International Journal of Law and Public Policy
p-ISSN: 2721-6934, e-ISSN: 2721-6942

Research Paper

The Practice of General Data Protection Regulations Fine and Penalty on Google Inc. vs CNIL Case

Rian Nugraha[1], Maskun[1]

[1] *Faculty of Law, Hasanuddin University. Indonesia.*

Article History
Received:
06.01.2020

Revised:
07.02.2020

Accepted:
23.03.2020

***Corresponding Author:**
Maskun
Email:
maskunmaskun31@gmail.com

Abstract: The development of technology on this era is bringing two side on the humanity which is the positive and negative side. On the positive side, the technology could help human to finding information easily from their device (e.g smartphone), while on the other side this techonology could bring harm on privacy side. There fore, with those harm, the concept of privacy is vital. On European Union where they have concern toward the personal data with General Data Protection Regulation (GDPR). On the GDPR, European Union have their own rule about the right of erasure, it also known as the right to be forgotten (RTBF) which written on Article 17. This article has it own problem due to the scope of application. On may 2015 the French Commission Nationale de l'informatique et libertés (CNIL) served a formal notice on google if individual asking about the remvoval of links to web page from the list of result displayed following a search performed on that individual name etc. Google have to apply that removal on all google domain (google.com) and not remove it just in the google local domain (google.fr). Due to the difference of perspective toward the Article 17 of General Data Protection Regulation, google wont remove it on the google main domain (google.com), and so on march 2016 (CNIL) found that google failed to comply the formal notice and imposed a penalty of €100.000 and so google sought to have the adjudication annulled. 11 September 2018, the European Court of Justice hearing this case where it is about the territorial scope of European data protection law. But then on 24 September 2019, Court of Justice held that the right to be forgotten on the article 17 doesn't require google to de-list search result on all of its domains, however google still required to de-list the result on the all of the European Union domain. The purpose of this study to analyze wether the court opinion and decision toward the google.inc v CNIL case. On other side it will also determine wether the European Union data protection law could be applied outside the European Union or not.

Keyword: CNIL, Data Protection, Right to be Forgotten.

1. Introduction

The development of technology has resulted the convergence on technology and communication, media and information developments. Each of these technologies seems to run separately from one another, but now all these technologies are increasingly integrated. The form of telematics convergence is marked by the birth of new technology products that integrate the capabilities of information systems and communication systems based on computer systems arranged in a network of electronic systems, both in local, regional and global scope [1].

More than 20 years ago, the European Community (now the EU) felt a need to align data protection standards within their Member States in order to facilitate EU-internal, cross-border data transfers. At that time, national data protection laws provided considerably different levels of protection and could not offer legal certainty—neither for individuals nor for data controllers and processors. In 1995, the European Community therefore adopted 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 (in short: the Data Protection Directive) in order to harmonise the protection of fundamental rights of individuals with regard to data processing activities and to ensure the free flow of personal data between EU Member States [2]. In 2016, the GDPR has been adopted to replace the Data Protection Directive from 1995. In contrast to the Data Protection Directive, the Regulation directly applies to its addressees—no further implementation measures by the EU Member States required. By equalising the rules for data protection, the GDPR shall lead to more legal certainty and remove potential obstacles to the free flow of personal data [2].

One issue that will have to be considered is the GDPR's "erasure" right. Article 17 of the GDPR demands that companies erase the personal data of individuals when they request to be "forgotten". The GDPR does not define what "erasure of data" means, which suggests that, to comply with this requirement, actual physical and logical deletion (a literal reading of the word "erase") is required [3]. With those issue, in May 2015 the French Comission Nationale de l'informatique et des libertés (CNIL) served a formal notice on Google. CNIL argue that the removal request on web pages result which display the person name, must be removed from all the search engine domain name extensions (.com domain). But google refused to comply that formal notice and only remove it on the local EU domain (.fr, .nl, etc.), furthermore, on March 2016 CNIL imposed a penalty of €100.000 to google, but google sought to have the adjudication annulled [4]. Both parties have a point. The CNIL rightly insists that the Right to be forgotten can only be effectively enforced if information is genuinely 'deleted' not just on European Union domains. At the same time, Google rightly pinpoints that an obligation to apply the Right to be Forgotten extraterritorially may compel firms to breach law elsewhere [5].

