CONSENT TO PERSONAL DATA PROCESSING – THE PANACEA OR THE DEAD END?

by

JAKUB MÍŠEK[*] [**]

The paper deals with the question of proper use of consent to personal data processing on the Internet. Legal requirements of such consent are discussed in the first part of the paper, when Directive 95/46/EC, Directive 2002/58/EC as well as their Czech implementation, Act No. 101/2000 Coll., on the Protection of Personal Data and Act No. 127/2005 Coll., on the electronic communications are examined. The second part of the paper questions capability of data subjects to make an informed consent and adequacy of this legal institute. The second part also points out a common problem of its wrong use which is a practice of data controllers, who try to legitimise data processing by consent even in situations, when it is not a proper way of doing so. Finally, a possible solution to the presented problem is discussed.

KEYWORDS

Personal Data Protection, Consent to Processing, Consent Fetishism, Informed Consent

1. INTRODUCTION

The European legal regulation of personal data protection is based on the principle of a strong legal protection, which can be breached only by certain legal means. This can be seen in article 7 of the European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (further referred as "Data protection directive"), which is key legal document for the whole European data protection framework. It states that the Member States shall allow the processing of personal data only if certain

[*] Jkb.misek@gmail.com.

[**] I am grateful for inspiration and comments from Josef Prokeš and Matěj Myška.

criteria are met. Consent of the data subject, by which she agrees with personal data processing, is such a criterion and it seems that for many, both legislator and data controllers, the most important one.

Consent to data processing was included in Commission's proposal of the Data protection directive from 1990 as one of the possibilities how to legitimise data processing. It is one of the key parts of the directive as can be seen from the text of the proposal itself: "*The data subject's consent to the processing of data relating to him is an important justification for the processing of personal data by the controller of the file.*"[1] Furthermore, a role of consent as a legal base for data processing is expressly acknowledged in the Charter of Fundamental Rights of the European Union.[2] Article 8, which introduces the Right to the protection of personal data, states in paragraph 2: "*[Personal] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law.*" Although the provision speaks about an existence of some other legitimate basis, consent is the only one explicitly named. Finally, the importance of the consent can be seen from a common daily experience, when everyone is a subject of consenting many times a week. Common tasks like registration to on-line services, approving of cookies, on-line commerce and many others might serve as an example.

Consent in data protection law is a way of expression of an individual's opinion whether and under what conditions the other party can process her personal data.[3] This legal instrument therefore can, and in my opinion should, serve as a tool by which can be achieved what Daniel J. Solove calls a "Privacy self-management".[4] This is a complex approach to personal privacy applicable by everyone, which allows an individual to control her personal data, weigh the price and benefits of data disclosure and decide when and to whom allow data processing.

The purpose of this article is to question whether the current approach of both legislator and data controllers to consent is still up to date with today's

---

1 Proposal for a Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287 and 288, Brussels, 13 September 1990. p. 26.

2 Charter of Fundamental Rights of the European Union, 2000/C 364/01.

3 Of course this applies only in the case when no other legal bases for data processing are applicable.

4 Solove, D. L. 2013, 'Privacy Self-Management and the Consent Dilemmas', Harvard Law Review, vol. 126, no. 7, pp. 1880-1903. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018 [cited 15th Jan. 2014].

massive use of the Internet and other electronic means of data processing, or whether it has flaws which need to be fixed. In the first part I present legal requirements of a valid consent to personal data processing. The second part of the paper questions capability of data subjects to deliver an informed consent and adequacy of this legal institute. The second part also points out a common problem of its wrong use, which is caused by practice of data controllers who try to legitimise data processing by consent even in situations, when it is not a proper time to do so. Finally a possible solution to the presented problem is discussed.

