School of Economics,
Business Administration and Legal Studies

A thesis submitted for the degree of LLM in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law

"The notion of consent in GDPR"

Maria Apostolina

February 2018

Thessaloniki-Greece

Student Name: Maria Apostolina

SID: 1104160047

Supervisor Professor: Dr Athanasios Kaissis

I hereby declare that the work submitted is mine and that where I have made use of another's work, I have attributed the source(s) according to the Regulations set in the Student's Handbook.

Table of Contents

Preamble

This dissertation was written as part of the LLM in Transnational and European Commercial Law, Mediation, Arbitration and Energy Law. The dissertation deals particularly, with the concept of data subject consent in the General Data Protection Regulation by tracking the changes between the previous legal regime and the Regulation. In other words, starting with the significance of subject's consent in the frame of data protection as a legitimate ground for data processing, although the GDPR is based on the previous legal framework, it intends to tighten and strengthen the role of consent by establishing more transparency and simple information policies and therefore, in this way, it gives the control to the data subject. More specifically, it adds criteria and conditions in order to ensure the provision of consent with regard to the freedom of choice and the total awareness of the subject when he gives his consent, it puts particular emphasis on strengthening child protection and it also extends the right to information to a more general principle of transparency. Therefore, it is appropriate to refer to what has been done so far and, finally, whether the Regulation intervenes on these points by making some changes as an evolutionary law.

Acknowledgements

This dissertation could not have been finished without the help and support of my supervisor professor, the academic staff, the academic library of International Hellenic University, and my family. It is my great pleasure to acknowledge people who have given me guidance, help and support and who have faith in me.

First of all , I would like to express my sincere appreciation and deepest gratitude to my supervisor professor and Scientific Director Professor Dr Athanasios Kaissis for providing me with the opportunity to attend the LLM in Transnational and European Commercial Law and Alternative Dispute Resolution Program , which enabled me to acquire valuable knowledge on international commercial law , economics and ADR . I would like to thank him for his extremely valuable guidance and support in order to complete this dissertation.

Similarly, I would like to thank Dr Komnios Komninos for his also extremely valuable guidance and suggestions, which were very helpful and precious to me in order to finish this dissertation.

Special thanks should be given to the academic library of International Hellenic University, which provided me with variety of resources, the library staff, the academic staff and assistants in general, who were always willing to help me and guide me through my research.

Also, I would like to thank particularly , a very beloved person , who is important to my life , who I consider to be my family , who urges me to reach my goals , who tells me to “fly as high as I can” , and who encouraged and inspired me to undertake and complete this particular dissertation .

Finally , I would like to thank my parents , my brother and my daughter , who have faith in me and always support and encourage me to overcome myself .

Maria Apostolina

February 2018

I. Introduction

Privacy is globally recognized as a personal, individual right. The philosophy of privacy in Europe is elevated as a fundamental right. The evolution of new computer technologies focused on the right to information privacy which concerns the protection of personal information infringement by others and this right is defined by Europeans in terms of "personal data". Personal data can be any kind of information provided and related to a person[1]. Consequently, a proactive approach to protecting personal privacy has been taken by the European Union and its Member States[2]. The European legislator, recognizes several reasons in order to protect the processing and the free movement of personal data on legitimate grounds particularly, one of which is the consent of the data subject. In 2010, in Europe, the concept of data subject consent was in the center of a debate within the framework of the review of the data protection. Therefore , in January 2012 , after three intense years, the European Commission in order to reform the data protection framework of the European Union, proposed the replacement of the Data Protection Directive with a Regulation , because it is considered that more legal certainty and coherence will be provided by a Regulation compared to a Directive[3].Consequently , in 25 May 2018 the General Data Protection Regulation (GDPR) 679/2016/EE is put into implementation[4] and particularly, by clarifying the conditions of the notion of the consent the data subject obtains more significant and activated role inter alia through the strengthening of the right of consent and by converting this right to a fundamental source of legitimization of the processing[5]. This particular research addresses the notion of data subject consent in the GDPR by tracking the changes between the previous legal regime and

[1] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, p 41

[2] Lasprogata G., King N., Pillay S., "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", Stanford Technology Law Review 4 (2004), pp7-11

[3] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 1-3

[4] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), pp 10,17

[5] Mitrou L.,"The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 71

the Regulation. More specifically, it will be mentioned the provisions of GDPR on the concept of i)"freely given", ii) specific, iii) informed, iv) unambiguous and v) explicit consent in conjunction with relative parameters, furthermore, the legal capacity of data subject in order to consent, the unlawfulness of the processing despite the existence of consent involving some exceptions to the rule of consent's necessity, moreover, the right of data subject to withdraw his or her consent and finally, the right to erasure or "to be forgotten" and the burden of proof for the acquisition of consent.

II. Consent as a legitimate ground for data processing in GDPR

With regard to the notion of the consent the General Data Protection Regulation is based on the previous legal framework, for example, on the provisions of the Data Protection Directive 95/46/EC and the e-Privacy Directive. However, the GDPR can be considered as evolutionary law by tightening and strengthening the role of consent[6]. It also set out the conditions for consent to be valid as a legitimate ground for data processing, while consent is still a ground for the processing of sensitive data, as well as for the transfers of personal data to a third country or an international organization that do not ensure an adequate level of protection. Moreover, the consent of children is strengthened in GDPR. It is also important to mention that the consent of the data subject is presented in various instances in the GDPR, concerning the right to be forgotten, automated profiling etc[7]. In particular , according to the article 4 (11) of GDPR " consent of the data subject means any freely given , specific , informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action , signifies agreement to the processing of personal data relating to him or her "[8]. The GDPR treats consent as the primary source of legitimating of processing by strengthening the right of self-determination, albeit,

[6] Reijneveld M. D., "Quantified Self , Freedom, and the GDPR", SCRIPTed: A Journal Of Law, Technology and Society, Vol.14 , Issue 2 (December 2017), p 299

[7] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 3

[8] Article 4 (11) GDPR. See also Reijneveld M. D., "Quantified Self , Freedom, and the GDPR", SCRIPTed: A Journal Of Law, Technology and Society, Vol.14 , Issue 2 (December 2017), p 299

without this implying a withdrawal from the right to protection of personal data[9]. In any case, all requirements should be fulfilled in order for the consent to be valid[10].

1. "Freely Given" Consent

In GDPR the consent should be "freely-given" expressing an act of informational self-determination**.** It should be an autonomous act of the data subject and a product of free decision, in other words, free from external manipulations. However , there are some cases in which consent actually , cannot be given freely, more particularly , when there is a clear unbalance between the data subject and the data controller , for example when personal data must be provided to public authorities or in the employment relations[11].

a. Involuntary actions and voluntary actions made under pressure

Taking into account that the consent of the data subject should be a genuine expression of the right to informational self- determination, it is presented as a "liberty right" with a voluntary mood. In this point, there should be made a reference to what has been done so far in accordance with the previous regime in order to make it understandable. According to the "Beyleveld and Brownsword" theory there is a distinction between involuntary action in the strict sense, because in this case the will is overborne and those cases where the action is voluntary but made under pressure. It is important to say that when the consent is given under pressure there is an indication of the data subject wishes, however, there is no valid consent, as the indication of the wishes is not freely given, because there is an external force and this is usually

[9] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 71

[10] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, p 56

[11] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 169-170

exercised by the data controller. In relation to the consent that is given involuntarily, the agent failed altogether to form a will rather than acted against its will .There is a difference between negative and positive force, because, negative is an act of force that intends to the negative impact on the interest of the individual, a threat for example, while positive is an act of force that intends to influence the individual positively, a persuasion for example[12]. Furthermore, generally, consent given under duress is not valid. In the field of data protection, the exercise of positive pressure does not invalidate the consent of the data subject as not given freely, to the extent that the data subject has been provided with all the necessary information relating to his personal data processing and has been given a real choice to decide. The General Data Protection Regulation has confirmed this position stating that the individual has to be provided with a genuine and free choice and should be able to refuse or withdraw his consent without any damage. Consequently, in any case, coercive acts always limit the ability of the data subject to provide his valid consent[13].

b. "Freely given" consent and Electronic Health Records (HER)

According to the sense of "freely given consent" the data subject should have acceptable alternatives in order to make a free choice. At this point, it is important to mention that in the context of the processing of personal data concerning health in electronic health records (EHR) a free consent is considered as a voluntary decision in possession of all of his faculties, without any social, financial, psychological coercion. In other words, the consent of the patient under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as freely given. Consequently, with regard to the processing of personal data concerning health in electronic health records (EHR) an informed data subject should have the opportunity to make a genuine choice within the framework of his autonomy in order to give a

[12] Ibid, pp 171-173

[13] Ibid, p 173. See also European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law" , Publications Office of the European Union, 2014, p 60

valid consent[14].

