Summer 9-11-2019

Towards Standard Information Privacy, Innovations of the new General Data Protection Regulation

Ali ALibeigi
University of Malaya, alibeigi_a_80@yahoo.com

Abu Bakar Munir
University of Malaya, abmunir@um.edu.my

MD Ershadulkarim
University of Malaya, ershadulkarim@um.edu.my

Adeleh Asemi
University of Malaya, adeleh@um.edu.my

Towards Standard Information Privacy, Innovations of the new General Data Protection Regulation

Ali Alibeigi[*a,b], Abu Bakar Munir[a], Md Ershadul Karim[a], Adeleh Asemi[c,d]

[a] Faculty of Law, University of Malaya, Malaysia
[b] Department of Law, Faculty of Law and Humanities, Isfahan (Khorsagan) branch, Islamic Azad University, Isfahan, Iran
[c] Department of Software Engineering, University of Malaya, Malaysia
[d] Department of Computer Engineering and IT, Safahan Institute of Higher Education, Isfahan, Iran

Abstract

Protection of personal data in recent decades became more crucial affecting by emergence of the new technologies especially computer, internet, information and communications technology. However, Europeans felt this necessity at time and provided for up-to-date and supportive laws. The General Data Protection Regulation (GDPR) is the latest legislation in EU to protect personal data of individuals based on the recent technological advancements. However, its' domestic and international output still is debatable. This doctrinal legal study by using descriptive methods, aimed to evaluate the GDPR through analyzing and interpreting its' provisions by especial focus on its' innovations. The results show that the GDPR is much developed in comparison with previous personal data protection documents and will be a referred reference for the rest of the world in the near future.

Keywords: Compliance, GDPR, Privacy, Personal data protection, Right to be forgotten, Harmonization.

1. Introduction

"Data Protection" as a sub-category of the right to privacy, is a set of rules and principles aims to protect the privacy of individuals through safeguarding the use of personal information. In fact, personal data protection law is about individual's right to control his/her information.[1] European Union[2] is one of the pioneers in recognizing and protecting personal information of individuals which is

***Corresponding Author:** Jalan Universiti, 50603 Kuala Lumpur, University of Malaya, email: alibeigi_a_80@yahoo.com, alibeigi@siswa.um.edu.my

[1] Munir, A. B. and S. H. M. Yasin (2010). Personal Data Protection in Malaysia, Law and Practice. Malaysia, Sweet & Maxwell, at 4.

[2] The European Union including 28 members is one of the advanced regions with respect to the science and technology and economy. EU allocated 6.7% (9,938,000 Sq. Km) of total land area on the earth, and 10% (738 million) of the world population (7.3 billion), as of 2015. See: http://www.enchantedlearning.com/geography/continents/Land.shtml;http://esa.un.org/unpd/wpp/publications/files/key_findings_wpp_2015.pdf.

regarded as the European invention.[3] It seems that privacy became crucial in the EU affecting by the emergence of new technologies especially computer, internet and also the Single Market Program.[4] According to Viviane Reding,[5] the data protection laws of the EU will protect 'every person' in Europe, all citizens and non-citizens without discrimination.[6] She added that "I want to make sure that this right is promoted in all our actions".[7] There are many Conventions, Directives and Guidelines in place concerning the protection of personal data throughout the EU.[8] However, modern technologies, globalization of data flow and accesses to personal data by law enforcement authorities were pointed out as the main challenges of data protection by the EU Commission.[9] These challenges urged the need of an adequate assessment of the current data protection regime in the Europe. Study of the Commission during 2009-10 along with public consultation have indicated the validity of the present general principles of EU legislations, but the need for a comprehensive, integrated and harmonized mechanism to protect individuals' information in line with new technologies was evident.[10]

The European Commission, Parliament and Council provided a data protection proposal on 25 January 2012. The Directive 95 is replaced by this new Regulation under Recital 171.[11] The proposal named the 'General Data Protection Regulation' (GDPR) to be binding upon all EU member states unlike the Directive 95. GDPR was approved by the Committee for the Civil Liberties, Justice and Home Affairs (LIBE) of the Members of European Parliament (MEPs). They have voted by 49-1 and 3 abstentions in favor of the Regulations.[12] Finally, the GDPR Bill

---

[3] Kuner, C. (2009). An international legal framework for data protection: Issues and prospects. Computer Law & Security Review, 25(4), at 309.

[4] Single Market Program refers to the EU as one territory without any internal borders or other regulatory obstacles to the free movement of goods and services. The Single European Act (SEA) 1992 was developed to support this scheme. The details are available at: https://ec.europa.eu/growth/single-market_en

[5] The former Vice-President of the Commission and Commissioner for Justice, Fundamental Rights and Citizenship.