And so, on September 2019, The European Court of Justice held that the Right to be forgotten doesn't required a search engine to de-list the result on all of its domain. Howewer, a search engine still required to de-list the search result on the European Union member states domain. The ruling left the referring court, the Conseil d'État, to apply the Court's holding to Google practice in France. In deciding the case, the Court of Justice considered both of the Data Protection Directive 1995 and the General Data Protection Regulations 2016. The Court first eshtabilished that Google fell within the territorial scope of the DPD and the GDPR, given its activities in French territories. It then considered the goal of the relevant EU law: guaranteeing a "high level of protection of personal data throughout the European Union." Even so, the right to protection of personal data is not absolute and must be balanced against other fundamental rights and the public interest in having access to information [6]. Therefore, the aim of this research to analyze the European Court of Justice opinion and decision toward the case between Google v CNIL, also to analyze wether or not the European data protection law, especially the right to be forgotten could be applied outside the European Union.

2. Literature Review

2.1. The European Union Data Protection Law

Data protection law has a long history in Europe and the continent's political and cultural contexts, such as secret police surveillance in East Germany, help explain a long tradition of citizens and governments alike seeking to craft a status of noninterference in individuals' private lives; indeed, the first modern data protection laws in the world were passed in the early 1970s in Germany (Hesse Data Protection Act in 1970) and Sweden (Data Act in 1973). Unlike in countries such as the US or

Canada, where the starting presumption in law is that processing personal data is lawful unless it is expressly forbidden, in Europe, processing personal data is prohibited unless there is a lawful basis that permits it [7]. Data protection standards are becoming increasingly high, and companies face the more and more complex task to evaluate whether their data processing activities are legally compliant, especially in an international context. Data—by their very nature—can easily cross borders and play a key role in global digital economy [8].

2.1.1. The Europe Data Protection Directive 1995 (Directive 95/46/EC)

The right of privacy develops well enough on European Union which is why all member of state which also the signatories of European Convention on Human Right (ECHR) should follow the rule on ECHR. Article 8 of ECHR explain "*Everyone has the right to respect for his private and family life, his home and his correspondence*". But, on the Article, the interpretation from European Court of Human Rights (ECtHR) toward privacy very wide, so on 1980 in an attempt to make a comprehensive data protection system in the whole European, the Economic Co-Operation and Development (OECD) made the Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans Border Flows of Personal Data [9]. The Data Protection Directive was build with 7 principle from OECD and the Recommendation which is notice, purpose, consent, security, disclosure, access, and accountability. This principle isn't binding and the privacy law still can change depends on where the subject at on the European Union. From there, the European Comission aware that the data flow still blocked by the differences of the privacy law on the European Union member state. With Data Protection Directive, European Comission adopt the directive of OECD and some of the terms of data protection that bind the European Union member state [10].

At the end of 1990, it therefore submitted a proposal for a Directive in order to harmonise the national laws on data protection in the private and most parts of the public sector. After four years of negotiation, this resulted in the adoption of the current Directive 95/46/EC which has a double objective. Firstly, it requires all Member States to protect the fundamental rights and freedoms of natural persons, and in particular the right to privacy with respect to the processing of personal data, in accordance with the Directive. Secondly, it requires them neither to restrict, nor to prohibit the free flow of personal data between Member States for reasons connected with such protection. Both obligations are closely interrelated. They aimed to bring about an equivalent high level of protection in all Member States with a view to achieving a balanced development of the internal market [11]. But, the very rapidly fast development of technology on the digital era, bringing new challenge to the privacy & data protection law. People have tendency to make new information that is private. Also, the economic and social integration resulting from the functioning of the internal market has also led to a substantial increase in cross-border flows of data. To take full account of all these developments and promote the digital economy, there is a need to ensure a high level of protection of personal data, while at the same time allowing for the free movement of such data [12].