c. Legal and factual dependencies-Uneven balance of powers

The consent cannot be considered as freely given, when the choices of the data subject can be limited by legal or factual dependencies .When the balance of powers between the data subject and the data controller is uneven, then the freedom of decision of the data subject is jeopardized .In such situations, the Member States have to provide for additional safeguards in order to protect the data subject in their national legislation. The GDPR foresees that when there is a clear imbalance between the data subject and the data controller, then the processing of personal data of the data subject should not rely on his consent. Furthermore, an imbalance may exist, when the data controller is a public authority and it can impose an obligation by virtue of its relevant powers[15]. In this case, taking into account the interest of the data subject, the consent of the data subject should not be considered as freely given. With regard to the requirement for freely given consent in the context of employment relations various Member States have enacted specific legislation or issued soft law instruments. In general, there are questions about whether the consent given is valid, when there is imbalance of powers, suggesting that a valid consent cannot be given in the employment context. Exceptionally, a legitimate ground for the processing of personal data in the employment context is the consent of the employee, when employees are requested to upload their pictures on the company intranet. In this case, the actual uploading of the picture should be considered as valid consent, when the employees are offered the choice not to upload their picture if they do not want to. Furthermore, it is important to say that in the context of transfers of employee data to third countries that do not ensure an adequate level of protection, the employee must have a real opportunity to withhold his consent without suffering any damage, or to withdraw it subsequently if he changes his mind. It is very interesting to be taken into account the position of the Greek Data Protection Authority (DPA) that with regard to the carrying out of genetic tests in the employment context it should only be allowed to be based on a specific and explicit legal provision and cannot be based on

[14] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 176-177

[15] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, p 58

the consent of the candidate or the employee . Additionally, for the collection and processing of personal data of candidates during recruitment, the Greek DPA took the position that the character and personality evaluation tests should be allowed only exceptionally and only when it is absolutely necessary and adequate for the achievement of a concrete purpose concerning directly the particular position and the relevant choice. Taking into account the nature of these data, their collection should be allowed only after the written consent of the candidate, after he has been adequately informed as regards the methods, criteria, purposes and potential recipients of the analyses and their results. Consequently, the Greek DPA, the Article 29 Working Party and the GDPR took the similar position that the consent of the data subject in the employment context is in most cases not freely given[16]. According to recital 43 of GDPR, in case of inequality concerning the processing of personal data in the context of working relationships, consent is rejected as a legal basis. The Authority of Personal Data Protection with Directive 115/2001 has taken the same approach. Furthermore, the Regulation recognizes the possibility for Member States to lay down national rules on the conditions under which personal data in the context of employment can be processed on the basis of the employee's consent[17]. However, in any case, the processing can be valid, if the data subject consent has not been abolished in a way that is contrary to law or morality[18].

d. Case law defining the context of "freely given" consent

At this point, in order for the context of "freely given" consent to be understandable, it is appropriate to quote case-law .On the one hand, according to the joined cases Volker and Markus ScheckeGbR/HartmutEifert v. Land Hessen the opinion of the Advocate General Sharpston on the validity of the offered consent is very interesting. In accordance with the facts of the case Volker and Markus ScheckeGbR and HartmutEifert , the applicants , after

[16] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 180-183

[17] Article 88 in conjunction with recital 155 of GDPR. See also Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 75

[18] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 88

applying to the competent local authorities , received agricultural subsidies from the European Agricultural Guarantee Fund (EAGF) and the European Agricultural Fund for Rural Development (EAFRD) . The competent authority, the Federal Agency for Agriculture and Nutrition, published on its website the data of the beneficiaries of the subsidies, more particularly, their names, their place of residence or establishment, their postal codes and the annual amounts awarded. Moreover, this website includes a search tool in order to enable users simply by entering for example the postal code to obtain the list of named beneficiaries of grants from the EAGF or EAFRD. However, the applicants wanted to prevent the publication of the relating to them data. Taking into account that the applicants were informed in the application form that the authorities are obliged to publish their personal data and thus the submission of the application form constitutes their consent to this purpose, someone could argue that they could have chosen to avoid publication by forgoing the aid. The Advocate General expressed his pointed opinion stating that due to a significant economic duress the applicants have no real alternative choice, therefore, by not consenting to such publishing, they would not get the financial aid, which is essential for their income. In this case, the consent is invalid, because is not freely given and non-voluntarily. In conclusion, the freedom in consenting is not invalidated only by the exercise of physical or emotional negative force, but also by a significant economic duress which is exercised on the data subject[19].

On the other hand, in accordance with the facts of the Payback case, a company, the defendant, offered consumers a loyalty card, the "Payback" card. A German association of consumer organization, the plaintiff, wanted the annulment of three clauses included in the paper form, via which consumers could join the loyalty program. According to one of the clauses , the customer with his signature agrees that the data he provides , for example services , price, amount of discount place and date of transaction etc , will be exclusively stored in order to be used for market research purposes .In this particular case, the German Federal Court of Justice in its reasoning stated that the consumer who was called to decide if he enrolls to the loyalty program and if he would fill in the application form with his personal data was not under any legal , financial or factual pressure or coercion and for

[19] C-92/09 and C-93/09 (Joined Cases) Volker and Markus Schecke GbR/Hartmut Eifert v. Land Hessen [2010], paras . 72-88

that reason his consent is considered as "freely given"[20].

2. Specific consent

The requirement for specific consent is closely related to the requirement for informed consent, because the consent should be specified on the basis of the information that is provided to the data subject. In other words, in the previous legislation , the consent should be very specific in order to safeguard the right to informational self-determination. **T**he requirement for specific consent is interpreted as a consent that concerns a specific processing of personal data, for a specific person by a specific data controller for a specific purpose and when the data is transmitted to a third party, it should be clearly specified who the recipients are . The consent of the data subject can also concern specific circumstances that may arise in the future[21]. It is noteworthy to mention that the CoJ recognized that there is no need for the data subject to renew his consent in case the data subject has been informed in the past about the processing of his personal data for a specific data processing operation[22]. Furthermore, if the statement of consent for the processing of personal data is blanket, the data subject cannot realize the importance and the consequences resulting from his consent to the processing, and thus, in this case, the consent does not fulfill the requirement of specificity[23]. One of the cases in which specific consent is significant according to the examination of the Article 29 Working Party, is in the context of transfers of personal data to third countries that do not ensure an adequate level of protection. In this case, the data subject should give his consent for the particular transfer or for a particular category of transfers. Consequently, the data subject cannot give his consent for future transfers that are not planned or known at the time when the consent is given. A typical example is that the customers of a company cannot give their earlier consent to the transfer of their data to a third country in the event when the company is taken over by a third one in the future. Nevertheless, the data subject can validly give his

[20] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 195-196

[21] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, pp 59-60. See also Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 219-220

[22] C-543/09 Deutsche Telekom AG v Bundesrepublik Deutschland [2011], para.67

[23] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 221

consent to future transfers of his data to a third county, in case the details of the transfer are already specified, notably in terms of purpose and categories of recipients. Another element that is important to mention about the specificity requirement is that the controller must provide the data subject information on the purpose of the processing for which the data are meant for , based on the fairness and the finality principles that safeguarded in the existing data protection legislation[24].

a. Specific consent and Electronic Health Records (EHP)

In the context of the processing of personal data concerning health the specificity requirement of the data subject' s consent concerns a well-defined, concrete situation in which the processing of medical data is intended . Thus , if the data subject generally agrees to the collection of his medical data for an EHR and to subsequent transfers of these medical data of the past and of the future to health professionals that are involved in treatment , then his consent would not be considered as specific and therefore , it is invalid[25].

b. Case law defining the context of "specific" consent

It is interesting to mention the opinion of Advocate General Sharpston on the joined cases Volker und Markus ScheckeGbR/HartmutEifert v. Land Hessen concerning the context of the specific consent .The facts of these cases are mentioned above .The Advocated General stated that the statement on the application form that was signed by the applicants and which referred to Article 44a of Council Regulation 1290/2005 , actually , did not explicitly mention the types of information that were going to be published and the fact that the data would be published on the website of the Federal Agency for Agriculture and Nutrition. Therefore, the application form does not make it unambiguously clear that an applicant is consenting to publication of his personal data and the amounts awarded to him from the EAGF and/or the EAFRD. Only Article 1(1) of Regulation No 259/2008 sets out

[24] Ibid, pp 221-222

[25] Ibid, p 222

the full detail of what publication will entail. However, Regulation No 259/2008 is not mentioned in the notice on the form and the fact that it is existed cannot be concluded from reading the text of either of the two regulations that the application form does concern[26]. Therefore, the Advocate General concluded that the fact that there is no specific information in the statement on the application form did not render specific the notion of the applicants' consent according to the definition of the data subject's consent in Article 2(h) of the Data Protection Directive. Consequently, the Advocate General focused on the information that should have been provided to the data subject, leaving the question concerning the actual meaning of the requirement for specificity without any particular answer[27]. For that reason, it is important to say that the specificity of consent has been always closely linked to the actual information that the data subject obtains. However, at this point it is important to mention that in the field of bioethics full or complete specificity of consent is unobtainable and unnecessary in order to be the consent valid. Actually, someone could reach the conclusion that with regard to the element of specificity of consent in data protection until now there is lack of uniform interpretation of what "specific" should mean in this context[28]. For example, the German Data Protection Act does not make any reference to the need for the consent to be "specific", however, it particularizes the informational requirements for a valid consent. The element that the consent has to be specific has not attracted much attention, possibly due to the difficulties it raises. Therefore, sometimes the informational requirement overlaps the element of specificity[29]. The GDPR in its article 4 (11) foresees particularly, that the subject's consent to the processing of his data should be, inter alia, specific and in full knowledge. More specifically, in its recital 43 the Regulation adopts the principle of prohibiting the provision of total consent, as separate consent is required for distinct processing operations[30]. In other words, in accordance with the article 6 in conjunction with recital 32 of GDPR , consent may relate to processing for one or more purposes. However , it must

[26] Ibid, p 223

[27] C-92/09 and C-93/09 (Joined Cases) Volker and Markus Schecke GbR/Hartmut Eifert v. Land Hessen [2010], para. 79

[28] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 224

[29] Ibid, pp 224-225

[30] Recital 43 GDPR. See also Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 43

be specific[31]. Exceptionally, the GDPR in order to ensure flexibility which corresponds to reality[32], introduces the concept of "broad" or "blanket" or "generic" consent, according to which it is possible to be granted an overall consent in the frame of certain areas of scientific research , to the extent permitted by the intended purpose . The aim is to facilitate scientific research in order for the researcher to get rid of the burden of multiple consents when changing purpose in his research[33].