[6] Reding, V. (2011). The upcoming data protection reform for the European Union. International Data Privacy Law, 1(1), at 3.

[7] Ibid.

[8] For instances The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108 or EoC), was the first collective attempt in the world to protect individuals' personal data while processing automatically. Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data (Directive 95) was the second major attempt in 1995.

[9] Reding, above n 6, at 3.

[10] Ibid, at 4.

[11] Recital 171 of the GDPR provides that: "Directive 95/46/EC should be repealed by this Regulation".

[12] S. Zeballos, G., A. Sherer, J., & M. Pate, A. (2013, December 30). International privacy - 2013 year in review - European Union. Retrieved April 7, 2017, from http://www.lexology.com/library/detail.aspx?g=22d51700-a8f0-4160-822f-92da316e3c51.

was adopted by the EU Council on 8 April 2016, adopted by the European Parliament on 14 April 2016, and was published by the EU Official Journal on 4 May 2016.[13] The text has been provided in official languages. It came into force on 24 May 2016, and was implemented by the members on 25 May 2018.[14] Hence, two years opportunity were given for the governments and private companies to provide necessary requirements to comply with the Regulation. However, there is a fundamental question as whether the GDPR can address the new and emerging privacy challenges at the beginning of the 21st century?

GDPR is the most latest and up-to-date document based on the technological advancements and is called as an exporting data protection rules. Hence, the study of its innovations would have the following benefits:

1. "GDPR is interesting because it is the first time that the EU is exporting regulation. In the past, everything created by the EU applied to the EU. Now we have this regulation, but it is going to apply globally. If anybody wants to use the data of EU citizens or consumers, they have to comply, so it is exporting privacy rules to other countries" said Rashmi Knowles, chief technology officer, RSA Security.[15]
2. Since the present data protection laws around the world were drafted many years back, the GDPR innovations would be a suitable reference for either future amendments of the Acts or issuance of the Orders by the commissioners.
3. There are many foreign companies/organizations have branches, offices in the UE or have websites targeting EU customers. Maybe there are businesses that track the EU individuals through internet to analyze the customers' behaviors. Hence, the study of the GDPR would be important for future of these companies especially the ICT industry.
4. Most of the present laws were drafted based on the Europeans' personal data protection regime. Hence, the study of their latest advancements, is significant from judicial and academic point of view.

2. Objectives of GDPR

Article 1 of the GDPR on Subject-matter and objectives has stated its 3 main objectives:

[13] For more information visit: http://www.eugdpr.org/eugdpr.org.html

[14] Article 99 states: "1.This Regulation shall enter into force on the twentieth day following that of its publication in the Official Journal of the European Union. 2. It shall apply from 25 May 2018". 4.5.2016 L 119/87 Official Journal of the European Union EN.

[15] Benady, D. (2018, May 31). GDPR: Europe is taking the lead in data protection. Retrieved October 5, 2018, from https://www.raconteur.net/hr/gdpr-europe-lead-data-protection

- to protect individuals' information while being processed;
- to protect information privacy right of individuals; and
- to protect free movement of personal information within the boundaries of EU.

Under Article 1, the GDPR protects natural persons (individuals). It tries to overcome the defects and silent features of the Directive 95 affected by the new technological advancements. In fact, it aims to harmonize personal data protection laws of the EU members. GDPR annuls the EU members' domestic legislations on personal data protection by providing a regional legal regime which is directly binding on all member states. Eventually, there will be one harmonized law to be implemented by all states and no need for any further national enactment. The need for free flow of information within boundaries of the EU while safeguarding the individuals' privacy right was another motivation for the so called Regulation.[16] Moreover, the need to modify the present laws of data protection with respect to police cooperation and judicial cooperation in criminal issues to be consistent and uniform, was another motivating force.[17]

3. Scope of GDPR

Article 2 and 3 of the GDPR set out the material scope and territorial scope of the Regulation. It applies to processing of personal data by automated means or through filing system. Controllers and processors that are established in one of the EU member states with one main establishment will be subject to the GDPR.[18] It applies to processing of personal data either inside the Union or outside. Sending anonymous data outside the EU to any country is permitted under the current data protection regime.[19] However, if a controller or processor who is based outside of the Union, but offers goods and services inside the Union or monitors the behavior of UE citizens, regardless of using equipment in the union or not, then the GDPR applies to them under Article 3(2).[20]

[16] Reding, above n 6, at 4.

[17] Ibid, at 5.

