacy: understanding privacy as the ally of surveillance', Information, Communication & Society (2014)

new decisional, operational or even legal problems may emerge. This section therefore asks, can some or even all of the utilisation of the recommendations be automated so that the individual only has to make a higher-level decision and the relevant details can be delegated to the recommender (provided the individual is always free to adjust any of the details should they wish to do so)? This question is becoming increasingly relevant as automated, machine learning based assistants are increasingly being deployed in different fields of life, so their applicability to consenting decisions will have to be addressed.

The trusted 3rd party (chosen by the data subject) or a machine learning based assistant system could, e.g., process their recommendations (from Scenario 2) into a *slider* with only a few options as shown in Figure 3. The recommendations of what data types to choose for each purpose have been pre-selected and only the purposes have been put in a specific order along the slider - and the further the data subject sets the slider, the more data processing will take place. When utilising a slider, by default the Data Subject is only shown the slider, so the minimal flow to consent is to trust the recommended choices, move the slider to the desired position and press the consent button. However, the detailed choices for each slider position are readily available, so that a data subject can be as informed as in in a manual consenting flow, but doesn't have to if they choose to trust the recommendations. Effectively, the individual delegates the decisions regarding the details to the creator of the slider. To better match the varying privacy preferences, a trusted 3rd party can create several sliders, but to make the slider even better match the data subject's intentions, the slider could also be uniquely generated by a machine learning/AI algorithm by utilising data subject's privacy profile and other relevant information.

Figure 3: Example Slider

From a GDPR compliance perspective, recommendations and their implementation in a slider come with several challenges. Firstly, the GDPR explicitly specifies that 'silence, pre-ticked boxes or inactivity' do not constitute a sufficient expression of consent.[20] Furthermore, if an individual expresses consent to a specific personal data processing operation, the consent is purpose-specific. This means that using personal data for different purposes will require gathering expressions of consent separately. A user interface presenting grouped and summarized information during a consenting process somehow needs to ensure that the data subject is still informed enough and free to choose. Also, the difficulty of obtaining valid consent in light of the complexities of processing operations and societal interactions visible as a discussion within the GDPR needs to be addressed. On the one side, data subjects need to be provided with detailed information, on the other hand, Recital 32 of the GDPR explains that obtaining consent also needs to be 'clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.' And while consent needs to be obtained separately for each processing purpose which in itself requires to be specific, explicit and legitimate, it should be presented as '...intelligible and easily accessible form, using clear and plain language and it should not contain unfair

[20] GDPR recital 32.

terms.'[21]

With this, the GDPR does not give detailed instructions as to the form of consenting, but it specifies a set of principles and requirements that apply to any form of consenting. It focuses furthermore on individual's capabilities to consent freely and with a high degree of self-determination so that no form of asking for consent should be coercing or luring a data subject. After all, consent should not be obtained via illegitimate pressure, hidden strings or exploited power imbalances. Consequently, the validity of a simplification of a form of acquiring consent in partially automated or pre-selected forms depends on the 'honesty' of the given settings. This would mean, that the utilisation of recommendations requires the source to be truly impartial and to formulate recommendations in a way that they are easily understandable and accessible. In how far that is realistically possible would have to be tested in practice. Furthermore, it is also questionable and will need to be assessed in how far recommendations for very specific settings can really contribute to the improved consent interfaces. In light of the slider example, which basically employs certain form of recommendations derived from an entity which is not the data subject, it is important to establish mechanisms which preserve the independence and impartiality of a recommendation. In that sense, a 'right' form of presenting consent recommendations would assist or even enable individual (informational) self-determination, while a 'wrong' form of consenting would recommend consenting in the best interest of the data controller. More or less, both examples come therefore with a certain risk of coercion.

After the importance of the independence of the recommendation as well as the way the recommendations is used, the third aspect under scrutiny is the consent interface design as such, here represented in the slider. The GDPR, as discussed above, due to its technological neutrality, does not determine specific ways and methods of consenting, but instead sets principles which need to be fulfilled by the overall process of obtaining consent. Consent doesn't therefore need to obtained always by complex choices. The GDPR specifies for example that consent can also be obtained for example through certain 'technical settings'.[22] This, however should not lead to luring data subjects into consenting to vast and unnecessary data processing operations. In this regard, a slider as presented in the example above may be regarded as a technical setting through which a data subject can have sufficient control and choices regarding personal data processing, while at the same time not being overwhelmed with too much complex information. Here, a slider may be an adequate solution, provided that it contains an adequate representation of the existing data processing operations and activities and further information could be obtained.