2. THE EUROPEAN LEGAL REGULATION OF THE CONSENT TO PERSONAL DATA PROCESSING

The first step on our journey is a proper analysis of consent to personal data processing in black-letter law. Data protection directive defines the consent in the Article 2 letter h) as "*any freely given specific and informed indication of [data subject's] wishes by which the data subject signifies his agreement to personal data relating to him being processed*". Article 7 states that data processing shall be lawful only if certain requirements are met. First listed in the list of requirements, marked by letter a), is an unambiguous consent given by the data subject. Other basis for legal data processing include for example the necessity of processing for the performance of a contract to which the data subject is party (letter b)); the necessity of processing for compliance with a legal obligation to which the controller is subject (letter c)) and the necessity of processing for the performance of a task carried out in the public interest or in the exercise of official authority (letter e)). Furthermore, in case that the "sensitive personal data", which are enumerated in Article 8 paragraph 1[5], are part of the processing, an explicit consent to the processing is necessary.

Two important findings are arising from the previous paragraph. First, in order to be valid, the consent must be cumulatively: 1) freely given; 2) specific; 3) informed and 4) unambiguous. Second, consent is not the only way how the data controller can achieve legality of its processing. As Working Party 29[6] (further referred as WP29) states, "*the order in which the legal grounds are cited under Article 7 is relevant, but it does not mean that consent is*

[5] E.G. data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sex life.

[6] Working Party 29 is an independent European advisory body on data protection and privacy, which was set up under Article 29 of Data protection directive.

always the most appropriate ground to legitimise the processing of personal data."[7] This will be further discussed in the chapters 3 and 4 of this paper.

Aside from Data protection directive is Directive 2002/58/EC, on privacy and electronic communications also important for data protection in on-line environment. Article 5 (3), which was amended by Directive 2009/136/EC specifies legal requirements for the use of cookies and other similar technologies carried out by electronic communication networks in order to store information or to gain access to information stored in the terminal equipment of a user.[8] In the original version of the provision this was allowed under the condition, that the user was informed by the data controller about the processing in accordance with Data protection directive and was offered to refuse such processing. In other words, it was a nice example of an opt-out principle. Directive 2009/136/EC, along with the introduction of a more restrictive exemption from the rule, changed the opt-out into an opt-in principle with this wording: "*storing of information or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent...*"[9] Since the art. 1(2) of the Electronic communication directive states that provisions of this directive particularise and complement Data protection directive, this has to be interpreted in a way, that the user of cookies and similar technologies has to give consent fulfilling all requirements defined by Data protection directive.

2.1 ANALYSIS OF THE REQUIREMENTS FOR A VALID CONSENT

According to WP29 the consent is freely given, if the data subject has a real choice and "*there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.*"[10] If there is not a real choice and for some reason the data subject has to consent, this consent cannot be seen as a valid one. For instance, if a data subject has a legal duty to grant her data for processing it cannot be done on the bases of consent because there

[7] WP29 Opinion No. 15/2011 on the definition of consent, from 13th July 2011. 01197/11/EN. WP187. P. 7.

[8] In the scope of this provision are for example also mobile applications or software distributed on-line via services like iTunes or Steam.

[9] Directive 2002/58/EC, on privacy and electronic communications, amended by Directive 2009/136/EC. Art. 5(3).

[10] WP29 Opinion No. 15/2011 on the definition of consent, from 13th July 2011. 01197/11/EN. WP187. P. 12.

is not a free will included. One such case is a creation of a bank account. The bank has legal duty to process certain data about the customer. In this case the useable legal ground for processing is therefore compliance with a legal obligation to which the controller is subject. Another example might be a registration to a social network service, e.g. Facebook. This time the consent is a valid ground for data processing, because the data subject has a real choice not to use the service. Even though the service might have a huge market share and the data subject can experience some negative consequences of not being a part of it, it hardly can be described as *significant negative consequences.*

To be "specific" the consent should be intelligible. As WP29 states, "*it should refer clearly and precisely to the scope and the consequences of the data processing.*"[11] The data subject must therefore be well informed about the details of the processing, what is the purpose of the processing, how her personal data will be used, who will have access to it and other important questions. Blanket consent cannot be valid. As we can see, there is a very narrow link between this condition and the purpose limitation principle. For example, a user of a mobile application for reviewing visited restaurants consents to the processing of her personal data in regard of using her geolocation to show nearby restaurants with certain number of positive reviews. If the data controller, in this case a company running the application, would have made the application able to show user's location to her friends, a new consent with the new purpose would be needed.