[18] Article 3 of the GDPR on territorial scope.

[19] Dowling Jr, D. C. (2009). International Data Protection and Privacy Law. White & Case, at 11.

[20] Article 3(2) provides that: "2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union".

For instance, setting of cookies is behavioral monitoring.[21] Therefore, geographical scope of the GDPR is the controllers and processors established within the EEA, or are established outside but process the EU citizens' information. Hence, it can be deducted that this document reserved an extraterritorial jurisdiction for its application and in fact, the scope of Regulation has been broadened in compare with the Directive 95. Under the current regime, the establishment is a criterion for the jurisdiction. Unlike Directive 95, the GDPR is a single regional binding document for all member states to be observed.

4. GDPR Overview

With respect to the text quantity, GDPR encompasses a preamble with 173 recitals and 11 chapters including 99 Articles, which is much larger than the Directive 95.[22] Regulation is supported as being strong protection for individuals' personal information and at the same time allows companies to innovate while accountable for privacy standards.[23] It speaks about personal data, sensitive data and pseudonymous data.[24]

Personal data defined under Article 4(1) as "*means any information relating to an identified or identifiable natural person"*.[25] Personal data under the regulation is widened by including IP address and cookies.[26] Although the regulation did not define the sensitive data directly, however it specifies only 3 specific types of data,[27] namely genetic data, biometric data and data concerning health.[28] Furthermore, Article 9 has numerated special categories of personal data to

[21] They can track online behavior of the users, provide their behavior profile and then analyze to find the results like their market interests.

[22] The official text of the GDPR is accessible at: http://data.consilium.europa.eu/doc/document/ST-5419-2016-INIT/en/pdf

[23] Cullen, P., & Gonié, J. (2012). 1995–2012: from a directive to a regulation, the Microsoft perspective. International Data Privacy Law, 2(3), at 117.

[24] Article 4(5) provides that: "'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information…".

[25] Article 4(1) states that: "personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

[26] Tankard, C. (2016). What the GDPR means for businesses. Network Security, 2016(6), at 5.

[27] Under Article 4(13), (14) and (15).

[28] Article 4 interprets that: "'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question"; "'biometric data' means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data";

be prohibited for any processing unless based on specific conditions like explicit consent. These special types of data are as follows: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, health data, sex life data or sexual orientation.[29] The debate here is that the common data may be processed to divulge sensitive data like the meal preferences, which may denote the religion or race of an individual.[30] Unlike Directive 95, GDPR addressed the data controller and data processor directly.

Controller is a legal or natural person who processes the personal data under certain purposes, and processor also as a legal or natural person, processes personal information on behalf of the data controller.[31] Regulation purposely defines and set out the duties and responsibilities of the controller and processor distinctively, of course the controller have more responsibilities.

Processor works under a legal contract and controller is responsible to ensure that the processor comply with the contract terms. A good example for processor is the cloud industry. Consent must be "freely given, specific, informed and unambiguous".[32] These requirements are quite strict and were purposefully worded.[33] However, explicit consent is required for processing of certain information like health data, political opinions or religious beliefs under Article 9(1) or data transfer to a third country under Article 49-1(a).

Data controllers must obtain parental consent if they want to process the child's data aged less than 16 years old.[34] The discretion is given to the states to reduce this to 13 years old.[35] The

---

and "'data concerning health' means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status".

[29] Article 9(1) of the GDPR.

[30] de Hert, P., & Papakonstantinou, V. (2016). The new General Data Protection Regulation: Still a sound system for the protection of individuals? Computer Law & Security Review, 32(2), at 183.

[31] GDPR defines 'controller' and 'processor' under Article 4(7) and (8).

[32] Article 4(11) of the GDPR explains that: "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".

[33] Consent has been addressed by the GDPR under Recitals 32, 33, 38, 42, 43, 51, 54, 71, 111 and Articles 4, 8, 9-2(a), 22-2(c) and 49-1(a) which denotes the importance of this requirement.

[34] Article 8(1) of the GDPR.

[35] Ibid.

parental consent is a new conversion under the GDPR since the children are vulnerable in comparison with adults.[36]

Notice to data subjects for processing should be fair, lawful, complete and transparent. GDPR has developed a set of standards to be observed by controllers upon starting the data collection.[37] GDPR clearly provided the requirements for processing. Article 5 on processing of personal data provided certain principles like lawfulness, fairness, purpose limitation, adequacy or data minimization, accuracy, storage limitation, security, integrity and confidentiality. Article 6(1) similar to Article 7 of the Directive 95 provides for the conditions of a lawful processing. A lawful processing may occur by obtaining the consent for the determined purposes, processing under a contract, based on a legal obligation, to protect vital interests of individual, performing a duty that asked by official authority and processing based on the legitimate interests followed by controller or third party.[38] In fact, this Article has provided the exceptions to the general rule of 'individual's consent'.