V. Scenario 4: Proactive Consenting

The final scenario imagines an even more automated way of consenting, a personal privacy assistant system controlled by the data subject. It is a machine learning based system that keeps track of all the data subject's consenting activity, learns how the data subject behaves in different consenting situations, and after that can take care of all the consenting activity. So, the data subject simply starts using a service, changes how they use the service, or even stops using the service - and the privacy assistant automatically adjusts the consents (without involving the data subject) to best protect the data subject's interest. The data subject is free to view and manually modify all the consents at will, but as long as the privacy assistant functions well enough, the data subject does not have to. Effectively, the date subject has delegated all the consenting activity to the privacy assistant. While this is currently a hypothetical case, for some users not interested in managing their privacy themselves this option could maximise user friendliness and efficiency: based on

[21] Recital 42

[22] For example in case of consenting to data processing for information society services, see Recital 32.

predefined privacy profiles, an automated system would apply the calculated privacy preferences of data subjects to all data processing activities. Similar systems (though not fully proactive) have already been implemented and studied e.g. for managing the permissions of apps on mobile phones[23].

On first sight, automation of consent presents a contradiction to the basic ideas enshrined in the GDPR. That is because the GDPR explicitly mentions that inactivity or silence of data subjects and even the preselection of boxes shall not constitute a valid method of obtaining consent. It goes without saying that in this regard any automation of consenting is inherently prone to abuse in that individuals may be tricked into tacitly agreeing to processing activities that may not be in their interest. Furthermore, fully automated consenting is additionally problematic because it appears not to respect the requirement of separately consenting to processing activities for each specific purpose.

When basing consenting on privacy profiles and consent templates that determine the wishes and preferences of data subjects, many obstacles deriving from data protection regulation need to be addressed. Such a consenting profile would need to qualify as a free and informed decision of an individual to a processing operation for a specific purpose. It would be difficult to imagine, how a general consent expression done by a data subject at some point in the past could fulfil such requirements. It is highly likely that such a consent template would fall prey to strong data processing interests of controllers. Nevertheless, if such a consent template would be designed in a way that it gives the individual enough choices for review at the time of expressing consent, and if the actual expressed consent would not significantly depart from what a data subject would de-facto choose when presented with a fully 'manual' consent form, consent templates may be able to enforce better consenting mechanisms for data subjects.

Even better results could be achieved with sophisticated analyses and profiling at the time of consenting, as this has the potential of making the template more accurate for the situation at hand. Automated profiling, however, is highly problematic in European Data Protection Law. Profiling, prediction and automation may have serious effects on an individual, and the automation of decisions does limit the chance to express free choices up to the point of loss of self-determination. Furthermore, automated decision making and profiling may have inherent discriminatory effects, and anti-discrimination lies at the core of a normative framework of European Union Law and its fundamental rights and freedoms.[24] Consequently, the GDPR flags automated decision making as problematic. The GDPR defines profiling as 'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person'[25] and furthermore specifies that individuals have a right to not be subjected to decision '…based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.'[26] This means that any decisions with legal effects or other significant effects on individuals should not be made automatically without review of a real person and without the option to challenge or object to such a decision. The GDPR explicitly lists the 'automatic refusal of an online credit application' and 'e-recruiting practices' as examples of such automated decisions.[27] The creation of a profile of a person which contains preferences for consent has to be regarded as profiling and the use of such a profile to automatically consent to certain processing activities clearly has a significant legal effect on a person. Consequently, automatic consenting through the prediction

[23] Bin Liu et al., 'Follow My Recommendations: A Personalized Privacy Assistant for Mobile App Permissions', Proceedings of the Twelfth Symposium On Usable Privacy and Security (2016)

[24] See Goodman B and S Flaxman 'European Union regulations on algorithmic decision-making and a "right to explanation"' arXiv, 31.08.2016, available at https://arxiv.org/pdf/1606.08813v3.pdf (accessed 09.01.2017) p 3-5.

[25] Art 4 (4) GDPR

[26] Art 22 (1) GDPR

[27] Recital 71 GDPR.

of likely personal preferences is interfering with the right to not be subjected to automated decision making and profiling in the GDPR.