2.1.2. General Data Protection Regulation

On 25 January 2012 the European Commission proposed a comprehensive reform of the EU's 1995 data protection rules. The reasons behind this important initiative had earlier been set out by the European Commission. The Commission's proposals update and modernize well-known and proven general principles enshrined in the 1995 Data Protection Directive. The proposals are also characterized by a number of important changes and improvements [13]. Both proposals, for the Regulation and for the Directive, are based on Article 16 of the Treaty on the Functioning of the European Union (TFEU). This Article, introduced by the Lisbon Treaty, is the new legal basis for the adoption of comprehensive data protection rules. Article 16 (1) TFEU provides that 'everyone has the right to the protection of personal data concerning them'. Together with Article 8 (1) of the Charter of Fundamental Rights of the European Union ('the Charter'), 6 Article 16 (1) TFEU therefore guarantees the fundamental right to the protection of personal data applying to all Union policies [13].

Basically, there are three reason why the Data Protection Directive should be updated. The first reason is that there is a clear need to update the present framework, more specifically Directive 95/46/EC as its central element. The term 'updating' means in this case, most of all, ensuring its continued effectiveness in practice. The second reason is that the present framework has led to some degree of harmonisation, but also to increasing diversity and complexity, if only for the reason that a directive - according to its legal nature - must be transposed into national law and we now are

confronted with 28 sometimes very different versions of the same basic principles. That is obviously too diverse and results not only in unnecessary costs, but also in a loss of effectiveness. The third reason has to do with the new institutional framework of the EU. As we have seen, the Lisbon Treaty has placed a considerable emphasis on the protection of fundamental rights, and especially on the right to data protection [14]. The GDPR introduced benefits both for business and for citizens. Individuals, on the one hand, have been awarded new instruments—such as a right to be forgotten, easier access to one's data, a right to data portability, and a right to know when one's data has been hacked— enabling them to gain more control over their data. Data controllers, on the other hand, have been obliged to follow the principle of data protection by design and by default. An institutional novelty of the GDPR is that the newly established European Data Protection Board has been equipped with the competence to issue binding decisions in the case of disputes between national data protection authorities, in addition to that of issuing guidelines on the application of the GDPR. Last but not least—and probably the most commonly known novelty—is, that the GDPR contains clear rules on the conditions for imposing administrative fines on legal entities which do not comply with the new EU rules [15]. Although many Chinese and American companies are obligated to comply with GDPR, the EU companies are still the most affected in the field of emerging technologies since they mostly deal with personal data of EU residents. If the EU emerging technology industry cannot effectively solve the above-mentioned restrictions by means of significant technological upgrading, which seems to be unlikely in the short term or in other ways, the development and application of emerging technologies within the EU will slow down significantly. Many other relevant industries, such as credit cards, e-commerce, as well as intelligent manufacturing, which are supported by those emerging technologies, will also be significantly affected [16].

2.2. Privacy

Humans have always had a need for privacy. Although the way it is appreciated differs from culture to culture and from person to person. At the same time it is clear that a need for privacy can never be absolute and must be balanced against other needs, for example the need for fighting terrorism, criminality, and fraud. As we will then see, the discussion on privacy primarily is a political discussion about the way the distinct individual and societal interests can be balanced. In the most fundamental form, privacy is related to the most intimate aspects of being human. Throughout history privacy is related to the house, to family life, and to (personal) correspondence [17]. Some of definition on privacy according to the expert:

1. According to Brandeis and Warren Privacy is is the right to be left alone. Among other things, privacy means freedom from surveillance and unreasonable personal intrusions [18].
2. According to the Ministry of Information and Telecommunication of Republic of Indonesia No. 20 of 2016 about The Protection of Personal Data on Electronic System, on Article 2 (3), Privacy is a freedom of the personal data owner to declare the confidential or not to reveal the confidentiality of his personal data, unless otherwise stipulated in accordance with statutory provisions.

2.2.1. History of Privacy

The history of privacy begin from the protection of the residence, and continuously to the protection of information and communication. The law of privacy at first was known well in Europe and United States. At that time, the law has provide against the activities such as eavesdropping, and also protecting people houses from illegal activites [19]. Traditionally, privacy interests were implicit in legal or social protection of personal property and space, intimate settings, or personal effects.' But by the Twentieth century, scholars had distilled privacy into an independent concept-breathing life into one of the most discussed yet poorly understood areas of modem legal thought. The modem evolution of the privacy right is closely tied to the story of industrial-age technological development' from the telephone to flying machines. As each new technology allowed new intrusions into things intimate, the law reacted-slowly-in an attempt to protect the sphere of the private. Digital technology-computing, databases, the Internet, mobile communications, and the like-thus calls for further evolution of privacy rights, both conceptually and in law [20].