Article 32 on security of personal data provided for "pseudonymisation and encryption of personal data" to keep the data in such a way that the data subject cannot be identified. Under Article 5-1(f) on integrity and confidentiality, controller and processor must provide necessary measures to secure personal data against unlawful processing, accidental loss, destruction and damages. The issue of security safeguards is addressed by the Regulation with special concern.[39]

The data transfer abroad is still restricted unless the data subject has granted his explicit consent. The data can be transferred to the countries with adequate data protection laws. The organization who sends the data also must equipped with appropriate safeguards.[40] However, the companies still can apply the EU Commission Model Clauses and binding corporate rules as well.[41]

---

[36] Under the current system, children are treated as same as adults.

[37] Under Recitals 39, 42, 58 and Articles 13 and 14.

[38] Article 6(1) of the GDPR on Lawfulness of Processing.

[39] Recitals 39, 49, 81, 83 and 94.

[40] Ryz, L., & Grest, L. (2016). A new era in data protection. Computer Fraud & Security, 2016(3), at 19.

[41] Ibid.

5. GDPR Innovations

GDPR seeks a greater protection for individuals' information privacy and a safer data flow environment. GDPR proposed many changes to the current information privacy regime, however, the outstanding innovation of the GDPR is the recognition of certain rights for data subjects. These innovations are adopted in line with the recent technological advancements.

A) European Data Protection Board

European Data Protection Board (EDPB or Board),[42] comprising of all supervisory authorities of the member states with a legal personality, will establish as a higher supervisory authority throughout the Union.[43] In fact, it will supervise and ensure the cooperation and consistency between all national supervisory authorities. The Board will replace by the Working Party under Article 29 of the Directive 95.[44] Basically the decisions of the Board are binding but are subject to the ECJ decisions.[45] The Board shall communicate with the Commission on its activities.[46]

National Supervisory Authority or information commissioner's office, must establish in each state.[47] The states may appoint more than one supervisory authority.[48] Basically the main functions of the supervising authorities are to enforce the Regulation, to monitor and assess the data controllers and processors, to promote public and private awareness and advising as well.[49] Under Directive 95, the supervisory authorities only monitor the data controllers; hence a significant progress has been achieved by the GDPR. Basically, a supervisory authority must monitor each data controller or processor.[50]

---

[42] Section 3 on European data protection board including Articles 68 to 76 have extensively explained the functions, members, independence, procedures and reports of the Board.

[43] Under Article 68 of the GDPR.

[44] Recital 139 of the GDPR.

[45] ECJ is the higher judicial authority of the EU and its decisions are final.

[46] Article 68(5) of the GDPR.

[47] Article 4(21) of the GDPR: "'supervisory authority' means an independent public authority which is established by a Member State pursuant to Article 51".

[48] Under Recitals 117 and 119 of the GDPR.

[49] Article 57(3) provides that all tasks of the supervisory authorities are free of charge for the data subjects and where applicable for the data protection officers as well.

[50] GDPR has allocated Recitals 117 to 135 and Chapter 5 on 'independent supervisory authorities' including Articles 51 to 59 to address the establishment process, members, independence, functions, powers and competence of supervisory authorities.

To determine the competent supervisory authority, Recital 36 provides a criterion as 'main establishment' of the controller which is the place where the central administration is located.[51] If a company has many branches in different countries, or is established in one country but process the individuals' information of other EU states, the company can select a lead supervisory authority to deal with.[52] Logically it will be easy for them to select the Commissioner of the country where they are headquartered. This is another new rule provided by the Regulation in order to prevent future conflicts. During the 2 year opportunity up to its implementation, perhaps the main duty of the privacy commissioners' community around the EU were providing the awareness to all private and public to understand what actually the Regulation intents to execute and what are its benefits.

B) One Stop Shop

There is a practical challenge for supervising the large companies with many subsidiaries and branches throughout the Union. Since there are may be different requirements and procedures applicable by each National Supervisory Authority, the GDPR allows working with one supervisory authority. The term 'one-stop-shop' as a new innovation, denotes the jurisdiction of one lead supervisory authority over an organization with many subsidiaries.[53] The reason behind this new criterion was to reduce the costs and make the processes faster only through a notification to be submitted to the supervisory authorities.[54] However, there is a legal debate on the issue of lead supervisory authority in practice as if an organization selects its lead supervisory authority in A country, however is engaged with processing of personal data of the individuals in B country in country C, in case of any data breach or auditing, the B and C supervisory authorities will not consider any right for themselves over the issue? Moreover, the controllers and processors who are established outside the EU but process the personal data of EU citizens, will be monitored by the regulator of each member state wherein they offer goods and services or processes the data.