The GDPR, however, allows profiling and automated decision making in three cases: firstly, when such automated decision is necessary for the performance or the entering into a contract, secondly, when the decision is based on adequately safeguarded laws, and thirdly, when the decision resulting from automated profiling is based in a data subject's explicit consent.[28] Furthermore, such automated decision cannot be based on the processing of special categories of personal data listed in article 9 GDPR, unless those are processed on explicit consent or substantial public interest. [29] In the context of consent automation for personal data processing for the provision of product or services, this leaves an explicit consent of a data subject as the only option to automate consenting.

Could therefore a profile which contains consent preferences be authorised by an individual through their explicit consent? The requirements for explicit consent and in-build safeguards are rather high. Explicit consent has been defined as '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,'[30] requiring the creation of a detailed and informative consent interface for allowing automated consent profiling. Furthermore, the data subject needs to have the possibility to adjust or withdraw the consent at will, and needs to be provided with meaningful information about the nature, significance and consequences of the profiling in order to ensure fair and transparent processing.[31] Nevertheless, algorithmic sophistication may arrive at a point where individual choices regarding personal data processing activities become entirely predictable. In that case, consent and choice would become a meaningless exercise and merely function as a formal tool for justification of processing, rather than a materialization of informational self-determination. This would require much broader academic and societal discussion on the effects of automation.

This means, however, that a fully automation of consent interfaces, based solely on prediction and without any involvement of the data subject is not in line with the GDPR. As consent is one of the core legal bases of processing, it is therefore at least highly questionable that this process could be fully automated. While recommendations may be implemented in one or the other way, it is always the data subject which needs to be fully informed and enabled constant access as well as the ability to modify given consents. Consent automation based on automated profiling remains therewith more a theoretical exercise than a practical option at the moment, though at the current rate of technological development, such tools may become available in not too distant future.

VI. Discussion

The new European Regulation tightens the requirements for consent significantly. Throughout the GDPR, consent is understood as a genuine, clear and free expression of a person's wishes to have personal information about them processed. As discussed above, an individual should be given at least a theoretical ability to make genuine and free choices. The GDPR therewith attempts to tackle a variety of existing theoretical and practical problems with the concept of individual consent. Firstly, it attempts to address

[28] See Art 22 (2) GDPR
[29] See Art 22 (4) GDPR
[30] See Article 29 Working Party, Opinion 15/2011 on the definition of consent, 01197/11/EN WP187, 13.06.2011, at p 25.
[31] See Recital 60, Arts, 13 (2) f), 14 (2) g) GDPR.

obstacles resulting from not being sufficiently informed by requiring the provision of information to the subjects of personal data: clarity and unambiguity shall empower an individual in decision making as much as possible. Secondly, the GDPR attempts to address problems with individual decision-making and rationality as such. Consent should come without strings, without coercion and should not be used when there are severe power imbalances between the controller and a data subject.

The GDPR also not only regulates the minimum requirements for valid consent as such, but it also sets standards for the communications between data controllers and data subjects when obtaining and retaining consents to personal data processing. Consent user interfaces therefore play a very important role in a variety of personal data processing operations and here, it is the design of such user interfaces that is important for the validity of consent. In some cases, however, as shown in scenario 1 above, particularly very complex consent management may have severe limitations with regards to usability. After all, a flood of choices and the need to tick countless boxes may overstrain users and create new decisional or evolutional obstacles. The amount of required actions then could produce a situation in which the individual is presented with so much information and options that free and informed choice becomes an impossibility.

One solution to this problem may be the simplification of consent through more or less detailed recommendations as discussed in scenario 2. This approach, however, has some limitations, particularly with regards to the importance of independence of the recommendations, and due to influence which may be exercised on data subjects. Recommendations could, if they become popular, also affect the choices the data controller provides in the first place thus changing the balance of power between the data subject and the data controller.

Another solution, as discussed in scenario 3 above, could be the simplification and automation of consenting process. While on first sight highly problematic, there may be technical ways in which consenting could be automated by employing for example a pre-set privacy profile. Recommendation and automation which influence data subjects' decisions require ensuring that they truly represent the genuine will and expression of such data subject. In this light, scenario 4's fully automated consenting system where the data subject does not participate in the consenting process at all is a step too far under GDPR.

However, the emergence of more and more sophisticated automated assistants can soon mean that for the individual, who may experience the large number of consenting decisions more as a chore than an expression of their free will, would rather leave at least some of the consenting decisions to the assistant - a situation the European data protection legislation will have to eventually address.