In 1950 the European Convention for the Protection of Human Rights and Fundamental Freedoms was drafted. Article 8 of the Convention is still one of the most important international agreements on the protection of privacy: "Everyone has the right to respect for his private and family life, his home

and his correspondence." At the same time the second paragraph of the article makes clear that this right to privacy is not absolute. Interference by a public authority is allowed when such is necessary in accordance with the law and is necessary in a democratic society in the interest of national security, public safety, and the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others. With this formulation three zones of privacy are defined, that is private and family life, home, and correspondence, although correspondence is very narrowly related to the secrecy of letters [21].

Privacy issues first appeared in some European countries in the 1970s, when countries started to process their citizens' data on a massive scale - which led to the first privacy laws. The demand for protection increased in the 1980s when private companies started gathering data about their customers. A common protection system was then implemented across Europe, followed by the EU Data Protection Directive in the 1990s (Directive 95/46/EC). Every European country had to adapt this set of rules to their national regulations. But as technology transformed the way personal data is handled substantially in the last twenty years, a review of the existing rules was needed. In 2016, the EU adopted the GDPR, which replaces the 1995 Data Protection Directive [22].

2.2.2. The Purpose of Privacy

According to Altman, there are 3 purposes of privacy [23]:

1. As a regulator and controller of interpersonal interaction which means the extent to which relationships with others are desired, when it's time to be alone and when it's time to be with other people desired.
2. As a plan and make strategies to connect with others, which include intimacy or distance in dealing with others.
3. Clarify people identity

2.3. The Right to be Forgotten

The right to be forgotten derives from the case Google Spain SL, Google Inc v Agencia Española de Protección de Datos, Mario Costeja González (2014). For the first time, the right to be forgotten is codified and to be found in the General Data Protection Regulation (GDPR) in addition to the right to erasure [24]. The right to be forgotten gained international attention in May 2014, when the European Court of Justice ruled that Google was obligated to recognize European citizens' data protection rights to address inadequate, irrelevant, or excessive personal information. The right to be forgotten is a legal concept that obligates others to obscure or delete personal digital information about another upon request of the data subject. Incorporating and developing such a right was explicitly stated as a goal of the European Commission when it declared intentions to update the 1995 European Union Data Protection Directive with the Data Protection Regulation, which would harmonize many of the national differences that had evolved under the Directive. The right to be forgotten was encoded in Article 17 of the 2012 draft Regulation and has since been retitled "the right to erasure" [25].

The right to be forgotten is addressed by Article 17 of the Regulation, a lengthy section, which defines the scope of this right, the exceptions to it, the entitlements of data subject and the corresponding obligations of controllers, and by Article 79, which provides sanctions for violations of this right. The scope of the right, however, also depends on other norms in the Regulation. In fact, since Article 17 addresses all cases when the continuation of a processing is unlawful, all norms specifying under what conditions a processing is, or may become, unlawful are potentially relevant [26]. GDPR also regulate about the exception for this right which is on Article 17 (3). According to which the controller is exempted from the obligation to erase the data to the extent that the processing is necessary for the sake of certain other rights and interests: (a) the exercise of freedom of expression, according to Article 80, (b) public health, according to Article 81, (c) historical, statistical, and scientific research, according to Article 83, and (d) compliance with legal obligations established by Union law or State law Article 80 authorizes Member States to limit data protection to enable processings carried out for the purpose of journalism and artistic and literary expression. This raises the issue of whether processings of personal data for the purpose of journalism and artistic and literary expression should be considered impermissible according to EU law, in the absence of an explicit permission from laws of member states [26].

3. Method

This research was conducted by doing a literature study, which the data was collected through library research. In addition to review the case, the source of the information used to review the case is from the books that is relevant to the case, and other literature like conventions, the expert research that relevant to this case, scientific journal and other media such as news that relevant to the case.