Third condition of a valid consent is that it has to be informed. According to the WP29 Opinion[12] it means that the consenting data subject must appreciate and understand the facts and implication of her action. There should be quite a high standard for the data controller when it comes to informing the data subject. "*The more complex data processing is, the more can be expected from the data controller. The more difficult it becomes for an average citizen to oversee and understand all the elements of the data processing, the larger the efforts should become for the data controller to demonstrate that consent was obtained based on specific, understandable information.*"[13] This condition is as important as it is problematic. In the Internet era it is very hard for a data subject to comprehend possible outcomes of consenting to the processing. It

[11] Ibid., p. 17.
[12] Ibid., p. 19.
[13] Ibid., p. 21.

is almost impossible to foresee future impacts of current privacy decisions and therefore it is questionable whether the data subject can really be informed. This problem is also discussed more in the third chapter.

The last condition of a valid consent is that it must be unambiguous. The Data protection directive does not prescribe a certain form in which the consent must be made. It can be any action of the data subject, by which she indicates that she consents with the data processing. However, there must be "*no doubt as to the data subject's intention to deliver consent.*"[14] This is a reason, why there might be a problem with the validity of the passive, silent, consent, even though this possibility is not forbidden by Data protection directive. An example of the silent consent can be notice like "By using our site you consent to processing of your personal data." Lack of action might not be sufficient as an expression of the data subject's consent and in the case of a conflict the data controller would have to stop the processing.

The four above analysed conditions are necessary for the consent to be valid. However with the condition of freely given consent comes hand in hand the withdrawal of the consent. As the data subject consents freely, so should she have an opportunity to withdraw the consent any time as easily, as it was given. Even though the option to withdraw the consent is not expressly written in the Data protection directive, it cannot be interpreted in such a way, that the data subject is not allowed to do so, as proposed by Curren and Kaye.[15] At least in continental Europe it is not possible to interpret it this way.[16] As WP29 claims, "*In principle, consent can be considered to be deficient if no effective withdrawal is permitted.*"[17] A withdrawal of the consent can be done also through a termination of a user account, uninstallation of a game or other way of ending the usage of a service. The consent to personal data processing is a part of broader informational self-determination principle and as such everyone should have a free will to decide what others can do with her personal information.[18]

---

[14] Ibid., p. 21.

[15] Curren, L. & Kaye J. 2010, ' Revoking consent: A 'blind spot' in data protection law?', Computer law & Security review, vol. 26, no. 3, pp. 273-283.

[16] Curren and Kaye restrict application of their claims for the British law area.

[17] WP29 Opinion No. 15/2011 on the definition of consent, from 13th July 2011. 01197/11/EN. WP187. P. 13.

[18] See Ibid., p. 32.

2.2 SITUATION IN THE CZECH REPUBLIC

Since the data protection law in the Czech Republic is harmonised with the law of European Union, the legal situation is quite similar. The constitutional base for data protection is anchored in the articles 7 and 10 of the Charter of fundamental rights and freedoms.[19] General privacy protection is a part of the Civil code[20] in sections 84 – 90. Consent is used here as a primary way of legalising the interference into the protected right for privacy. Withdrawal of the consent is guaranteed and is permit even in the case when the consent is given for limited time.[21] Data Protection Act[22], a key statute of personal data protection, regulates the matter of consent very similarly to the Data protection directive. Finally, opinions of the Czech Office for personal protection are also consistent with the opinion of WP29.