.

3. Informational requirements for valid consent

Taking into account that in the frame of data protection, the consent of data subject has to be based on his free decision in order for the data subject to understand what he is consenting to, it is significant to support that the data subject should be properly informed about the processing of his personal data before giving his consent, in other words, the data subject should be aware of the circumstances[34]. In article 10 of the Data Protection Directive it was specified that the data controller should at least inform adequately the data subject about data controller's identity and the purpose of the processing, about the recipients of the data, the obligation to response to questions and the consequences in case of a probable failure to reply, the existence of the right to rectify and the right to access. The information obligation intends to make data processing more transparent to the data subject[35]. However, there are many cases that the complexity of data collection in practice, relationships between vendors and technological applications exceed the individual's ability or willingness to decide to control the use and sharing of information through an active choice[36].

The Data Protection Directive has foreseen also the option that data controllers are

[31] Recital 32 GDPR. See also Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 79

[32] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 76

[33] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), pp 43-44

[34] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, p 59

[35] Ibid, p 74

[36] Kosta E., "Consent in European Data Protection Law" , Volume 3 , Leiden-Boston 2013, pp 202-203

obliged to give to the data subject additional information, if it is necessary, for example additional information concerning some categories of recipients of the data, whether responses to the questions are obligatory or voluntary, probable consequences in case of failure to reply, or information relating to the existence of the right of access to and the right to rectify the data regarding him**.** Additional information may be required in specific situations in order to guarantee the fairness and lawfulness of the processing of the data with regard to the data subject[37]. Several Member States have used this provision. It is interesting to state that the UK Data Protection Act has explicitly linked the informational requirement to the fairness principle in order to enable processing with regard to the data subject to be fair. More particularly , in such case , a fairness test should be engaged every time there is collection and processing of personal data in order to secure that the data subject is provided with all the information that is necessary for him in order to give a completely informed consent[38]. According to the Data Protection Directive some specific items of information should always be provided to the data subject in order for the consent to be valid. The data subject should be duly informed before the transfer of his personal data on the specific circumstances in the frame of the general principle of loyalty. For instance, the data subjects should be informed about the particular risk arising from the fact that their data will be transferred to a country that does not provide adequate protection in order for their consent to be valid[39]. The fact that some Member States regulate in their national laws the provision of specific information to the data subject has led to a number of divergences and to some extent to a lack of harmonization on this issue. Therefore, the "fairness test" that was suggested above is a better way in order to have sufficient flexibility with regard to the information obligations of the data controller and the particularities of each processing[40].

Consequently, the data subject should be provided in a clear and understandable

[37] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, pp 96-97

[38] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 206-207

[39] Ibid, pp 208-209

[40] Ibid, p 209

manner with accurate and absolute information about the types of data that are processed and also has to be provided at least with the information included in the Data Protection Directive**.** However, there is still a difficulty in determining in each particular situation whether the information is significant. According to the European approach to data protection the principle of transparency is required in the frame of the data processing .In case of inaccurate or insufficient information, in other words lack of transparency, the consent of the data subject renders to invalid[41].

In this point , it is very interesting to be mentioned that in the field of bioethics the issue concerning how exact the informed consent needs to be both in terms of the information to be provided to the patient and of the purposes for which the consent was given , is very important in order to give an answer to the question "*how much information should be provided to the data subject"* .Taking into account that absolutely specific informed consent forms can lead in most cases to lengthy and incomprehensible documents ,one approach could be that the specificity of the information should be grounded on what a "reasonable" data controller would be willing to disclose or on what a "reasonable" data subject would need to know. However, it would not be possible to define these with certainty. In accordance with the proposal of Manson and O'Neill in the field of clinical ethics the patients should obtain a limited amount of accurate and relevant information by providing friendly ways for them to extend this amount and easy ways to abolish consent once given in order not to confront the danger of "overinformation"[42]. The GDPR agrees and emphasizes that "overinformation" should be avoided as it may lead to data subject's confusion[43]. In accordance with article 12 of GDPR the controller shall take the appropriate measures in order to provide the data subject with any information included in articles 13 and 14 and any communication in the frame of articles 15 to 22 and 34 concerning the data processing. More particularly, according to these provisions, the information should be provided in writing or else electronically. At the request of the subject, the information may also be given orally, on the condition that the identity of the subject is proved by other means. Therefore, the fulfillment of the

[41] Ibid, pp 209-210

[42] Ibid, pp 210-212

[43] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), pp 59-60

oral information should be recorded. The subject must be informed by the data controller within one month, however , this time period may be extended for a further two months , if required due to the complexity or the number of subject's requests. The data controller has to inform the data subject about the extension and also about any delay[44]. In GDPR applies the principle according to which the information is in the same form as that of the application, for example, if the subject submits the request electronically, the information is provided, if it is possible, in the same way. Although any request by the data subject does not imply an equivalent obligation of the data controller, however, the controller is obliged to inform within one month about his inaction, about the possibility of a complaint to a supervisory authority or about litigation. For instance, the data controller stagnates, in case he cannot verify the identity of the data subject. On the other hand , if there is any doubt with regard to the identity of the data subject , the controller may request additional information , which are necessary for confirmation and consequently , in such a case , it is not about collecting new data[45]. In principle, the information is made without any charge, however, in case the request of the data subject is obviously abusive or excessive due to their recurrent nature, the data controller can either to charge a reasonable fee or to refuse to meet the request. According to the article 12 paragraph 3 and article 78 paragraph 2 of GDPR the clause of abuse of rights is introduced, and for example, a request every three months is not an abuse[46]. Furthermore, the GDPR distinguishes between personal data collected by the subject (article 13) and those that have not been collected by the subject (article 14). Basically, the subject should be informed about the identity of the data controller , his contact details , the purpose of the communication , the recipients of the data and the intention of the data controller to transfer the data to a third country or organization[47]. Moreover, the existence of risks, rules, guarantees and rights of the subjects, as well as the specific purposes of the data processing, which should be clear, legal and determined at the time of the collection of the data, must be disclosed. The GDPR, in article 13 paragraph 2a, introduces also, a new type of information regarding the time period in which the data will be stored,

[44] Ibid, p 60

[45] Ibid, pp 60-61

[46] Ibid, p 61

[47] Ibid, p 63

while, according to article 14, in case the data are not collected by the data subject, then the origin of the data must also be communicated. Additionally, the GDPR establishes an obligation to inform about the change and the new purpose of the data processing, in case the personal data are used for a purpose other than that for which they were collected[48]. The Regulation extends the existing right of information by the data controller under articles 33 and 34 by informing the data subject and the supervising authority about the breach of personal data. In its recital 85 specifies that the data controller within 72 hours from the discovery of the data breach or data loss must notify the competent authority and the data subject of the infringement, if the nature of the data so requires. In case the notification cannot be made within 72 hours, the delay must be justified. Moreover, the data subject is entitled to know the data recipient even if he breached the law. The relevant information needs to be comprehensive, including the type of data, the number of persons affected, the way of the infringement, the persons that were being informed, the method of the breach recognition, the handling procedures, the corrective measures, the existing security measures, the contact details and the future actions of the data controller[49].

Taking into account that the Data Protection Directive has not clarified when the data subject should be informed in order to give his consent for the processing of his personal data, it is important to be stated that according to the 1984 and 1988 UK Data Protection Act and the Greek Data Protection Law the data subject must be informed at the time when the data are collected from the data subject. Therefore, by offering to the data subject after the collection of his personal data, it could be considered that the informational requirement is not fulfilled, because, in such case, the validity of the consent is endangered[50].The right of access is one of the fundamental rights of data subject which is satisfied by the obligation of the data controller to provide to the data subject with information about the impending data processing and more particularly, with relevant information and in an intelligible form. For instance, in the online environments, it is not sufficient when the

[48] Ibid, pp 63-64

[49]Ibid, pp 64-65

[50] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014, pp 96-97. See also Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 212

information is available somewhere on the website, but the information notice should be definitely visible to the user. Although such a condition is not explicitly mentioned in the Data Protection Directive[51], the GDPR, according to its recital 58, gives special gravity, particularly, to the information that are given to children by providing that they should be adjusted in such a way in order to be understood easily by them[52]. Additionally , the GDPR, according to its article 12 paragraph 7, provides the possibility of information in combination with standard icons in a clear , comprehensible and readable way , which even if it is available electronically , they must be readable also for visually impaired people. However, these symbols should not be given without the provision of any other information[53].