4. Analysis

4.1. Google as Multinational Company

Before jumping to the analysis of this research, we need to know that google is one of big company and one of a multinational company. Multinational company is a company which have their other office in many states. An example for that, Google headquarter at Mountain View, California, United States. But Google as multinational company have other office outside the United State, example on Europe, google have many office in the European Union member states, in Netherland, Germany, United Kingdom, Spain, Italy, and other country of EU member. The establishment of offices in several countries makes it easy for Google as a large company to solve every problem that occurs in a country related to Google. Not just a company that provide search engine, google also provide many services such as email, cloud storage, operating system for smartphone/tablet, maps, internet provider, etc.

On GDPR, there's two type of company which is controller and processor. Google stand as a Controller company. As a company that bind with the state, especially on this case bind with the GDPR, google must comply the data protection law. With that, google have provide the data subject with some mechanism if someone want to delete their data. Google also made the report so public could see it, which the page called Google Transparency Record. As 16 February 2020, there are 3.511.157 request for URL de-listing and 894,043 request for individual de-listing [27]. Those request were divided into categories such as social media, news, directory, miscellaneous, and other thing. According to the Transparency Report page, google have their own team that specially trained reviewers for this purpose, based primarily in Dublin, Ireland. Their team uses dedicated escalation paths to senior staff and attorneys at Google to adjudicate on difficult and challenging cases [28].

After the data subject submit the form that google provide for de-listing, google and the team will evaluate it first case by case. On certain case, google will need more information about the request, and also the reason behind. And then google decision toward the request will be informed to the user by email and google reason behind the decision. There is some reason that could make the request was denied by google. If the page contain some information that is for public, google will likely deny the request toward that page. If the data subject didn't accept the google decision, the subject could request for a judicial review for the request.

4.2. General Data Protection Regulation towards Company

The GDPR binding European citizen inside and outside the union, it also binding the companies that were established inside the European Union and outside the European Union as long as those companies processing the European Union citizen personal data. With GDPR, the company can't process the personal data without the data subject consent. Those rule was explained on Article 6(1) of GDPR "Processing shall be lawful only if and to the extent that at least one of the following applies: (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes".

According to Article 27 which related to Recital 80 of GDPR, any company that process the personal data of European Union Citizen either as controller or processor are asked to established a representative office in the union. The purpose behind the estabilishment to facilitate the company business if in the future there are some violation toward the use of European Union citizen personal data, example in the case of prosecution. And so with those rule, the company should adjust their old rule to match with the GDPR. Not just the company, the government agencies such as ministries must also adjust to the GDPR if they want to carry out personal data processing activities for European Union Citizen [29].

GDPR also regulate about Binding Corporation Rules, which is explained on Article 47. Binding corporate rules (BCR) are data protection policies adhered to by companies established in the EU for transfers of personal data outside the EU within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate

safeguards for data transfers. They must be legally binding and enforced by every member concerned of the group [30]. Binding Corporate Rule are therefore one of the appropriate safeguards for the transfer of personal data within a group of undertakings, or group of enterprises engaged in a joint economic activity ("Group") from the European Economic Area ("EEA") to countries which do not provide an adequate level of data protection. In practice, Binding Corporate Rule are a set of internal rules, standards and processes, such as codes of conduct, that regulate internal data management practices in a binding and consistent manner throughout the Group, with the primary objective to facilitate the free movement of personal data within that Group while ensuring an effective level of data protection [31].

4.3. Type of Infringements, Fine and Penalty on General Data Protection Regulation

There are two type of fine and penalty on GDPR, which is the low level and high level. Each of these levels has differences both in the area of the violation and in the amount of the fine. For lower level of infringements, the companies could be penalized with fine and penalty up to €10 million, or 2% of the worldwide annual revenue of the prior financial year, whichever is higher. It shall be issued for infringements of: Controllers and processors under Articles 8, 11, 25-39, 41(1), 42, 43, certification body under Articles 42, 43, and monitoring body under Article 41(4). While for higher level of infringements, the companies could be penalized up with fine and penalty up to €20 million, or 4% of the worldwide annual revenue of the prior financial year, whichever is higher? It shall be issued for infringements of: The basic principles for processing, including conditions for consent, under Articles 5, 6, 7, and 9 The data subjects' rights under Articles 12-22, the transfer of personal data to a recipient in a third country or an international organisation under Articles 44-49, any obligations pursuant to Member State law adopted under Chapter IX, and any non-compliance with an order by a supervisory authority [32].