The comparison of Czech and European legal framework is much more interesting in the case of cookies and similar technologies. This matter is governed by the Electronic communications act,[23] which, as it is stated in its section 87(2), is in the field of data protection lex specialis to the Personal data protection act and should therefore be interpreted accordingly. Art. 5(3) of the Directive 2002/58/EC is transposed in the section 89(3) of the Electronic communications act. Interestingly, although other parts of Directive 2009/136/EC amendment found their way into Czech legal order, the part which regulates conditions for use of cookies and similar technologies remained unchanged, matching the original wording of Art. 5(3). Current legal framework of cookies and similar technologies is therefore still set to the opt-out principle. To make things even more confusing, the legislator stated in the explanatory report of the amendment, that from now on cookies and similar technologies are governed by the opt-in principle. However, this statement has no backing in the positive law. As o result of this situation web masters and other data controllers are confused about how they should set their services. A possible way out of this problem might be consenting via the Internet browser setting. This option, which is expressly recognised in the recital 66 of Directive 2009/136/EC, however encounters two prob-

[19] Resolution No. 2/1993 Coll., on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic.

[20] Act No. 89/2012 Coll., Civil Code.

[21] Ibid., section 87.

[22] Act No. 101/2000 Coll., on the Protection of Personal Data.

[23] Act No. 127/2005 Coll., on the electronic communications.

lems. As WP29 states in the Opinion on Online Behavioural Advertising,[24] first problem is that since the browser setting is done before data subject receives the information about processing, it would be very difficult to meet the condition of specific consent. Second problem is that in order for the browser setting consent to be valid, the user would have to alter the factory setting of the browser at least once and thus express his intention to consent.

3. CONSENT IN REAL LIFE

As we can see, the definition of consent provides quite a strong impression, that consent to personal data processing is a solid, well-oiled machine, which works almost without any flaws and provides a data subject with a possibility to effectively manage her privacy. The truth is that there is one major problem. That problem lies in human nature and capability to comprehend. In his article[25] Daniel J. Solove recognises several partial problems which he divided into two categories – Cognitive problems, connected with the data subject, and Structural problems, connected more with the use of consent itself.

3.1 COGNITIVE PROBLEMS

Solove[26] compares the situation of a data subject to position of the protagonist from Franz Kafka's novel "Before the law". The problem with informing data subject is that people do not read privacy policies. If they read them, they do not understand them and even if they read them and understand them, they often lack background knowledge to realise what policies mean and what are implications of consent. Therefore people cannot make an informed choice. Finally, in case that people read policies, understand them and realise their implications, the decision might be deflected by various psychological factors.

The first three obstacles make together what Solove calls "*The problem of the Uniformed Individual*"[27]. Even though data controllers spend recourses on the creation of privacy notices, privacy policies and other documents offer-

[24] WP29 Opinion No. 2/2010 on online behavioural advertising, from 22nd June 2010. 00909/10/EN. WP 171. p. 14.

[25] Solove, D. L. 2013, 'Privacy Self-Management and the Consent Dilemmas', Harvard Law Review, vol. 126, no. 7, pp. 1880-1903. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018 [cited 15th Jan. 2014].

[26] Ibid., p. 1888.

[27] Ibid., p. 1883.

ing the data subject information about the processing, practically no one really reads them. There might be several reasons for this, e.g. the data protection policies are long, often complicated and there is way too many of them hence the data subject needs a lot of time to read them. According to Frederik Zuiderveen Borgesius[28], an average American would spend 244 hours a year reading privacy policies of the webpages she visits and therefore time invested in the reading of privacy policies can be seen as transaction cost. It is a cost which data subject pays by her time and since, as will be discussed later, she does not really see an equivalent value in the reading it, she often decide not to do so. Assumption that people regularly read privacy policies is incorrect.

In order to be sufficiently informative, the privacy policies are not only long; they are often too complicated and difficult to read as well. Borgesius claims[29] that a research showed that more than a half of privacy policies involved in the survey were too difficult for a majority of American internet users and that more than 25% of Europeans also find privacy policies also too onerous.