According to the previous regime the information on the processing of personal data should be provided in a clearly visible and simple way directly to the data subject at a point where the subject can easily regain it[54].

Another interesting and important issue concerning the validity of informed consent is the responsibility of the data subject. According to the position of Beyleveld and Brownsword the consent is considered as valid, when the data subject has been informed adequately and in an intelligible form, however, he did not pay the necessary attention. In such case, for example, in the field of online world, when the data subject indicates his consent for the processing of his personal data by ticking a box or signing a consent form without reading it, the data subject will not be able to claim this fact in order to prove his consent's invalidity[55]. However, the opinions differed, while issues arise with regard to the consent and privacy policies in the field of electronic communications and online environments[56], when the consent cannot be grounded on direct communicative transactions between the data controller and the data subject[57]. The GDPR gives solution to this issue by contemplating specifically

[51] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 213

[52] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 59

[53] Ibid, p 62

[54] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 214

[55] Ibid, pp 214-215

[56] Ibid, p 217

[57] Ibid, p 219

that although it is required for the data subject to be given the possibility to be informed , however , the data subject is not obliged to take account of the available information on the processing of his personal data . In other words, data subject's consent is not invalid, in case the data subject does not pay the necessary attention to the available information[58].

Undoubtedly, a major problem arises in the online world concerning the language in which the information is provided to the data subject, because the language of internet is English and the majority of information with regard to online services is provided in English. Therefore, the information society presupposes that the internet user knows the English language adequately in order for his consent to be informed[59]. The GDPR based on a transparent information policy with regard to the data subject's consent, according to article 5 paragraph1a, which is specified in recital 39, introduces that any information relating to the processing of personal data must be comprehensible in clear and simple language without misinterpretations[60]. The language must be the official language of the Member State, while information can be given only cumulatively, and not alternatively in another language. Moreover , the language should be simple and understood to someone who is not legal and to people with little difficulty in reading due to their age , low educational level , or because their mother tongue is not the official language of the Member State . In other words, legal terms and terms of foreign languages should be avoided[61].

Eventually, the GDPR in its article 13 paragraph 3 foresees that the information duty does not exist, when the data subject has already the information. Furthermore, there is also no information duty, when data have not been collected by the subject and include some business secret in accordance with the Union or Member State law[62].

---

[58] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 60

[59] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 218

[60] Carolan E., "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review 32 (2016), p 467

[61] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 59

[62] Article 14 paragraph 5 GDPR. See also European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union,

However, the GDPR in its article 5 paragraph 1a emphasizes the duty of information by stating that the breach of the principle of transparency in the processing of personal data has a significant impact on the lawfulness of the processing, and therefore, the Regulation in its article 83 paragraph 5b imposes an administrative fine of 20.000 Euros or, in case of a business, 4% of the total world-wide turnover for the preceding business year, whichever is the higher[63].

It is remarkable the fact that data subjects as users have the tendency to give easily their consent , even if their privacy is threatened , they seek access to services and wait for the benefits by suffering in the comfort of "negligent" choice and thus , they fall in the trap to give their consent . In this case, the consent is the most easy and crucial legitimate basis for the legitimacy of "online tracking profiling"[64]. Although the Regulation requires sufficient and reasonable information to be provided to the data subject in order to enhance the awareness of the subject's actions, however, it should not be overlooked the "fatigue of information", because, according to surveys, it is necessary to have an average of twenty five days a year to read the terms and conditions for the use of the online services. Therefore, the subjects-users, facing the dilemma "take it or leave it", choose to give their consent, because they worry about being excluded from the access to information and services. In such case, the truth is that the final choices of individuals are not always harmonized with their reservations about the risks of their informational privacy, because they are subjected to psychological influences and manipulation[65]. However, in this point, it should be paid particular attention to the fact that in a "take it or leave it" situation, according to recital 43 of GDPR, the consent in no case can be considered as freely given[66].

2014, p 97 and Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 64

[63] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), pp 62-63

[64] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 77

[65] Ibid, p 78

[66] Reijneveld M. D., "Quantified Self , Freedom, and the GDPR", SCRIPTed: A Journal Of Law, Technology and Society, Vol.14 , Issue 2 (December 2017), p 300

4. The qualification for unambiguous consent

In the Data Protection Directive there is a reference to the consent of the data subject as "unambiguously" given in order to legitimatize the processing of personal data (article 7) and in the context of transfers of personal data to third countries that do not ensure an adequate level of protection (article 26(i) (a))[67]. However, the European Commission in its report on the review of the Data Protection Directive concluded that there is a necessity for the notion of "unambiguous consent" to be further clarified and interpreted in a more uniform way. It is interesting to mention that the United Kingdom and Germany did not adopt the qualification for unambiguous consent[68].The additional condition of the unambiguous consent does not add any actual value to the interpretation of the way the consent should be given. Actually, in general, a valid consent can be ambiguous[69]. Actually, according to the GDPR, when consent is used as a legitimate ground for data processing, the qualification for "unambiguously given" consent has been removed on the transfer of personal data that do not ensure an adequate level of protection[70].

At this point, it is very interesting to mention the Lindqvist Case that implied the need for the unambiguous consent of individuals even when someone thinks that such consent is unnecessary and clarified the sense of unambiguity. According to the facts, Mrs Bodil Lindqvist, a catechist in the parish of a small city in Sweden, during the course of a data processing, created an internet page. Parishioners, using this page, could obtain information they might need. On this page, she provided personal information about her and some of her colleagues, for example information about their jobs and hobbies, family conditions and telephone numbers. She even included information about her colleagues, for example that one of them had injured her leg and for that reason she was working half time. Mrs Lindqvist did not inform them about this internet page and therefore, their colleagues did not consent on the processing of their personal data .Taking into account the large number of personal information that is published online every day, questions raise .Would the consent of

[67] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 226

[68] Ibid, pp 226-227

[69] Ibid, p 235

[70] Ibid, pp 145-146

the colleagues of Mrs Lindqvist be necessary? The Court of Justice found that if Mrs Lindqvist had obtained the consent of her colleagues, in this case, the processing of personal data could have been legitimated. However, someone could support that the data subject's consent on publishing information about him online, would be practically unnecessary[71]. Additionally, the Court of Justice in its ruling on the *Lindqvist* case took an interesting position on the "household exemption" and its interpretation in accordance with the data publication on the internet. More particularly, the household exemption is related only to activities in the context of private or family life of individuals and it has clearly not to do with the processing of personal data by publishing on the internet. In 2007, the Swedish data protection legislation introduced the "unstructured processing", which facilitated the everyday processing of personal data in electronic communications. In this case, there is a focus on the structure of the data and not on the type of the information in any continuous text, the sending of e-mails with personal data, the publishing of personal information on websites or the recordings of images or sound. In other words, the unstructured processing of personal data is allowed unless it constitutes an abuse of individual's privacy, for example, such infringement is constituted by the spreading of personal data in order to harm the reputation of an individual or the intentional use of misleading personal data .Consequently, the exceptional unstructured processing of personal data implies a balance test in order to ensure that individual's privacy is not infringed[72]. The European Commission with regard to the provisions of the Data Protection Directive made a distinction between processing of personal data in the public and in the private sector putting as priority the consent of the data subject on the processing of personal data and therefore, the processing of personal data without the consent of the data subject was only allowed in certain circumstances. In 1992, the European Parliament eliminated this distinction introducing the consent as one of the six grounds that legitimated the processing of personal data. Actually, the Czech Republic, France, Greece and Portugal, have adopted consent as the primary ground in order to be the processing of personal data legitimate[73]. The Essence of

[71] Ibid, pp 227-229

[72] Ibid, pp 228-231

[73] Ibid, pp 231-232

"Unambiguously" is necessary in order to cover cases when the data subject is under pressure for giving his consent for the processing of his personal data. For instance, this could be happened when an employee gives his permission for the processing of his personal data by his employer. The unambiguity entails that the data processing is based on a decision of the data subject. The fact that the consent is given unambiguously inferred from certain actions of the data subject and therefore, there is no doubt about the fact that the consent has actually been given[74]. Additionally, it is important to say that according to the position of the article 29 Working Party, in the frame of transfers of data to third countries, "unambiguous consent" should be constituted by a positive and specific act, which entails that the beyond any doubts consent of the data subject for the transfer of his data has to be obtained prior to the actual transfer. Taking into account that in the frame of transfers of data to third countries there is indirect contact between the data controller and the data subject , in practice , it is difficult to base the transfer of personal data to third countries that do not ensure an adequate level of protection on the consent of the data subject, because the data controller on one hand has to prove that the consent of each data subject has really been obtained, and on the other hand that the consent of the data subject is based on sufficiently precise information, including information on the lack of protection in the third country . In practice, in most of these cases, a contract between the data subject and the data controller could be useful. Portugal, Spain, Sweden and Luxembourg, which have included the element that the consent has to be unambiguous, have already adopted this approach[75].

The General Data Protection Regulation foresees specifically, already from the definition given in its Article 4 (11), consent must be a statement of will, free, concrete and in complete awareness by which the data subject indicates that he agrees with a statement or a clear positive action that his personal data may be processed[76]. In other words, in practice, there must be an unambiguous indication of the data subject's wish that the way the consent is collected should leave no room for doubt[77].