These penalties are for a worst-case breach but they are punitive and they are meant to act as a deterrent. But on the bright side, the GDPR could prevent the companies to not act outside these rules. The fine and regulation might sound very strict, but with this regulation, the company which intentionally ignoring this regulation could get a fine that will hurt, and can cause so much damage toward the companies [33]. GDPR also regulate about compensation on Article 82(1) for those who suffer a material and non-material damage from the infringement of this regulation.

In order to determine the fine and penalty, fines are administered by individual member state supervisory authorities (according to Article 83(1)). There are 10 criteria to determine how big the fine is and penalty that the Supervisory Authorities could imposed to the company (Article 83(2)). Those criteria are the nature of infringement, intention, mitigation, preventative measures, history, cooperation, type of data, notification, certification, and other factor that may include financial impact to the infringements [34].

4.4. The Cases between Google and CNIL

The cases between Google and CNIL isn't just about the right to be forgotten, but there are many cases out there. But on this research, it will focused on the case of the right to be forgotten. On this case, back to 2015 CNIL have made a formal notice to google as data controller to de-list the data of a France citizen, but google refused the request, and so on 2016 CNIL as the Supervisory Authority giving fine to goole €100.000 but google seek for annulment to the Conseil toward the CNIL adjudication. Until on 2018 this case was brought to the court of justice. This case is about the extraterritoriality of the right to be forgotten.

On the Document of Court of Justice, Judgement of 24 September 2019, Case C-507/17, Google v Commission nationale de l'informatique et des libertés (CNIL), according to the paragraph 64 "*It follows that, currently, there is no obligation under EU law, for a search engine operator who grants a request for de-referencing made by a data subject, as the case may be, following an injunction from a supervisory or judicial authority of a Member State, to carry out such a de-referencing on all the versions of its search engine*". According to that consideration, Court of Justice stated that under European Union law, google and other search engine provider didn't have obligation to apply the right to be forgotten in global level. With those decision, it does explain that the right to be forgotten can only be applied inside the European Union. In the analysis toward this case, the court of justice consider both regulation which is the Data Protection Directive 1995 and General Data Protection. The decision is critical because, at first glance, it appears to have closed the door for EU residents to

demand a worldwide removal of their information, under certain circumstances, from search engine results under the GDPR regime. The Court, in this case, decided to set limits on the territorial scope of an individual's right to de-reference. In simple terms, this means that Google is only required to remove links to an individual's personal data from internet searches conducted within the Union [35].

A key part of the judgment appears to neutralise Google's purported victory in this case. Paragraph 72 of the judgment reveals the Court's effort to establish the lawfulness of global de-referencing. By finding that European Union law does not prohibit worldwide de-listing and that Member States remain competent to order search engine operators to dereference globally in certain circumstances, the Court leaves open the possibility for France's CNIL and other national Data Protection Authority to require global de-referencing in cases where they deem it necessary [35]. If only Google was an entirely European Union company then it is clear that data protection would have required it to achieve a fully global result in all cases. That this was not necessary here arose from Google having its seat in a third State. That goes to show that ultimately this case was primarily about public international law. In that regard, the Court's confirmation that the powerful impact of global communicative networks can trigger extra-territorial jurisdiction under the effects doctrine is of great significant [36].

5. Conclusion

Based on the result of study, several conclusion toward the cases can be drawn as follows:

1. According to the GDPR, google can be penalized for the infringement. But, due to the scope of territoriality of the right to be forgotten is just applied in the local domain such as google.fr, google.nl, etc. If Google applied the right to be forgotten in the whole domain, it could be raised a problem about the extraterritoriality of the law. With the judgement from the court, on this case, it doesn't prohibit for worldwide de-listing. The Court still open for the possibility for the National Data Protection Authority to require a global de-referencing in certain cases where it is necessary to do. Also, from the cases it could be conclude that the international law need to arrange a law that is related to the right to be forgotten that is binding to all of the signatories, so there will be a mechanism toward it about global de-referencing.
2. The GDPR work really well on protecting their citizen fundamental right. With GDPR, the European citizen personal data could be manageable by the data subject it self. The GDPR also make a transparency toward their own personal data on how the company process their data.