Finally, people often lack the necessary knowledge to make a proper informed decision. As Chris Hoofnagle et al. found out in their research, 75% of 974 participants of the survey answered correctly 2 or less out of 5 basic questions concerning online privacy knowledge.[30] Even if people understood privacy policies, without a proper knowledge, without capability to see the big picture what implications might the processing have, it is impossible to decide correctly whether to allow it or not.

The fourth obstacle Solove calls "The Problem of Skewed Decisionmaking"[31], which is connected with factors that Borgesius calls from the behavioural economics point of view "biases"[32]. First of them is Myopia, a bias which means that people favour immediate benefit over possible future inconvenience. Surprisingly this is in a contradiction to, what people say

---

[28] Borgesius, F. Z. 2013, 'Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?', (June 7, 2013). Available at http://www.ivir.nl/staff/borgesius.html [cited 13th Jan. 2014]. P. 32.

[29] Ibid.

[30] Hoofnagle, Ch. J. et al. How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies? (April 14, 2010). Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 [cited 13th Jan. 2014]. P. 19.

[31] Solove, op. cit., p. 1886.

[32] Borgesius, op. cit., p. 38.

about how much they value their privacy. Even though people claim that they would not change privacy for a small benefit, the bias is stronger. This is also connected with overconfidence and optimism about the future as well as with the underestimation of future risk. Solove[33] points out an interesting observation that people consider familiar dangers riskier than those with which they do not have as much experience. Since for many the privacy harm is very hard to imagine, people tend to underestimate it and therefore are more willing to give away their data.

The four above mentioned problems are sufficient to question, whether a person is capable of giving an informed consent. If we insisted on the interpretation of WP29 presented in the second chapter, that informed consent means that "*consenting subject must appreciate and understand the facts and implication of her action*", suddenly the question could be, whether the consent can ever be valid. Clearly there are huge differences between paper and breathing version of a data subject.

3.2 STRUCTURAL PROBLEMS

According to Solove[34], when a hypothetical super-data subject successfully passes all four cognitive problems, there still are three more structural ones. First of them is "The Problem of Scale", which is connected with the first cognitive problem, and says that there are just way too many data controllers, by which the data subject should exercise her rights. It is impossible for a human being to micro manage dozens of different accounts and web pages.

The second structural problem is "The problem of Aggregation" [35]. The nature of personal data is that its effects aggregate. The more data is at one place, the more it can say about the data subject. It is impossible to remember, track or imagine all possible connections of data and information given away on different occasions. Then one day, suddenly data can click into each other and reveal facts that the data subject did not want to reveal. And since the Internet does not forget, the time between data disclosures can be a long one. This represents a trouble for the data controller as well, because it might happen, that two or more "normal personal data" create together a "sensitive personal data", which the controller is not entitled to process.

---

[33] Solove, op. cit., p. 1887.
[34] Ibid., p. 1888.
[35] Ibid., p. 1889.

The third and last Solove's structural problem is "The Problem of Assessing Harm". It means that people generally underestimate consequences which the data disclosure might have in the future. Since it is closely connected with the last cognitive problem I will not elaborate on it here any further.

It is true, that these three aspects constitute a problem for data subject to properly execute privacy self-management. However their effect multiplies when consent to processing is regularly used by data controller in a wrong manner. And that brings us to the next section.

3.3 CONSENT FETISHISM

Problems mentioned in previous two sections have one common denominator. It is a wrong way of how the legal institute of consent is used. Nowadays from actions of both legislator and data controllers it almost seems as if everyone was fascinated by consent, every processing had to be legitimised via consent and there was a shared believe in a supernatural power of consent, which could be used as an universal cure for both data subject and data controller. As was proven in previous sections, this is not true. I think that an appropriate description of this behaviour is "consent fetishism".

