DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4190

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

OLD WINE WITH A NEW LABEL : RIGHTS OF DATA SUBJECTS UNDER GDPR

Sandeep Mittal
Cyber Security & Privacy Researcher
Former Director, LNJN NICFS (MHA)
New Delhi, India

Abstract: Recent reforms in data privacy protection framework in European Union have lead to enactment of General Data Protection Regulation (GDPR). However, it remains debatable if GDPR would lead to significant improvement in the protection of privacy rights of individuals, which is always considered the fundamental right. The advent of technology and movement of data across geographical barriers and outsourcing of data processing jobs to countries outside the EU necessitated enactments of GDPR. An analysis is done to demonstrate that though some of the provision of GDPR remain generically remain similar to the Data Protection Directive, GDPR has incorporated some new provisions by choosing the 'regulation' as an instrument of law for better harmonisation, expensing the 'right to be forgotten, legitimisation the role of consent, providing data protection by design and default, increasing accountability of data controllers and expanding the scope of provision of the directive to extra territorial jurisdiction would be remain to be seen whether GDPR is an old wine with the new label or something else in a wine bottle.

Keywords: Rights of Data; Data Protection Regulation; Accessing of Personal data; Internet of Things; Control of Users over Their Personal Data; Data Protection Framework; General Data Protection Regulation

I. INTRODUCTION

With about 46 per cent of the world's population having access to it, the Internet has emerged as most popular medium of free expression, and as tool for conducting free trade and the use of smart devices. This propensity to use the Internet for various applications has thus resulted in the generation of a large volume of personal data online including (but not limited to) the name, address, mobile number, date of birth, email address, geographical location, health record of the user, among other things. This data has a high potential of secondary use which necessitates the protection of privacy and confidentiality of this personal data both at residence and in motion across the borders.[1] [2] [3] European Union Directive 95/46/EC (The Directive) [4] remained the basic instrument for protection of data privacy for over 20 years in European Union (EU) recognizing privacy as a fundamental human right.[5] However, the practical implementation of the Directive across the EU states and the seminal decisions of Court of Justice of European Union (CJEU) raised several issues regarding an understanding and need for individual rights to protection on the Internet in EU.[6] This, in turn, triggered the process of reform in the Data Privacy Protection Framework, leading to enactment of the General Data Protection Regulation (GDPR)[7], which is slated to usher in reforms and changes in the EU Data Protection Framework. The scope of this essay is to discuss whether the GDPR signifies any improvement over the current directive in terms of the Right of Individual Data Subjects.

II. THE TRIGGER

The Directive had almost become antiquated in view of the evolution of new technology such as Internet of Things (IoT), and Cloud, among others, giving rise to a new type of risk that was unknown when the Data Protection Directive was enacted. With the advent of advanced technology and the outsourcing of online services across borders, the adoption of divergent approaches to privacy prevalent both within and outside Europe have given rise to the concern for protection of data privacy in the EU.[8] [9] [10] [11] [12] However, the more immediate trigger for reformation in this policy was the taking of seminal decisions by the CJEU, which led to a lot of important changes in the understanding of the Data Protection Regulation legal framework. In Google Spain,[13] [14] [15] it was ruled that Google would be classified as the controller, as the search, indexing, and storage of information implied the processing of personal data as defined by the Directive. Therefore, search engines are obliged to remove the links to web pages from their results if so requested by the data subject. This gave rise to serious consequences for the search engine and its credibility, as also for the role of intermediaries, as this judgement empowered individuals to ascertain their 'right to be forgotten', affecting the free flow of information on the Internet in the process. Another case in which the decision changed the legal situation relating to the data protection law was the Schrems Judgement,[16] wherein the CJEU ruled that a third country ensuring an adequate level of protection cannot eliminate or reduce the power of national supervisory authority to assess the adequacy of data protection under the Directive. Further, the court declared that the Safe Harbor Agreement [17] with the USA was invalid.[2] (Burri and Schär 2016)[18] This judgement highlighted the various challenges that the existing data protection framework was facing in an overwhelming environment of use of advanced technology over two decades since the enactment of the Directive. The following section presents a discussion on the selected key provisions of the GDPR, which could prove to be in terms of their

implications for the protection of the rights of individual data subjects.