[74] Ibid, p 232

[75] Ibid, pp 233-234

[76] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 43

[77] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 150

a. Ways how to express unambiguous consent

The General Data Protection Regulation particularize the ways how the consent can be given in order to signify the agreement of the data subject to the processing of his personal data .In particular , this can be happened either by a statement or by a clear affirmative action . In other words, consent can be expressed via the ticking of a box, in online environments, and via any other statement or conduct that would clearly show that the data subject wishes to consent to the processing of his personal data in a particular context[78]. In this point, it is important to say that the recital 32 of GDPR points out that with regard to the example of providing consent via ticking a box should be complemented by the explicit clarification that an active action on behalf of the data subjects in ticking the box is needed and that the use of pre-ticked boxes should not be considered as giving valid consent. Moreover, in connection with the electronic consent the GDPR introduces that in case the consent of the data subject is to be given after an electronic request, the request must be unambiguous, concise and not unnecessarily disruptive to the use of the service for which it is provided[79].This fact is actually, softening the requirements of the consent in online environments, because it would also allow actions such as downloading an application or playing an online game to constitute consent[80].

b. Implied consent

Generally, the consent of the data subject cannot result from silence. Proportionally, in data protection the data subject's consent can be inferred from specific actions of the data subject, however, it should not be inferred in case there is no action or complete silence of the data subject[81]. In this point, it is significant to be clarified that

[78] Reijneveld M. D., "Quantified Self , Freedom, and the GDPR", SCRIPTed: A Journal Of Law, Technology and Society, Vol.14 , Issue 2 (December 2017), p 299

[79] Recital 32 GDPR. See also Carolan E., "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review 32 (2016), p 467

[80] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 150-151

[81] Ibid, pp 168-169

the full silence of the data subject, in the notion of complete lack of action cannot be considered as "signification", because some kind of action is needed for the processing of his personal data[82]. However , although the total silence of the data subject would not be considered as consent , when the silence is combined with some other actions of the data subject , for example with the fact that the data subject had given an earlier positive indication of his consent , then it could be sufficient[83]. The GDPR in its recital 32 follows the same line by quoting indicative ways of expressing consent, for example, the completion of a box when visiting a website, the choice of the desired technical arrangements for information society services or a statement or a behavior that clearly states that the data subject accepts the proposal to process the personal data that concerned[84], while it is clarified that silence, pre-filled squares or inaction should not be considered as consent[85].

5. Explicit consent

The General Data Protection Regulation initiates some significant changes to the definition of consent. Besides freely given, specific and informed - requirements which are already foreseen in the Data Protection Directive-, the consent of the data subject has to be also unambiguous. The Data Protection Directive requires that consent is 'explicit' only in relation to the processing of sensitive data. In General Data Protection Regulation the criterion that consent has to be 'explicit' is added in order to avoid parallelism with 'unambiguous' consent and in order to have one single definition of consent, ensuring that the data subject realizing that, and to what, he or she gives consent . In other words, in practice, there must be an unambiguous indication of the data subject's wish that the way the consent is collected should leave

[82] Carolan E., "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review 32 (2016), p 467

[83] Kuner, Ch., European Data Protection Law - Corporate Compliance and Regulation, 2nd edition, Oxford University Press, 2007, para 2.17

[84] Recital 32 GDPR. See also Carolan E., "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review 32 (2016), p 467

[85] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 73

no room for doubt[86].

a. Explicit consent for the processing of sensitive data

Although the processing of sensitive data, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, is in principle prohibited, however, their processing is exceptionally allowed, when the data subject has given his explicit consent, except in cases when the prohibition of the processing of sensitive data may not be lifted by the data subject's giving his consent**.** Until now the exceptional processing of sensitive data was allowed, in case the processing is necessary to protect the vital interests of the data subject and when the data subject is physically or legally incapable of giving his consent and also, when it is carried out by a foundation, association or any other non-profitseeking body with a political, philosophical, religious or trade-union aim, when the processing takes place in the course of its legitimate activities. This is allowed only when the processing concerns solely the members of the body or to persons who have regular contact with it in relation to its purposes and that the data are not disclosed to a third party without the *consent* of the data subjects[87]. The concept of "explicit" consent in the context of the processing of special categories of data is also met in the Data Protection Directive .This kind of data are commonly known as "sensitive data". In principle, their processing is prohibited and exceptionally allowed when there is an explicit consent of the data subject. Some Member States have interpreted the condition for explicit consent as written[88]. The consent is explicit when it is indicated in such a way (for example electronically, verbally, written) that the relative wish of the subject comes directly[89]. The GDPR, in its article 9 paragraph 2a, refers to explicit consent as an additional guarantee in the case of lawful processing of specific data categories[90].

[86] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 150

[87] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 146-147

[88] Ibid, p 236

[89] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 91

[90] Article 9 paragraph 2 GDPR. See also Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 73

b. The concept of sensitive data

In this point, it is necessary to clarify the notion of "Sensitive Data". In principle, it is important to say that the data subjects' right to privacy is not jeopardized by the content of the personal data itself. However, there are particular categories of personal data that can threaten the data subjects' right to privacy exactly due to their content[91]. In accordance with the Data Protection Directive 95/46/EC, such data are personal data which concern the past , current or future , disclosing racial or ethnic origin , for example , the information on the skin color of the data subject , political opinions, religious or philosophical beliefs , for example , all relevant activities of the data subject, including the case when a data subject does not belong to any relevant organization , trade-union organization , and data with regard to health or sex life , for example , the drug or alcohol abuse of the data subject[92]. The General Data Protection Regulation, in article 9 paragraph 1, apart from these categories, includes further in the frame of the notion of sensitive data the processing of genetic data with regard to genetic material analysis, biometric data for the unambiguous identification of the individual and data that regard to the sexual orientation[93]. It should be stated that there is an important change from the Directive to the Regulation in the frame of sensitive data, as particularly, the Regulation includes genetic and biometric data as personal data[94].

At this point, it is important to make a discrimination between health data as a term and medical data. In particular, health data as a term is wider, because these data are kept not only by doctors but also by persons who do not have the medical capacity, for example, physiotherapist or psychologist. It is interesting to mention that health data are not only those which are kept in the records of the National Medical Assisted Reproduction, but also the data concerning the donors and the recipients of human

[91] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 236

[92] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law" , Publications Office of the European Union, 2014 , p 47

[93] Article 9 paragraph 1 GDPR. See also Zarsky, Z., "Incompatible: The GDPR in the Age of Big Data", Seton Hall Law Review, Vol.47, Issue 4 (2017), pp 1012-1013

[94] Safari B. A., "Intangible Privacy Rights: How Europe's GDPR will set a New Global Standard for Personal Data Protection", Secton Hall Law Review, Vol. 47 Issue 3 (2017), p 826

tissues and are kept by the National Organization of Transplantation. Additionally, as sensitive data can be considered the data administered by the Social Services, for example, issues of adoptions, and also the data administered by Insurance and Retirement Institutions[95]. Also, it should be noted that data of economic behavior and bank accounts are not sensitive, although they are protected by banking secrecy[96]. Nevertheless the Data Protection Directive did not include the data regarding to criminal convictions to the list of sensitive data in its relevant article, the processing of which is prohibited, it provides particular safeguards in connection with the processing of data concerning offences, criminal convictions or security measures, which may have taken place only under the control of official authority, or if suitable particular safeguards are provided under national law. Some Member States have actually extended the list in order to include more types of data, such as data on debts, financial standing and the payment of welfare[97].

The GDPR introduces a specific provision with regard to the processing of personal data concerning criminal convictions and offences in its article 10. It foresees particularly, that "Processing of personal data relating to criminal convictions and offences or related security measures…shall be carried out only under the control of official authority or when the processing is authorized by Union or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority"[98].

The distinction between simple, in other words non-sensible and sensitive data is of practical importance, because sensitive data should receive reinforced legal protection. According to the Greek Data Protection Law (Law 2472/1997) in the processing of sensitive data the consent is required to be written, while in the processing of simple data it is sufficient to be verbally, however in any case explicit[99]. Particularly, in electronic communications consent is required to be written or

[95] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 48

[96] Ibid, pp 51-52

[97] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 237

[98] Article 10 GDPR

[99] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek) , p 94

electronically supplied[100]. According to the article 9 paragraph 2a of the GDPR in the frame of sensitive data the data subject is required to give his explicit consent[101].