---

[51] Recital 36 of the GDPR states that: "The main establishment of a controller in the Union should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union, in which case that other establishment should be considered to be the main establishment…".

[52] Under Recital 36 and Article 56 of the GDPR.

[53] The term has been addressed in Recitals 127 and 128 of the Regulation.

[54] Tankard, above n 26, at 6.

C) Data Breach Notification

Another considerable innovation under the GDPR is the data breach notification which is not compulsory under the Directive 95.[55] Basically, data breach notification is mandatory in case of any fault with respect to personal data and the company must report it to the supervisory authority and also to the data subjects.

Article 4(12) defines the term 'personal data breach' as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed". The necessity of data breach notification is specified under Recital 85 of the GDPR. It states that the breach notification tries to prevent physical, material and non-material damages to the individuals like loss of control, restriction of rights, identity theft, fraud, financial damages, discrimination, unauthorized reversal of pseudonymisation, harm to reputation, loss of confidentiality of information, or any other significant economic or social disadvantages.

If the breach causes a risk to the rights and freedoms of citizens, then the data controller must provide the description of breach and notify the supervisory authority without undue delay and within 72 hours under Article 33. In cases that the breach is unlikely to cause a risk to the rights and freedoms of data subjects, Article 33 will not apply. GDPR kept silent to define the term 'undue delay', perhaps the Board will provide a clarification for this ambiguous phrase. Moreover, the debate arises for instance with respect to the cloud companies in case of breach, as what kind of data they shall provide for breach notification? They may claim that we didnt know what are the content of data and we just store the information. Data controller must communicate with the data subjects in case of data breach if it causes a high risk to the rights and freedoms of the data subject under Article 34 of the GDPR.[56] The requirement for data breach notification is in line with the *principle of transparency*.

[55] Articles 4(12), 33, 34, 40-2(i), 58-2(e), 70-1 and Recitals 73, 85, 86, 87, 88 have been drafted to address the data breach notification.

[56] Article 34(1) provides that: "When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay".

Supervisory authorities can ask the data controller to inform individuals of a data breach incident, however, there are some exceptions.[57] The opposite sense of Article 34 is that while the breach is unlikely to result in a high risk, then the communication to the individuals is not necessary even if it merely cause a risk. Article 34 has provided for 3 exceptions for communication to the data subjects.[58] The phrase "breach is likely to result in a high risk to the rights and freedoms of natural persons" under Article 34 on the duty of controller to communicate a personal data breach to the data subject, did not explain by the Regulation and seems to be a vague assumption. What is high risk under Article 34 and what is risk under Article 33? High risks for example may relate to the health data or credit card information. However, the determination is vested to the decisions of organizations.

Supervisory authorities may force the company to notify individuals in case of the high risks.[59] With respect to data processor under Article 33, any data breaches with no exception caused by the data processor must merely notify to the data controller, without any delay since become aware of that breach incident. Eventually, the controller has to notify supervisory authority without undue delay within 72 hours or with delay based on reasonable justification and communicate with the data subjects under Article 34 as well.

D) Data Protection Officer

GDPR remarkably requires the controllers and processors including public authorities who processes a large scale of personal data and special categories of data and those who process the criminal convictions and offences data to appoint an independent 'data protection officer'.[60] This will enhance the level of compliance with the GDPR provisions through increasing the

[57] Article 34(4) states that: "If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met".

[58] Article 34(3) clarifies that: "…(a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise; (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner".

[59] Article 4(4) provides that: "If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met".

[60] Articles 4, 37 to 39 and Recital 97 of the GDPR are allocated to the data protection officer.

responsibility and accountability of data controllers and processors.[61] Data protection officer must be expert in data protection law and practices in line with the type of data are being processed by controller and he is the responsible person to monitor compliance with the GDPR. The controller must provide the contact details of data protection officer for data subjects.[62]

The advice of Data Protection Officer is required for automated processing, creating legal effects, profiling, in a situation affects individuals importantly, monitoring in a wide-ranging, and information on criminal offences or conviction, processing wide-ranging of sensitive data.

E) Rights to Access

GDPR like its predecessors has provided for the rights of data subjects. However, certain rights have developed and some are witnessed significant changes like consent, data portability and access right. One of the important right has been stipulated under the GDPR is the rights to access based on principle of transparency.