III. THE DIRECTIVE VERSUS THE REGULATION

The legal instruments that are used by the EU are in the form of Communication, Directive and Regulation. A directive has to be transposed into the national law by enacting an amendment or new laws that would be applicable within the national territory inhabited by the members whereas a regulation can be directly applied as a law. Therefore, the problem of harmonisation of the Directive across the EU member-states has been overcome through the choice of regulation during enactment of the GDPR [19]. Albeit the Commission has promised a "strong, clear and uniform legislative framework at [the] EU level" that will "do away with the patchwork of the legal regime across the 27 member-states and remove the barrier to market entry" [20]. However, the coordination of the member countries, their respective data protection authorities, national laws and courts would not be an easy task to achieve by 2018, when the Regulation comes into force.

IV. EXPANSION OF SCOPE OF PERSONAL DATA

The 1995 Directive specifies that "personal data shall mean any data relating to identified or identifiable nature person data subjects".[21] While the identified individual is more or less clear, identifiability is not explained in the Directive. This has been explained in the GDPR and expanded in Article 29 of the Working Party Document [22] and Article 41 of the GDPR has adopted the same approach. However, the Recital 23 has introduced a proportionality test (positing that identifiability is related to "mean reasonably and likely to be used" taking account of "all objective factors such as technology, effort and cost") in order to assess each time the nature of the data that may help protect the identifiable individual. If the proportionality test is not passed, then such data will not be considered, as the personal data provision and the GDPR does not apply to anonymous data.[23] The regulation has also introduced a new class of data, that is, "pseudonymous data", which alludes to the processing of personal data in such a way that data can no longer be attributed to a specific data subject without the use of additional information, as long as such additional information is kept separately and is subject to technology and organisational measures for ensuring its non-attribution to an identified and identifiable person".[24] However, the questions that arise are: What is the relationship between pseudonymous data and personal data? Is pseudonymous data a sub-category of personal data, and does it fall under the scope of the GDPR? According to the Recital 23, "data which has undergone pseudonymization, which could be attributed to [a] natural person by use of additional information should be considered as information on an identifiable natural person". [25] If this is so, then the proportionality test would have to be applicable to the information pertaining to an identifiable person and only then should it be considered as personal data for the purpose of data protection legislation. The GDPR would also not apply to information concerning a deceased person.[26] As regards the issue of sensitive data, the regulation has adopted and applied the same approach as the Directive. It propounds that sensitive data are data which reveal "racial or ethnical origin, political opinion, religious, philosophical believes, trade union membership, processing of genetic data, biometric data in order to uniquely identify a person or data concerning health or sex life or sexual orientation".[27] Thus, genetic data, biometric data, and sexual orientation data are new categories included under sensitive data. The processing of data relating to criminal conviction and offences or relating to security measures is allowed only under the control of an official authority or after adequate safeguards have been provided under the law.[28] However, Articles 4 and 9 of the GDPR, while remaining similar to the Directive at the generic level, provide some improvement in terms of privacy protection.

V. STRONGER RIGHTS

The **"**right to be forgotten" is currently one of the most hotly debated issue because of the Google Spain judgement and has been incorporated in Article 17 of the GDPR. A data subject can now get his personal data erased and put an end to further processing if the data in question is no longer necessary for the purpose for which it was collected irrespective of whether a data subject as an individual is the subject or whether his personal data is being processed.[29] However, this right is not absolute.[30] The right to be forgotten includes an obligation on the part of the data controller who has made the personal data public to inform other controllers who would process such personal data to erase any links, copies, or replications pointing to that personal data. Also, while doing so, the data controller concerned would have to take reasonable steps in accordance with the technology and resources available to him for use including technology measures.[31] However, Article 17 may lead to certain problems, some of which are delineated below:

i) The controller may not even know or be able to contact all the third parties.

ii) The third party may have different legal grounds for not agreeing to erasure of the request of the original controller.

iii) The issue of who the third party controller would be in the case of 'Internet-bounces' is ambiguous, as the modern Internet has blurred the distinction between the controller and the data subject, leading to a grey area in the data protection law.

However, it is claimed that actually the right to be forgotten would become an absolute right only when the data is removed by every controller but ironically, modern technology developments do not allow data subjects to know the identity of the controller(s) processing their data. [32] Therefore, theoretically, it may be claimed as a 'right to be forgotten', but with practical implementation in the future, it may become 'a right forgotten'.