Demonstration of this wrong approach is when a controller asks for data subject's consent even though it has other lawful possibilities of legitimising the processing[36]. What many seem to forget is that consent is just a one of grounds for lawfulness of data processing. As WP29 states in the opinion on consent, it is crucial to use consent in the right context.[37] If the consent is used in an ill measure, it cannot serve its purpose, which is to let the data subject decide how she deals with her personal data. It is confusing for the data subject when controller asks for consent although there are other possible grounds for legitimisation of the processing, e.g. performance of a contract or compliance with a legal obligation, available. When asked for consent subject has an impression, that she can freely control her data. How-

[36] The situation of a scientific conference might serve as an example. The participants of the conference had to consent with data processing for the sake of a report for a National Fund, because the conference was supported by the Fund. In this case the data controller (organiser of the conference) had a legal obligation to disclose list of participants in order to obtain the support and therefore the correct legal ground for processing was not necessarily consent, but compliance with a legal obligation to which the controller was subject.

[37] WP29 Opinion No. 15/2011 on the definition of consent, from 13th July 2011. 01197/11/EN. WP187. P. 10.

ever, that is not true, since should the data subject withdraw the consent, the processing would still continue, just with a different legal ground. Furthermore, massive usage of consent overloads the data subject with unavoidable consent related decisions and readings, which is a major cause of problems described in previous sections of this paper.

As can be observed from the legal regulation of cookies and similar technologies, and its shift from opt-out to opt-in principle, new legislation also puts more and more weight on consent. It might seem that the new opt-in version offers better protection for the users, but in the end it devaluates the institute of consent. And as seen from the WP29 documentation concerning cookies[38] and from the proposal of Data protection regulation[39], the future development does not seem to take a more consent-sensitive turn.

4. A LIGHT AT THE END OF THE TUNNEL

There is a way out of this situation, or at least out of consent fetishism, which might provide a good ground for future development of a better privacy self-management. The data controllers should realise that there are other legal grounds for processing and use consent only in the case that other possibilities are not applicable. For a vast majority of daily life situations the consent is not necessary, since the processing is either for the performance of a contract to which the data subject is party, or for compliance with a legal obligation. For example, when a data subject wants to use a map and navigation service in a mobile phone, the controller does not need to ask for consent to process geo localisation data, since these are needed to carry out the requested service.

The granularity of services and consent is very helpful.[40] Granularity means a possibility for the data subject to decide which parts of the service she wants to use, and what personal data she wants to disclose. This principle can work even when different legal bases for processing are involved. If we use the example from the previous paragraph, navigation is a basic function of a mapping service, which is requested by the user and therefore the consent is not applicable. However, the new version of the application

[38] See WP29 Working Document 02/2013 providing guidance on obtaining consent for cookies. 1676/13/EN. WP 208.

[39] The Proposal of the Regulation states that the consent must be "explicit". See Art. 4(8) of the Proposal for a General Data Protection Regulation, from January 25, 2012. COM(2012) 11 final. 2012/0011 (COD).

[40] See WP29 Opinion No. 15/2011 on the definition of consent, from 13th July 2011. 01197/11/EN. WP187. P. 17.

offers some value added service, like schedule and reviews of local theatres based on user's preferences, or tracking of movement of the user and posting it on-line. Processing for purposes of these functions would have to be based on consent. The user can decide which functions she wants to use and disclose her data according to her wishes.

It is important to remind, that even in the case of processing based on other legal grounds than consent, the controller still has a duty to inform the subject about the processing, so the subject is aware of its existence, purposes and other important information.[41] Now, it may seem as if nothing would change compared to the current state, since there would be the same amount of documents to read. That might be true, but if consent was used properly and therefore it was more uncommon, the difference between consenting and acknowledging might become evident. If consent was scarcer, users might be more sensitive when the controller asks for it, and they would be more likely to read privacy policy to find out, why is it necessary to consent in this particular case.