Although under the current regime the data subject is empowered with access request, however the GDPR has expanded this right.[63] Under this right, a data subject can ask the controller whether his/her information are being processed or not and other information like the purpose(s) of processing, categories of personal data, the identification of third parties the data may disclose to, the retention period, rectification of data, restrict or object the processing, to complain with the supervisory authority, the source of information if did not collect directly, operating through a decision-making and its consequences.[64] The report must provide in electronic form.[65] In case of an access request by the data subject, the Regulation has set out a one month period to respond the access request.[66] Remarkably, the access request shall be free of charge under Article 12(5) of the GDPR. Further copies may be charged under Article 15(3).

---

[61] Ryz, above n 40, at 18.

[62] Under Articles 13-1(b), 14-1(b) and 37(7) of the GDPR.

[63] Recital 63 states that: "…every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing…".

[64] Article 15 of the GDPR on 'Right of access by the data subject'.

[65] Articles 12(3) and 15(3) of the GDPR.

[66] Article 12(3) of the GDPR.

F) Accountability Principle

The phrase 'Accountability Principle' has been used under Recital 85 and Article 5(2), but the GDPR did not define it nor allocated special provision for this issue. However, the reference of Article 5(2) as accountability,[67] to paragraph 1 of this provision on principles with regard to the processing of personal data is the main reference of Accountability Principle envisaged by the Regulation. In a simple language, this new principle means compliance with all processing principles provided under Article 5 with special emphasis in addition to fulfilling all other required principles. Compliance with all required principles of the GDPR based on the accountability principles can be inferred from Recital 85 while addressing the data breach requirements.[68] Under accountability, the data controller must develop a comprehensive document including the detail information on what they do and how and generally on personal data they have. This is provided under the GDPR as a new requirement. This document will use for cases like data breach notification.

However, the data controller does not need to report regularly to the supervisory authorities, but they have to provide a comprehensive document containing the details of processed or processing personal information. In fact, it is a kind of record keeping obligation. Article 30 has provided the description of records of processing activities to be provided by the controllers. Albeit, the SMEs with less than 250 employees are exempted to provide such documentation unless they do risky activities under certain conditions.[69] Nevertheless, this exemption itself is subject to 4 exceptions as follows:

- processing may result in risk to the rights and freedoms of individuals;
- processing is not occasional;
- processing of special categories of data under Article 9(1); and
- processing of criminal convictions and offences data under Article 10.[70]

[67] Article 5(2) of the GDPR provides that: "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')".

[68] Recital 85 provides that: "…the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle…".

[69] This exemption has been addressed through Recital 13 and Article 30(5) of the GDPR.

[70] Article 30(5): "The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data

H) Privacy Policy

GDPR provides for certain privacy information to be communicated to the data subjects as their privacy rights which is the privacy policy. GDPR tried to overcome the challenges and debates of the current privacy policies by requiring the easy language and accessible privacy policy according to the principle of transparency.[71] Of course it would be regarded as a step forward, however, still the definition of simple language will remain unanswered under the Regulation. Recital 58 also emphasis on the concise, easily accessible, understandable and plain language privacy notices with special concern while addressing children under the principle of transparency.

G) Data Protection Impact Assessment

The Regulation required for data protection impact assessment or privacy impact assessment,[72] for certain categories of companies, like conducting systematic and extensive evaluation of personal behavior, processing sensitive data on a large scale, and systematic monitoring of publicly accessible areas. An example for monitoring publicly accessible areas is installing CCTV to monitor the traffic or security of a park. The example for "Systematic and extensive evaluation of personal behavior" is big data or cloud industry. Under Article 35, the data protection impact assessment is required when implementing new technologies and there is a high risk to the rights and freedoms of data subjects. Hence, the project must undergo an impact assessment prior to the processing. If it is concluded that the high risk may affect the individuals, then the controllers must notify the supervisory authority to review their operations.

Supervisory authority also must notify the high risk processing activities, hence those will be subject to the prior data protection impact assessment. The data protection impact assessment as a soft law mechanism is in fact the result of repealing the notification system and development of accountability principle.[73]

---

subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10".

[71] Recital 39 specifies that: "…The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used…".

[72] Conditions and obligations for impact assessment were provided under Recitals 84, 90, 91, 92, 94, 95 and Section 3 including Articles 35 and 36 of the Regulation.

[73] de Hert, above n 30, at 192.