VI. IMPROVED CONTROL OF USERS OVER THEIR PERSONAL DATA

A host of other rights are included in the GDPR, including the right to transfer information,[33] the right of access to personal data,[34] the right to data portability,[35] and the right to object.[36] A data subject cannot be subjected to a decision based on automatic processing including profiling, which has legal or other considerable effects on the data subject. However, this right is limited if the processing is necessary for contractual obligation between the data subject and the data controller or is authorised by law as applicable in the EU, or in any of its member-states of which the data controller is a subject or if it is based on the data subject's explicit concern.[37] The right to data portability is a considerable and significant protection for users, who now have the potential right to receive their personal data in a structured, commonly used and machine-readable format. This can be transferred to another controller without hindrance from the controller who is controlling the original personal data.[38] However, it has been argued by a few that data portability may hamper innovation by making it freely available, and thereby hurting the self-correcting power of the market.[39]

The GDPR, however, limits the access right of the subject in a situation wherein the data controller is not in a position to identify the subject. The right to confirmation and the right to access to data represent greater risk of harm if the information is disclosed to someone who is not a data subject.[40] If the person requesting for this data provides additional information that facilitates his identification for restoring the right to full access to the subject, the right itself becomes a risk.[41] For example, if the data subject is asked to prove his identity by providing a copy of his passport, this proves that the person requesting for the data could be someone with the same name as data subject, but does not prove that he himself is the data subject.[42] Therefore, this right entails an undue risk to the privacy of the individual concerned and is a necessary limitation of the data protection right.

VII. THE ROLE OF CONSENT

Article 2H of the Directive defines the data subject's consent as "any freely given specific information and indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".[43] Article 7 (2) of the Directive also lists the legal grounds that make data processing legitimate, with the unambiguous consent of the data subject being one of them.[44] However, the Directive does not define how the unambiguity and the consent would be validated as both are affected by cognitive factors attributable to the data subject's behaviour, becoming even more complex in the online environment. In the context of the EU's data privacy framework, the consent is an important instrument in the hands of the data subjects for controlling their personal data. The GDPR has placed a responsibility on the data controller to demonstrate that the consent was given by the data subject.[45] It stipulates that the consent to process personal data is conditional to the performance of a contract, and that it would not be considered 'given freely'.[46] The GDPR also provides that the personal data processing of a child of or below 15 years of age is unlawful in the absence of the consent of the person having the parental responsibility of such a child.[47] The data controller also has the responsibility of making a reasonable effort to verify that such a consent is lawful.[48]

However, it remains to be seen if in practice, the consent of the data subject correlates autonomy [49] with its legitimacy. Several cognitive and psychological imitations, coupled with the demographic, cultural and racial profile of the data subject, affect and influence the complex process of giving or withholding of consent. The data subject has the right to withdraw his consent at any time, as the regulation explains that "it shall be as easy to withdraw as [to] give any consent"[50].

VIII. THE MISSING RIGHT TO EXPLANATION

It has been widely claimed that the right to explanation of a decision made by an automatic or artificial intelligence algorithm system will be legally mandated by the [3](Wachter, Mittelstadt, and Floridi 2016)GDPR,[51] which is viewed as a mechanism for ensuring better accountability and transparency.

The right to explanation can possibly to derived from:[52]

i) *Safeguard* against automated decision making;[53]
ii) Notification duties; [54] and
iii) Right to access [55]

Scholars have argued that Article 22 of the GDPR has the potential of dual interpretation as a 'prohibition' or the 'right to object', and would need to be clarified before the GDPR is implemented by 2018. Without any such clarification, prior to enforcement, Article 23 will allow for a conflicting interpretation of the right of the data subject to control any automated decision-making across the EU member-states. This conflict would become inevitable especially because different interpretations protect very different interests. Article 22, while being interpreted as ensuring prohibition, offers greatest protection of the data subject. On the other hand, if interpreted as a right, Article 22 creates a loophole that allows the data controller to prevent the person requesting for information access to Article 22 to requester under the automated decision-making rule unless an objection against that is raised by the data subject [56]. Thus, the GDPR does not guarantee transparent and accurate automated decision-making and there is no legally binding right to an explanation in this context.

IX. DATA PROTECTION BY DESIGN VERSUS DEFAULT

Article 25 of the GDPR provides new obligations under the title of "Data Protection by Design[57] and by Default".[58] This obligation requires the data controller to build in data protection functionality in his system. It has been suggested that the issue of 'Data Protection by Design and by Default"

may become a real game-changer if implemented by the data controller, processor, producer, and the supervising authority. However, it would not be an easy task for all stakeholders to benefit from this right as it would require in-depth knowledge and resources, and access to state-of-the-art technology, unless researchers, practitioners and supervisory authorities collaborate with each for a meaningful implementation of the said right.[59]