In the frame of the sensitive data the *explicit* consent of the data subject is required, because the *unambiguous* consent that is asked for the processing of personal data is not considered as sufficient. However, the term *explicit* in the context of the processing of sensitive data and how it differs from unambiguous consent is not defined in any way[102]. A higher standard of proof, in which the consent is distinctly stated is implied by an explicit consent. In the frame of the meaning of the explicit consent it is considered as an affirmative act by the data subject which clearly consent to the processing .In accordance with the Article 29 Working Party, a written consent is not required for the processing of sensitive data, because on the one hand, the *explicit* consent must be related specifically to the sensitivity of the data, taking into account that the data subject must be aware that he is disclaiming special protection. However, on the other hand, oral consent may not be easy to be proved. It is interesting to mention that the Dutch Data Protection Authority supported that the consent of the data subject is explicit when the data subject has expressed itself actively with regard to the scope of the consent[103]. However, in practice, difficulties arise, because the data controller has to be in a position to prove that the explicit consent of the data subject is obtained relying on precise information. For example, when the consent of the data subject for the processing of his health data has to be obtained by the data controller and the two parties have no direct contact. Therefore, several Member States have promoted written consent with regard to the processing of sensitive data. In particular, it is worthy to be said that the French Data Protection Act and the Greek Data Protection Law required the "express consent" for the processing of sensitive data and the French Courts interpreted this provision as "*in writing".* According to the Belgian Data Protection Act the processing of sensitive data also required the written consent of the data subject .Due to this fact criticism has been raised by legal scholars, who argue that the Belgian Data Protection Act goes

[100] 7/2001 decision of the Greek Data Protection Authority, KNoB 50 (2002) 1675,1676

[101] Article 9 paragraph 2a GDPR. See also Zarsky, Z., "Incompatible: The GDPR in the Age of Big Data", Seton Hall Law Review, Vol.47, Issue 4 (2017), pp 1012-1013

[102] Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 241

[103] Ibid, p 244

beyond the Data Protection Directive by requiring written instead of explicit consent. This example proves that there is no perspicuity among the European Member States with regard to how the requirement for explicit consent should be interpreted[104]. Consequently, it has to be said that a harmonized pan-European interpretation of the requirement for explicit consent is not easy to be achieved[105]

.

c. Explicit consent and profiling in the Data Protection Regulation

It is important to note that the General Data Protection Regulation introduces consent with regard to the automated processing of personal data for profiling**.** In particular, the GDPR provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. According to the Article 22 of the GDPR the data subject has the right not to be subject to a decision when it is based on automated processing and it produces a legal effect or a similarly significant effect on the data subject. This right does not apply if the decision inter alia, based on explicit consent[106]. The GDPR defines profiling as any form of automated processing intended to evaluate certain personal aspects of the data subject, specifically, to predict or analyze his performance at work, economic situation, health, personal preferences, reliability, behavior, location or movements. Additionally, automated decisions taken for the purposes listed in article 9 paragraph 2 should not inter alia, be based on the explicit consent of the data subject[107].

III. Legal capacity for the provision of consent-Physical or legal incapacity

The consent can be given by the data subject or by the statutory or legal representative, when the data subject is incapable of giving his consent. The previous

[104] Ibid, pp 245-247

[105] Ibid, p 251

[106] Article 22 in conjunction with article 9 paragraph 2a GDPR

[107] Article 22 GDPR. See also Safari B. A., "Intangible Privacy Rights: How Europe's GDPR will set a New Global Standard for Personal Data Protection", Secton Hall Law Review, Vol. 47 Issue 3 (2017), p 827

legislation with regard to the Data Protection did not address the issue of physical or legal incapacity, but leaves this to the national legislation of the Member States. However, it is important to mention that the agreement of an individual who is incapable of consenting to the processing of his personal data, should not be taken into account as *strict sensus* consent, in accordance with the Data Protection Directive[108]. The General Data Protection Regulation introduces Article 8 to the processing of personal data of children, paying special attention to issues concerning under ages' consent. When an information society service is offered directly to a child, the GDPR is differentiating between children above at least and below 16 years of age. In the latter case, the processing of the children's data is lawful only to the extent that the child's parent or custodian has given or authorized their consent. However, in any case, if Member States want to provide by law a lower age for similar purposes, such lower age is not below 13 years[109]. In this point, the Regulation leaves a blank by not making any provision on other sensitive groups without physical or legal capacity. It could be indicated that the Regulation probably, leaves this issue to the national legislation of the Member States.

IV. Unlawful processing despite the existence of consent

It should be emphasized that the consent of the subject to the processing of his personal data, even if it is freely given, specific, unambiguous and informed, in other words it meets the requirements of the law as it was mentioned above, is not considered as lawful, when the consent is not legal for any other reason, for example, when it violates the principles of the processing or when there is a law stating that in a particular case the consent does not cease the prohibition[110]. At this point, it is important to mention indicatively some cases in order to be understandable. For instance , it is not legitimate to complete a specific question to a form of the National Statistical Service on the consent of the subject on the removal of his tissues in the

[108] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 160-161
[109] Ibid, pp 164-165. See also article 8 GDPR

[110] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 94

frame of transplantation , because it exceeds the purpose of the relative processing[111], or it is not legitimate to include the religion or the fingerprint or the gender or the occupation or the surname of the husband or wife or the place of residence or the nationality in the police identities , because any processing of personal data that goes beyond the intended purpose, for example the confirmation of the identity of the subject , or is not offered and necessary to achieve this purpose , is not lawful and all these data are unnecessary in order to confirm the identity of the subject[112], moreover, it is unlawful to process the personal data in the frame of the concept of a television show , because in this case the processing leads to the disappearance of private life and the depreciation of human existence[113]. At this point, it is remarkable the fact that the GDPR remains silent by not foreseeing anything specific.

V. Exceptions to the rule of necessity of consent

The subject's right of informational self-determination is delimited by deliberations, which serves either his contractual relations, or his objective interest, or the general interest, or the interest of third persons, which in any given case exceeds the rights and the interest of the subject. Therefore, the data controller's obligation to obtain the consent of the data subject is amenable to exceptions. However , it is important to emphasize that even if the subject's consent is not required for the processing of his personal data , the data controller has the obligation to inform the subject about the processing , unless it is an exceptional case , where , according to the law , no information is needed , when the collection of the data relates particularly to public persons for journalistic purposes , for national security or for the investigation of particularly serious crimes . There are exceptions to the rule of necessity of consent firstly, in the frame of simple data and subsequently, in the frame of sensitive data[114]. At this point, it is interesting to mention that in accordance with the 87/2013 decision, the Court of Appeals of Thessaloniki in Greece judged that in the frame of this case,

[111] 7/2001 decision of the Greek Data Protection Authority, KNoB 50 (2002) 1675,1676

[112] 510/17/2000 decision of the Greek Data Protection Authority

[113] 92/2001 decision of the Greek Data Protection Authority, KNoB 50 (2002) 1681

[114] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 96

although the employer was not required to obtain the employee's consent in order to inform the third party about the amount of the redundancy payment received by the employee, however, he was obliged to inform the employee first about what he intended to do[115].

a. Processing of simple data without subject's consent

There are some exceptional cases in article 6 paragraph 1b,c,d,e,f of GDPR based on the provisions of the Data Protection Directive , in which processing of simple data is allowed without subject's consent[116]:

- **when processing is necessary for the performance of a contract to which the data subject is a party [117]**, for example , the indication of the shared data block of the apartment owners may be carried out without their consent, to the extent that it is necessary for management purposes , because it is required for the fulfillment of contractual obligations . Additionally, the consent of employees is not required in order for their data to be processed, in case, it is necessary for determining their payment[118].
- **when the processing is necessary in order to fulfill the obligation of the controller , which is imposed by the law**[119], for example, the processing of customers' data from a merchant for tax purposes to the competent tax authority[120].
- **when processing is necessary in order to preserve the vital interest of the data subject[121]**, for example, it is legitimate to process the personal data of the

[115] 87/2013 decision of Court of Appeal of Thessaloniki, Armenopoulos 67 (2013), pp 521-523

[116] Article 6 paragraph 1 b, c, d, e, f GDPR. See also Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), pp 97-99

[117] Article 6 paragraph 1b GDPR

[118] 72/2001 decision of the Greek Data Protection Authority, KNoB 50(2002) 1678

[119] Article 6 paragraph 1c GDPR

[120] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 97

[121] Article 6 paragraph 1d GDPR

subject, whose life or health is in danger, and therefore, he is unable to give his consent to the hospital in order to create a medical file, because he is presumed that he would have given his consent, if he was not in a physical or legal weakness[122].

- **when the processing is necessary for the execution of a project of public interest or a project , which is carried out by a public authority , or assigned by this authority to the controller or a third party[123]**,for example , the processing of personal data of taxpayers in order to impose on them legal fees[124] and also , the disclosure of the names of the members of the Administrative Board and their remuneration to the Members of Parliament in the frame of parliamentary control[125].
- **When the processing is absolutely necessary in order to satisfy the legitimate interest of the controller or of third parties , or when the pre-mentioned legitimate interest obviously overrides the rights and interests of the subject and does not undermine his fundamental freedoms, however, this shall not apply when the public authorities carry out the processing in the performance of their tasks[126]**, for instance , it is legitimate for the company TEIRESIAS S.A. to keep a "black list" of bad-payers , because the interest of the bank overrides the interest of the subjects not to process their financial data[127], and also , the providing of evidence from the disciplinary file of an employer to her colleagues is deemed to be lawful for the purpose of using them in order to challenge her claim against them[128].