5. CONCLUSION

Answer to the question from the title of this paper is "Consent is none of those two things", which can hardly be considered as a surprise. Consent to personal data processing is a just a legal instrument and its quality depends on the manner how it is used. In my opinion, the way how is it used nowadays is far from perfect. But there is a number of ways how to make it work better. For instance a more thorough education of data subjects in the field of personal data protection would be very helpful. Then they could better understand privacy policies of data controllers.[42] Another option is to change the way how data policies are written, so they would be more understandable. As we know from Creative Commons a system of graphical symbols[43] might help. However the cost here is a loss of complexity of information, which is needed to properly inform the data subject. Furthermore as claim Myška et al.,[44] simplification of legal language, which an introduction of graphical symbols undoubtedly is, can lead to an increase of

[41] Art. 10 of Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data.

[42] See Solove, op. cit., p. 1886.

[43] See Borgesius, op. cit., p. 49.

[44] Myška M. et at. 2012, 'Creative Commons and Grand Challenge to Make Legal Language Simple', AICOL Workshops 2011, Berlin, Heidelberg, p. 276. Available at http://link.springer.com/chapter/10.1007/978-3-642-35731-2_19 [cited 15th Jan. 2014].

legal uncertainty. An interesting option comes from authors who argue that an automated consent through privacy agents[45] can solve the privacy self-management problems.

These solutions were out of scope of this paper. My goal was to show the current situation and try to offer at least a partial solution that would be directly applicable without any legislative needs.

REFERENCES

Borgesius, F. Z. 2013, 'Consent to behavioural targeting in European Law: What are the policy implications of insights from behavioural economics?', (June 7, 2013). Available at http://www.ivir.nl/staff/borgesius.html [cited 13th Jan. 2014].

Curren, L. & Kaye J. 2010, 'Revoking consent: A 'blind spot' in data protection law?', *Computer law & Security review*, vol. 26, no. 3, pp. 273-283.

Hoofnagle, Ch. J. Et al. 'How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes & Policies?', (April 14, 2010). Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1589864 [cited 13th Jan. 2014].

Métayer, D. Le. & Monteleone S. 'Automated consent through privacy agents: Legal requirements and technical architecture', *Computer law & Security review*, vol. 25, no. 2, pp. 136-144.

Myška M. et at. 2012, 'Creative Commons and Grand Challenge to Make Legal Language Simple', *AICOL Workshops 2011*, Berlin, Heidelberg, pp. 271 – 285. Available at http://link.springer.com/chapter/10.1007/978-3-642-35731-2_19 [cited 15th Jan. 2014].

Solove, D. L. 2013, 'Privacy Self-Management and the Consent Dilemmas', *Harvard Law Review*, vol. 126, no. 7, pp. 1880-1903. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2171018 [cited 15th Jan. 2014]

WP29 Opinion No. 2/2010 on online behavioural advertising, from 22nd June 2010. 00909/10/EN. WP 171.

WP29 Opinion No. 15/2011 on the definition of consent, from 13th July 2011. 01197/11/EN. WP187.

[45] See Métayer, D. Le. & Monteleone S. 'Automated consent through privacy agents: Legal requirements and technical architecture', Computer law & Security review, vol. 25, no. 2, pp. 136-144.

WP29 Working Document 02/2013 providing guidance on obtaining consent for cookies. 1676/13/EN. WP 208.

Directive 95/46/EC, on the protection of individuals with regard to the processing of personal data.

Directive 2002/58/EC, on privacy and electronic communications.

Directive 2009/136/EC, amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

Proposal for a Directive concerning the protection of individuals in relation to the processing of personal data, COM (90), 314 final, SYN 287 and 288, Brussels, 13 September 1990.

Proposal for a General Data Protection Regulation, from January 25, 2012. COM(2012) 11 final. 2012/0011 (COD).

Charter of Fundamental Rights of the European Union, 2000/C 364/01.

Resolution No. 2/1993 Coll., on the declaration of the Charter of Fundamental Rights and Freedoms as a part of the constitutional order of the Czech Republic.

Act No. 101/2000 Coll., on the Protection of Personal Data.

Act No. 127/2005 Coll., on the electronic communications.

Act No. 89/2012 Coll., Civil Code.