I) Data Portability Right

Another development is the 'data portability right' which mostly will affect the social networks.[74] A data subject can ask the organization to transfer his 'electronic' data to another service provider. Two conditions must fulfill in order to request this right, firstly the consent was given for processing or processing based under a contract and secondly, the processing was done by automated means.[75]

J) Automated Decision-making

GDPR under Articles 21 and 22 has provided certain restrictions on automated decision-making of personal data. The automated decision-making would be restricted in case it has significant effects on data subjects. On the other hand, the data subjects have the right to oppose automated design-making except they have given explicit consent for processing or it applies under a contract.

K) Right to be Forgotten

CJEU held a remarkable decision in May 2014, which is called "Right to be forgotten". Mario Costeja Gonzales a Spanish lawyer complained against Google. An article was published by the La Vanguardia newspaper with regard to Gonzales' financial case in 1998. He approached the Spanish data protection agency to erase the link to that digitalized article since the problem was solved. The data protection agency concluded that the newspaper published that article legally, however the Google is responsible based on EU data protection regime.[76] Further, the case was brought before the Spain National High Court and subsequently to the CJEU. The CJEU held a landmark decision. The Court held that the eraser applications must consider as whether the present online information of an individual is relevant or not, inadequate or excessive based on the primary purposes of data collection. Furthermore, the search engines are regarded as a data controller and hence are responsible for erasure request.[77] This decision applies to European citizens only. However, there is an exemption to this general tight.

---

[74] Ibid, at 189.

[75] Recital 68 and Article 20 of the GDPR are allocated to describe this right.

[76] QC, F. G., & Berova, N. (2014). The rule of law online: Treating data like the sale of goods: Lessons for the internet from OECD and CISG and sacking Google as the regulator. Computer Law & Security Review, 30(5), at 473.

[77] Bartolini, C., & Siry, L. (2016). The right to be forgotten in the light of the consent of the data subject. Computer Law & Security Review, 32(2), at 231.

The public figures are excluded to enjoy this right since it conflicts with the right of citizens to know about the politicians and important persons.[78] Perhaps it is in line with the freedom of information and the right to know. It is also in line with transparency principle. However, the final decision to remove the content from the internet is handed over to Google. After this landmark decision, Google received many requests from individuals to erase their online information.[79] Under the current regime based on Directive 95, the retention period is required and the data users are not allowed to keep the data after the end of processing, or the data subject can withdraw his consent. The 'right to be forgotten' is a significant legislative development by the GDPR.[80] The whole idea of right to be forgotten is that the personal data must be deleted without undue delay, if no needs for further retention.

If the data is no longer needed, and also when the data subject withdraws his consent, the data must be deleted. Under the right to be forgotten, individuals have right to request the search engines to remove any link from their database which is directed to the individuals inaccurate, incomplete or irrelevant information or of those will invade their privacy. Therefore, the search engines are responsible for the content of the links they provide. However, Article 17 is criticized for its application under the following grounds: the controller maybe unable to contact all third parties, the third parties may claim their lawful processing and ambiguity on determination of third party controller responsible for internet bounce.[81] Although with respect to the territorial jurisdiction of the "right to be forgotten", Andrus Ansip, the EU vice president in charge of the digital single market argued that the delisting application of information from Google's search engine by EU citizens should apply around the world not only within the EU.[82]

L) GDPR Sanctions

Chapter 8 of the GDPR is allocated to the issues of remedy, liability and penalties. Individuals have right to complain to the supervisory authority of their place of residence, work or place of the alleged violation.[83] The outcome must announce to the complainant within three months.[84] If

---

[78] Ibid.

[79] Google received 41000 requests within one month. See: QC, above n 76, at 474.

[80] Recitals 65, 66 and Article 17.

[81] Bartolini, above n 77, at 229.

[82] Meyer, D. (2015, February 12). EU privacy ruling should apply globally, says digital chief. Retrieved January 9, 2016, from https://gigaom.com/2015/02/12/eu-privacy-rulings-should-apply-globally-says-digital-chief/

[83] Article 77(1) of the GDPR.

the complainant is not satisfied, the Regulation has provided for an effective judicial remedy against the supervisory authority under Article 78.

The third alternative is the right to the effective judicial remedy against data controller or processor by the data subject in case his privacy has been infringed due to data processing.[85] This is applicable to both private and public data processors. The Regulation has considered the judicial jurisdiction to hear such complaints as:

- place (country) where the data controller or processor has the establishment
- place (state) where the data subject is habitually resided.