[122] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 98

[123] Article 6 paragraph 1e GDPR

[124] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), pp 98-99

[125] 48/2001 decision of the Greek Data Protection Authority, KNoB 50(2002) 1678

[126] Article 6 paragraph 1f GDPR

[127] 24/2004 decision of the Greek Data Protection Authority, KNoB 52(2004) 683

[128] 87/2013 decision of Court of Appeal of Thessaloniki, Armenopoulos 67 (2013) , p 525

b. Processing of sensitive data without subject's consent

Additionally, there are some exceptional cases, according to the GDPR based on the provisions of the Data Protection Directive, in which processing of sensitive data is also allowed without subject's consent. These are the following[129]:

- **when processing is necessary in order to preserve the vital interest of the data subject[130]**, for example, it is legitimate to process the personal data of the subject, whose life or health is in danger, and therefore, he is unable to give his consent to the hospital in order to create a medical file, because it is presumed that he would have given his consent, if he was not in a physical or legal weakness[131].
- **When the processing relates to data made public by the subject[132]**, for example, with his interview, publications or public speech, or on the internet, or it is necessary for the recognition, the exercise or the defense of subject's or third party's right to a court or to a disciplinary body, on condition that the processing was not done illegally at the stage of collecting or at a subsequent stage[133].
- **When the processing concerns health data and is performed by a person professionally engaged in the services of health care[134]**, for example, physiotherapists, doctors , midwives , psychologists etc. , who have a duty of confidentiality under the condition that processing is necessary for the prevention, diagnosis, hospitalization or management of health services.

[129] Article 9 paragraph 2c, e, f GDPR. See also Zarsky, Z., "Incompatible: The GDPR in the Age of Big Data", Seton Hall Law Review, Vol.47, Issue 4 (2017), pp 1012-1013

[130] Article 9 paragraph 2c GDPR

[131] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 101

[132] Article 9 paragraph 2e GDPR

[133] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 102

[134] Article 9 paragraph 2f GDPR

Instead, the consent of the subject is required, when personal data of patients are used at medical conferences[135].

The GDPR in paragraph 2 b, d, f, g, i, j of article 9, apart from these cases, introduces further some additional relevant cases[136]. More particularly , the processing of sensitive data in GDPR is allowed without subject's consent , additionally , when *<< (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law , in so far as it is authorized by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political , philosophical , religious or trade-union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; (f) processing is necessary for the establishment , exercise or defense of legal claims or whenever courts are acting in their judicial capacity; (g) processing is necessary for reasons of substantial public interest , on the basis of Union or Member State law which shall be proportionate to the aim pursued , respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject ; (i) processing is necessary for reasons of public interest in the area of public health , such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal devices , on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject , in particular professional secrecy ; or (j) processing is necessary for achieving purposes in the*

[135] Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek), p 102

[136] Ibid, p 101 reference 249. See also Zarsky, Z., "Incompatible: The GDPR in the Age of Big Data", Seton Hall Law Review, Vol.47, Issue 4 (2017), pp 1012-1013

public interest , scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued , respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject>>[137].

Despite all these mentioned above, it is also significant to state that although the GDPR in its article 9 paragraph 2e repeats the relevant provision of the Directive 95/46/EK, but in a different social and technological context, and particularly, that processing of sensitive data is allowed without subject's consent when the processing relates to data made public by the subject, the Regulation seems to ignore the reality of the subject's self-exposure and the problems that arises[138]. For instance, in case employees have posted their personal data in an unreasonable time and in a different context on digital social networks, employers should not consider these information, even if they are the same as those posted in publicly available profiles or in public accounts in social networking tools[139]. In the frame of subject's self-exposure and his sensitive data, it should be evaluated not only the obvious character and the purpose of the publicity, but also the context in which it is carried out, because the subject may upload personal information that relate to it in a different context and relevance and possibly at moments that are at a distance from their use[140].

Moreover, at this point, it should be noted that according to article 9 paragraph 4 of GDPR, Member States may adopt more conditions in order to include limitations concerning the processing of genetic data, biometric data or health data[141].

In conclusion, taking into account the silence of the Regulation mentioned above with regard to the exceptions in the context of the absence of consent to the processing of simple personal data, someone could note in this point that the Regulation in any case

[137] Article 9 paragraph 2b,d,,f,g,i,j GDPR

[138] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 79

[139] Ibid, p 80 reference 223

[140] Ibid, pp 80-81

[141] Article 9 paragraph 4 GDPR

intends to give particular importance to the promotion of sensitive data.

VI. The withdrawal of consent

Although the previous legislation did not explicitly refer to the withdrawal of consent, this right derives from the right to informational self-determination of the data subject. The data subject cannot waive his right to withdraw his consent in the future. At this point , it is important to indicate that there is a differentiation between the withdrawal of consent and the data subject's right to object, because , on the one hand, the withdrawal of consent concerns a consent that has already been given by the data subject for the processing of his personal data, and on the other hand, the right to object is applicable to data processing that is not based on the consent of the data subject, but on another of the grounds that is necessary for the lawfulness of the data processing. The data subject has also the possibility to withdraw his consent, whenever he wishes. Moreover, due to the withdrawal of consent, the data has no obligation to delete all traces of prior processing, if documentation is necessary[142]. The GDPR is stricter than the previous legislation with regard to the withdrawal, therefore, it is required explicitly in accordance with its article 7 paragraph 3 that the withdrawal of subject's consent must be as easy as providing it in the frame of principle of freedom of subject's choice and it shall not influence the lawfulness of processing before consent's withdrawal. Moreover, like the previous legislation, it requires subject to be informed of his right to withdraw his consent before he gives it[143].

VII. Right to erasure or " right to be forgotten"

The withdrawal is effective only for the future and not retrospectively, because in such case, the data processing that was based on the given consent unlawful, would be rendered. In that sense the data subject is not able to control personal data to the

[142] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law" , Publications Office of the European Union, 2014 , p 60. See also Kosta E., "Consent in European Data Protection Law", Brill, 2013, p 251

[143] Tovino, S., "The HIPPA Privacy Rule and the EU GDPR: Illustrative Comparisons", Seton Hall Law Review, Vol.47, Issue 4 (2017), p 988. See also article 7 paragraph 3 GDPR

processing of which he consented in the past[144]. The GDPR introduces the "right to be forgotten" in order to restore the power balance between data subjects and data controllers with regard to the adaption of the data subject' s choices for the processing of his personal data . This right ensures that when an individual no longer wants their personal data to be processed, and if there is no legitimate reason for an organization to keep it, they should be removed. The GDPR complements the right of the data subject to ask the erasure of his personal data which was foreseen in the Data Protection Directive by the right to be forgotten. At this point, it is important to state that the GDPR improperly identifies the meaning of the oblivion with the sense of deletion[145]. More specifically, the General Data Protection Regulation in article 17 foresees that the data subject has the right to ask the data controller to erase personal data that relate to him and not to disseminate them further. For example , this can happen when the data are no longer necessary for the purposes for which they were collected or further processed, when the data subject withdraws his consent for the processing of his personal data and the processing cannot be based on another legitimate ground, when the storage period to which the data subject had consented has expired, when the data subject objects to the processing of his personal data, and when the data processing does not comply with any provisions of the GDPR[146]. Furthermore, the GDPR introduces that when the data controller has made the personal data public, third parties should be informed that they are processing data for which the data subject wants to exercise his right to be forgotten, asking them to eliminate any links to, or copy or replication of the data. In this case, technical measures have to be taken by data controller with "all reasonable steps" generally, concerning the related data. In this point , it is important to be mentioned the fact that the data controller sometimes may not even be knowledgeable of all existing copies or replications of the data or of all the places where personal data have been diffused . In any case, the GDPR actually, does not introduce an obligation of these third parties to

[144] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law" , Publications Office of the European Union, 2014, p 111

[145] Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), p 75

[146] Edward L., "Recognizing Rights in Real Time : The Role of Google in the EU Right to Be Forgotten" , U.C. Davis Law Review, Vol.49 , Issue 3 (February 2016), pp 1047-1048

carry out the erasure of the data. Therefore, it is remarkable that the right to be forgotten in the GDPR may have significant interpretative difficulties on the Internet use[147].

VIII. Burden of proof for the acquisition of consent

The General Data Protection Regulation reinforces the concept of consent by introducing the general principle of accountability into its article 7 paragraph 1[148]. It clarifies that the data controller has the burden of proof that the data subject consent has been provided for specified purposes. Taking into account that the data controller will be responsible to prove that the data subject consent was provided in a valid way for a specific data processing operation, the data controller should also use reliable means in order to obtain the consent within the framework of the sensitivity of each particular data processing[149]. In this way, the need to document the receipt of consent in writing or by electronic means is registered[150].

IX. Overall assessment and future perspectives

The replacement of the Data Protection Directive with the GDPR entails the development of the existing legislation in the frame of data protection and more particularly, the empowerment of the right of consent by converting this right to a fundamental source of legitimization of the processing. In other words, it provides more flexibility, legal certainty and coherence by covering the gaps of the law and clarifying some ambiguities. It has added criteria and conditions in order to ensure the provision of consent in relation to the freedom of choice and the total awareness of the subject when he gives his consent. Furthermore, the GDPR establishes more

[147] Kosta E., "Consent in European Data Protection Law", Brill, 2013, pp 252-254

[148] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), p 74

[149] European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law" , Publications Office of the European Union, 2014 , pp 75-76

[150] Inglezakis I., "The consent in Personal Data Law" in: Kotsali L., Personal Data (in Greek), Nomiki Bibliothiki Publications, 2016, p 95 (109)

transparency and simple information policies and thus, it gives the control to the data subject[151].