X. DATA CONTROLLER AND PROCESSOR HAVE BEEN MADE MORE ACCOUNTABLE

The GDPR has also introduced the novel concept of Data Protection Impact Assessment (DPIA).[60] When the data processing based on the use of new technology is likely to result in a high risk to the right and freedom of a natural person, the data controller is obligated to carry out an impact assessment.[61] The Regulation prescribes the minimum elements that should be considered for the DPIA, that is, a description of the processing operation, an assessment of the necessity and proportionality of processing with reference to the purpose of assessment of risk to the right of the data subjects, the remedial measures taken, and freedoms and safeguards.[62] The data controller must consult the supervising authority before processing the data wherever the DPIA points to a high risk to the processing of data. The supervisory authority has been given the power to impose limitations including banning the processing of data.[63] The data protection [4]("Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 " 2016) authority can also impose a fine up to a maximum of 2 crore Euros, or in the case of business, 4 per cent of the total business turnover, whichever is higher.[64]

XI. THE EXTRA-TERRITORIAL SCOPE OF APPLICATION

Article 31 of the GDPR mentions that the scope of territorial application of the Directive covers the process of accessing of personal data in the context of activities leading to the establishment of a controller or a processor in the EU, regardless of whether the processing of data has taken place or not. Thus, independent obligations have been implemented on the person responsible for processing the data. The GDPR may also apply to a controller or processor of data who is not established in the EU under certain conditions having wide ramifications.[65] This would potentially mean that many companies incorporated outside the EU but targeting the EU market would be brought to book.[66]

XII. CONCLUSION

The issue of protection of the privacy of an individual is always considered as a fundamental right in the EU, and is the hallmark of the data protection framework. The advent of technology and movement of data to a cloud across geographical barriers, and outsourcing of data processing jobs to countries outside the EU have made the data protection directive of 1995 a little redundant in terms of its ability to overcome practical difficulties and judicial enactments. The GDPR has, therefore, been enacted to provide better privacy protection to individuals. It has also been demonstrated that though the basic principle and guidelines of the Data Protection Directive and GDPR are generically similar, the inclusion of some new provisions in the GDPR regulations provides for a better protection of the privacy rights of individual data subjects. Some of the provisions of the new Directive that signify better protection of the right of individual subjects include the choice of 'regulation' as an instrument of law for better harmonisation, expansion of scope of the 'right to be forgotten' in the case of personal data, improved control of users over their personal data, better legitimisation of the role of consent in data processing, data protection by design and default, increased accountability of data controllers for their actions, and the extra-territorial scope of application of the provisiosn of the Directive. However, some provisions like Article 22 of GDPR need to be clarified before GDPR is implemented the next year in order to avoid their conflicting dual interpretation. It remains to be seen how the GDPR is actually implemented and what its impact would be when it come into force in 2018.

XIII. REFERENCES

[1] M. M. Group. (2015, 24.11.2015). World Internet Users Statistics and 2015 World Population Stats. Available: http://www.internetworldstats.com/stats.htm

[2] S. R. Salbu, "European Union Data Privacy Directive and International Relations, The," Vand. J. Transnat'l L., vol. 35, p. 655, 2002.

[3] J. Kang, "Information privacy in cyberspace transactions," Stanford Law Review, pp. 1193-1294, 1998.

[4] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050 (Accessed at: http://www.refworld.org/docid/3ddcc1c74.html on 14 November 2016), 1995.

[5] ibid.

[6] M. Burri and R. Schär, "The Reform of the EU Data Protection Framework," Journal of Information, vol. 6, 2016.

[7] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 2016.

[8] D. R. Nijhawan, "Emperor Has No Clothes: A Critique of Applying the European Union Approach to Privacy Regulation in the United States, The," Vand. L. Rev., vol. 56, p. 939, 2003.

[9] J. R. Reidenberg, "E-commerce and trans-atlantic privacy," Hous. L. Rev., vol. 38, p. 717, 2001.

[10] D. Zwick and N. Dholakia, "Contrasting European and American approaches to privacy in electronic markets: property right versus civil right," Electronic Markets, vol. 11, pp. 116-120, 2001.