Right to compensation is provided under Article 82 of the GDPR for the data subjects who have suffered. The data controller and processor are responsible if did not comply with the requirements of Regulation. [86] This can proceed by the judiciary only. It seems that under Article 82, the data subject has been given discretion to either sue both controller and processor or one of them. Furthermore, Article 83 has provided for penalties in the form of administrative fines. The supervisory authorities are empowered to impose administrative fines in case of infringement of the Regulation. The fines are either €20 million or up to 4% of global annual turnover in the preceding financial year, the one which is greater shall apply.[87] The penalties for the non-compliance with the GDPR are very high.

6. GDPR Challenges

66% of the EU IT professional say that the GDPR is a financial burden since needs up-dating and new technologies.[88] With respect to the implementation of the GDPR by states, a question arises as whether is it easy to be executed? And in case the national data protection laws provided detail rules for a specific issue, but the GDPR did not provide specific rules, so whether

---

[84] Article 78(2) of the GDPR.

[85] Article 79 of the GDPR.

[86] Article 82(1) provides that: "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered".

[87] Under Article 83(5) of the GDPR.

[88] Ipstwich survey shows that this rate is 77% in UK, 66% in France and 61% in Germany. The investment is needed for encryption technologies as stated by 62% of respondents, analytic and reporting technologies 61%, perimeter security technologies by 53% and file sharing technologies by 42%. See: Rossi, B. (2015, September 29). 77% of UK businesses say EU's new data law is a financial burden . Retrieved February 7, 2016, from http://www.information-age.com/77-uk-businesses-say-eus-new-data-law-financial-burden-123460254/

it will hampers its execution? It seems that the most crucial issue with respect to the GDPR is the proper implementation. Hence, in this situation the Board plays a significant role in an effortless implementation. The difficulties with implementation and expenses may involve all companies, governments and individuals. However, it is the nature of every new phenomena and it is inevitable to precede these steps to cope with new technologies. The different interpretations of the Regulation like the age of consent for a child are another obstacle toward a fully harmonized law.[89] Furthermore, the GDPR new innovations like right to be forgotten or data breach notification will affect mostly the big multinational companies.

Blume believes that the Directive 95 and new Regulation texts are not easy to understand in many parts, while the domestic data protection legislations are more complicated.[90] He added that the Regulation is apropos and likely toward harmonization, but includes limitations.[91] He challenged the harmonization perspective of the Regulation as in practice the understanding of each state from the regulation and the decisions and actions may be different.[92] He challenged the Regulation on the ground that it is far to be a complete harmonized instrument throughout the EU.[93] He argued that the Regulation will reduce the level of data protection in some of EU members.[94] However, David Cameron the UK Prime Minister (at that time) stated that the regulation is "wrong" and we have to "hold it up so we get it right".[95]

7. Concluding Remarks

GDPR is about the rights and protection of personal information in the new information and communications age. Regulation is a significant reform happened on information privacy in

[89] Ryz, above n 40, at 18-19.

[90] Blume, P. (2012). Will it be a better world? The proposed EU Data Protection Regulation. International Data Privacy Law, 2(3), at 130.

[91] Ibid, at 133.

[92] Ibid. He construed the regulation as being impressive but also a legal monster.

[93] Ibid, at 130.

[94] He described this deficiency by providing an example from Danish Data Protection Act, Section 11. Under this provision, personal identity number (PIN) is specially protected. The data on PINs operates as sensitive data. The Regulation did not consider general identity number maybe because some of the members do not use it, however it will make problem in future and such information will be regarded as ordinary data. Hence, the regulation will reduce the level of protection in some EU members like Denmark. See: Blume, above n 90, at 132.

[95] S. Zeballos, above n 12.

Europe based on the recent technologies.[96] It can be concluded the GDPR aims to compel the data controllers and processor to develop a systematic, structured and strategic data privacy plan with proper responding policy, to re-designing the processing operations, to review privacy policies and contracts and to enhance their security mechanisms. Moreover, in near future, most of the large companies in the world will review their data protection regime in order to deal with the Europeans, perhaps before their respective countries. Europeans are the pioneers of the information privacy legislations. The EU approach is capable of being a proportional template for the new drafters of data protection laws, since EU has undergone a significant practice of trial and error.[97]

Acknowledgment

This research work has been funded by the University of Malaya Research Grant (UMRG), Project No: RP006C/13ICT. The authors would like to thank the University of Malaya for the financial support.

[96] "According to Ovum, 52% of organisations believe that the GDPR will result in fines for their business and 68% feel that it will dramatically increase the costs of doing business in Europe, with some believing that their budgets will need to increase by some 10% to deal with its ramifications over the next two years". See: Tankard, above n 26, at 6.

[97] Zhang, K. (2014). Incomplete Data Protection Law. German LJ, 15(6), at 1071.