More specifically, in GDPR the consent should be "freely-given" expressing an act of informational self-determination**.** It should be also an autonomous act of the data subject and a product of free decision, in other words, free from external manipulations. However, there are some cases in which consent actually, cannot be given freely, more particularly, when there is a clear unbalance between the data subject and the data controller.

Moreover, the GDPR in its article 4 (11) foresees particularly, that the subject's consent to the processing of his data should be, inter alia, specific and in full knowledge. More specifically, in its recital 43 the Regulation adopts the principle of prohibiting the provision of total consent, as separate consent is required for distinct processing operations. In other words, in accordance with the article 6 in conjunction with recital 32 of GDPR, consent may relate to processing for one or more purposes. However, it must be specific. Exceptionally, the GDPR in order to ensure flexibility which corresponds to reality, introduces the concept of "broad" or "blanket" or "generic" consent, according to which it is possible to be granted an overall consent in the frame of certain areas of scientific research , to the extent permitted by the intended purpose. The aim is to facilitate scientific research in order for the researcher to get rid of the burden of multiple consents when changing purpose in his research.

Furthermore, the GDPR based on a transparent information policy with regard to the data subject's consent, according to article 5 paragraph1a, which is specified in recital 39, introduces that any information relating to the processing of personal data must be comprehensible in clear and simple language without misinterpretations. In GDPR with regard to the concept of unambiguous consent there must be an unambiguous indication of the data subject's wish that the way the consent is collected should leave no room for doubt. The criterion that consent has to be 'explicit' is added in order to avoid parallelism with 'unambiguous' consent and in order to have one single definition of consent, ensuring that the data subject realizing that, and to what, he or

[151] See also Albrecht J. P., "How the GDPR will change the World", European Data Protection Law Review (EDPL), Vol.2, Issue 3 (2016), p 288

she gives consent. In particular, the GDPR, in its article 9 paragraph 2a, refers to explicit consent as an additional guarantee in the case of lawful processing of specific data categories.

Additionally, the General Data Protection Regulation introduces Article 8 to the processing of personal data of children, paying special attention to issues concerning under ages' consent. However, it should be taken into account that the GDPR foresees nothing with regard to the protection of sensitive groups other than children, for example, online illiterates.

However, it is remarkable the fact that the GDPR remains silent by not foreseeing anything specific with regard to the unlawfulness of the processing despite the existence of consent. It is also significant to state that although the GDPR in its article 9 paragraph 2e repeats the relevant provision of the Directive 95/46/EK, but in a different social and technological context, and particularly, that processing of sensitive data is allowed without subject's consent when the processing relates to data made public by the subject, the Regulation seems to ignore the reality of the subject's self-exposure and the problems that arise.

The GDPR is stricter than the previous legislation with regard to the withdrawal , therefore, it is required explicitly that the withdrawal of subject's consent must be as easy as providing it in the frame of principle of freedom of subject's choice and it shall not influence the lawfulness of processing before consent's withdrawal. Moreover, the Regulation based on the previous legislation requires subject to be informed of his right to withdraw his consent before he gives it. The General Data Protection Regulation introduces the "right to be forgotten" in order to restore the power balance between data subjects and data controllers with regard to the adaption of the data subject' s choices for the processing of his personal data . This right ensures that when an individual no longer wants their personal data to be processed, and if there is no legitimate reason for an organization to keep it, they should be removed. Furthermore, the GDPR introduces that when the data controller has made the personal data public, third parties should be informed that they are processing data for which the data subject wants to exercise his right to be forgotten. . In any case, however, the GDPR actually, does not introduce an obligation of these third parties to carry out the erasure of the data. Therefore, it is remarkable that the right to be

forgotten in the General Data Protection Regulation may have significant interpretative difficulties on the Internet use.

The General Data Protection Regulation also reinforces the concept of consent by introducing the general principle of accountability into its article 7 paragraph 1. The data controller will be responsible to prove that the data subject consent was provided in a valid way for a specific data processing operation, the data controller should also use reliable means in order to obtain the consent within the framework of the sensitivity of each particular data processing.

In any case, it can be argued that the GDPR, on the one hand, rejects the trend towards liberalization of personal data that is adopted by Member States such as Germany, on the other hand, the Regulation should not be considered as conservative. It is an evolution of the previous data protection law and not a revolutionary law[152]. Eventually, it cannot be overlooked the fact that the rapid development of the technology and the complexity of contemporary needs lead, in practice, to the emergence of problems. In conclusion, although the contribution of the Regulation is very important with the changes it brought in the frame of the notion of consent, however, there is a possibility of completing and further developing, because it still leaves voids and ambiguities in the law. Otherwise, the legislation in the context of either European or global harmonization will always have the need for development and improvement.

X. Concluding remarks

In conclusion, consent has always been a basic concept in the context of the protection of personal data, nevertheless it has not always been clear, when it is required and under what conditions it is valid. There have been divergences in the transposition of the relevant provisions of the Directive 95/46/EK into the Member States, while the Law 2472/97 has been more detailed. Eventually, the GDPR brings about few, however, significant changes[153].The replacement of the Directive with the

[152] See also Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek), pp 123-124

[153] Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek), pp 72-73

Regulation was aimed at more flexibility, legal certainty and coherence by strengthening the right of consent and by converting this right to a fundamental source of the processing legitimization. Indeed, the Regulation puts some important standards in order to define a uniform regulatory environment for different legal systems[154]. However, considering that we are living at a time when technology is rapidly evolving, and therefore, a harmonized pan-European interpretation and application of the requirements for consent is not easy to be achieved, it could be supported that the GDPR is a further step in the evolution of the law in the frame of the protection of personal data, however, with clear margins of development. Consequently, due to the complexity of contemporary needs and the trend for development, there will always be room for improvement in each legislation.

[154] Albrecht J. P., "How the GDPR will change the World", European Data Protection Law Review (EDPL), Vol.2, Issue 3 (2016), p 288

REFERENCES

BIBLIOGRAPHY

Albrecht J. P., "How the GDPR will change the World", European Data Protection Law Review (EDPL), Vol.2, Issue 3 (2016), pp. 287 et seq.

Alexandropoulou - Egyptiadou E., "Personal Data", Nomiki Bibliothiki Publications, 2016 (in Greek)

Carolan E., "The continuing problems with online consent under the EU's emerging data protection principles", Computer Law & Security Review 32 (2016), pp. 462 et seq.

Edward L., "Recognizing Rights in Real Time: The Role of Google in the EU Right to Be Forgotten", U.C. Davis Law Review, Vol.49 , Issue 3 (February 2016), pp. 1017 et seq.

European Union Agency for Fundamental Rights / Council of Europe, "Handbook on European Data Protection Law", Publications Office of the European Union, 2014

Inglezakis I., "The consent in Personal Data Law" in: Kotsali L., Personal Data (in greek), Nomiki Bibliothiki Publications, 2016, pp. 95 et seq. (in Greek)

Kosta E., "Consent in European Data Protection Law", Brill, 2013

Kuner, Ch., European Data Protection Law - Corporate Compliance and Regulation, 2nd edition, Oxford University Press, 2007

Lasprogata G./ King N./ Pillay S ., "Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada", Stanford Technology Law Review 4 (2004), pp. 4 et seq.

Mitrou L., "The General Data Protection Regulation", Sakoulas Publications, 2017 (in Greek)

Panagopoulou – Koutnagi F., "The General Data Protection Regulation 679/2016/EU", Sakoulas Publications, 2017 (in Greek)

Reijneveld M. D., "Quantified Self, Freedom, and the GDPR", SCRIPTed: A Journal Of Law, Technology and Society, Vol.14 , Issue 2 (December 2017), pp. 285 et seq.

Safari B. A., "Intangible Privacy Rights: How Europe's GDPR will set a New Global Standard for Personal Data Protection", Secton Hall Law Review, Vol. 47, Issue 3 (2017), pp. 809 et seq.

Tovino, S., “The HIPPA Privacy Rule and the EU GDPR: Illustrative Comparisons”, Seton Hall Law Review, Vol.47, Issue 4 (2017), pp. 973 et seq.

Zarsky, Z.,”Incompatible: The GDPR in the Age of Big Data”, Seton Hall Law Review, Vol.47, Issue 4 (2017), pp. 973 et seq.

CASE LAW

510/17/2000 decision of the Greek Data Protection Authority

7/2001 decision of the Greek Data Protection Authority, KNoB 50 (2002) 1675,1676

92/2001 decision of the Greek Data Protection Authority, KNoB 50 (2002) 1681

72/2001 decision of the Greek Data Protection Authority, KNoB 50(2002) 1678

48/2001 decision of the Greek Data Protection Authority, KNoB 50(2002) 1678

24/2004 decision of the Greek Data Protection Authority, KNoB 52(2004) 683

C-543/09 Deutsche Telekom AG v Bundesrepublik Deutschland [2011]

C-92/09 and C-93/09 (Joined Cases) Volker and Markus Schecke GbR/Hartmut Eifert v. Land Hessen [2010]

87/2013 decision of Court of Appeal of Thessaloniki, Armenopoulos 67 (2013)

LEGISLATION

GDPR 679/2016/EU

Data Protection Directive 95/46/EC

The Greek Data Protection Law 2472/1997