[11] M. Boban, "DIGITAL SINGLE MARKET AND EU DATA PROTECTION REFORM WITH REGARD TO THE

PROCESSING OF PERSONAL DATA AS THE CHALLENGE OF THE MODERN WORLD," in Economic and Social Development (Book of Proceedings), 16th International Scientific Conference on Economic and Social, 2016, p. 191.
[12] G. Shaffer, "Globalization and social protection: the impact of EU and international rules in the ratcheting up of US data privacy standards," Yale Journal of International Law, vol. 25, pp. 1-88, 2000.
[13] S. Singleton, "Balancing a Right to be Forgotten with a Right to Freedom of Expression in the Wake of Google Spain v. AEPD," Ga. J. Int'l & Comp. L., vol. 44, pp. 165-195, 2015.
[14] A. Bunn, "The curious case of the right to be forgotten," Computer Law & Security Review, vol. 31, pp. 336-350, 6// 2015.
[15] C. Rees and D. Heywood, "The ?right to be forgotten? or the ?principle that has been remembered?," ibid.vol. 30, pp. 574-578, 10// 2014.
[16] "Maximillian Schrems v Data Protection Commissioner, C-362/14, Court of Justice of the European Union," ed: Court of Justice of the European Union 2015.
[17] M. A. Weiss and K. Archick, "US-EU Data Privacy: From Safe Harbor to Privacy Shield," Congressional Research Service, 2016.
[18] M. Burri and R. Schär, "The Reform of the EU Data Protection Framework," Journal of Information, vol. 6, 2016.
[19] P. de Hert and V. Papakonstantinou, "The new General Data Protection Regulation: Still a sound system for the protection of individuals?," Computer Law & Security Review, vol. 32, pp. 179-194, 2016.
[20] V. Reding, "The European data protection framework for the twenty-first century," International Data Privacy Law, p. ips015, 2012.
[21] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050 (Accessed at: http://www.refworld.org/docid/3ddcc1c74.html on 14 November 2016), 1995.
[22] Article 29 Working Party Opinion 4/2007
[23] Regulation (EU) 2016/679, 2016. Recital 23
[24] ibid. Article 43 (b)
[25] ibid. Article 23
[26] ibid. Article 23a
[27] ibid. Article 9
[28] ibid. Article 23
[29] ibid. Article 17 (1)
[30] ibid. Article 17 (3) Recital 65
[31] ibid. Article 17 (2) Recital 66 & 67
[32] A. Mantelero, "The EU Proposal for a General Data Protection Regulation and the roots of the ?right to be forgotten?," Computer Law & Security Review, vol. 29, pp. 229-235, 6// 2013.
[33] Regulation (EU) 2016/679, 2016. Article 12
[34] ibid. Article 13, 14, 15, 19
[35] ibid. Article 20
[36] ibid. Article 21, 22
[37] ibid. Article 22 (2)
[38] ibid. Article 21
[39] M. Burri and R. Schär, "The Reform of the EU Data Protection Framework," Journal of Information, vol. 6, 2016.
[40] Regulation (EU) 2016/679, 2016.
[41] A. Cormack, "Is the Subject Access Right Now Too Great a Threat to Privacy," Eur. Data Prot. L. Rev., vol. 2, p. 15, 2016.
[42] ibid.
[43] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data Official Journal L 281 , 23/11/1995 P. 0031 – 0050 (Accessed at: http://www.refworld.org/docid/3ddcc1c74.html on 14 November 2016), 1995.Article 2H
[44] ibid. Article 7 (a)
[45] Regulation (EU) 2016/679, 2016. Article 7 (1)
[46] ibid. Article 4 (4)
[47] ibid. Article 8 (1)
[48] ibid. Article 8 (2)
[49] E. Carolan, "The continuing problems with online consent under the EU's emerging data protection principles," Computer Law & Security Review, vol. 32, pp. 462-473, 2016.
[50] Regulation (EU) 2016/679, 2016. Article 7(3)
[51] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," 2016.
[52] ibid.
[53] Regulation (EU) 2016/679, 2016. Article 20 (3) read with Recital 71
[54] ibid. Article 13, 14 read with Recital 60, 61, 62
[55] ibid. Article 15 read with Recital 63
[56] S. Wachter, B. Mittelstadt, and L. Floridi, "Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation," 2016.
[57] Regulation (EU) 2016/679, 2016. Article 25(1)
[58] ibid. Article 25(2)
[59] E. Hanson, "The History of Digital Desire, vol. 1: An introduction," South Atlantic Quarterly, vol. 110, pp. 583-599, 2011.
[60] Regulation (EU) 2016/679, 2016. Article 33
[61] ibid. Article 35
[62] ibid. Article 35(7)
[63] ibid. Article 58
[64] ibid. Article 83, 85, 86
[65] ibid. Article 3(2)
[66] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) OJ L 119, 4.5.2016, p. 1–88 2016. Recital 23