References

[1] M. Maskun, *Perkembangan Hukum Telematika: Prospek dan Tantangan.* 2017. [Online]. Available: https://www.researchgate.net/publication/318520006_Perkembangan_Hukum_TelematikaProspek_dan_Tantangan. [Accessed: October. 5, 2019].

[2] P. Voigt and A. V. D. Bussche, *The EU General Data Protection Regulation (GDPR).* Springer, Switzerland. pp. 1-2, 2017.

[3] N. Kramer, *"Blockchain, Personal Data and the GDPR Right to be forgotten"*, 2018. [Online]. Available: https://www. natlawreview.com/article/blockchain-personal-data-and-gdpr-right-to-be-forgotten. [Accessed: October. 6, 2019].

[4] The Society for Computers and Law. *"Google only has to remove de-referenced search results from searches made in the EU: Advocate General's Opinion in Case C-507/17 Google v CNIL",* 2019. [Online]. Available: https://www.scl.org/news/10393-google-only-has-to-remove-de-referenced-search-results-from-searches-made-in-the-eu-advocate-general-s-opinion-in-case-c-507-17-google-v-cnil. [Accessed: October. 5, 2019].

[5] M. Finck, *"Google v CNIL: Defining the Territorial Scope of European Data Protection Law",* 2018. [Online]. Available: https://www.law.ox.ac.uk/business-law-blog/blog/2018/11/google-v-cnil-defining-territorial-scope-european-data-protection-law. [Accessed: October. 5, 2019].

[6] S. Wong, *"Google v. CNIL: EU Rules that Right to be Forgotten Does Not Apply Globally"*, 2019. [Online]. Available: https://jolt.law.harvard.edu/digest/google-v-cnil-eu-rules-that-right-to-be-forgotten-does-not-apply globally. [Accessed: Desember. 9, 2019].

[7] E. S. Dove, "The EU General Data Protection Regulation: Implications for International Scientific Research in the Digital Era," *the Journal of Law, Medicine & Ethics*, vol. 46, no. 4, pp. 1014, 2018.

[8] P. Voigt and A. V. D. Bussche, *GDPR.* Springer, Switzerland, 2019.
[9] The Organization for Economic Co-Operation and Development, *"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data",* [Online]. Available: https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#scope. [Accessed: October. 15, 2019].
[10] N. Lord, *"What is the Data Protection Directive? The Predecessor to the GDPR",* 2019. [Online]. Available: https://digitalguardian.com/blog/what-data-proction-directive-predesor-gdpr. [Accessed: October. 20, 2019].
[11] P. Hustinx, "EU Data Protection Law: The Review of Directive 95/46/EC and the Proposed General Data Protection Regulation," *New Technologies and EU Law, Oxford University Press,* 2017.
[12] E. Council, *Data Protection Reform,* 2019. [Online]. Available: https:// consilium.europa.eu/en/policies/ data-protection-reform/. [Accessed: October. 17, 2019].
[13] V. Reding, "The European Data Protection Framework for the Twenty-First Century," *International Data Privacy Law*, vol. 2, no. 3, 2012.
[14] P. Hustinx, *Op. Cit.* pp. 148-149, 2019.
[15] M. Kedzior, "GDPR and beyond—a year of changes in the data protection landscape of the European Union," *ERA Forum*, vol 19, no. 4, 2019.
[16] H. Li, L. Yu, and W. He, "The Impact of GDPR on Global Technology Development," *Journal of Global Information Technology Management,* vol. 22, no. 1, pp. 4, 2018.
[17] J. Holvast, "History of Privacy, the Future of Identity in the Information Society. Privacy and Identity," *IFIP Advances in Information and Communication Technology*, Springer, Berlin, Heidelberg, vol. 298, 2008.
[18] T. Christopher and J. D. Anglim, J. D, *Privacy Right in the Digital Age.* Grey House Publishing, 2015.
[19] Anggara, "Menyeimbangkan Hak: Tantangan Perlindungan Privasi dan Menjamin Akses Keterbukaan Informasi dan Data di Indonesia," Institute for Criminal Justice Reform: Jakarta, 2018.
[20] W. T. DeVries, "Protecting Privacy in the Digital Age," *Berkeley Technology Law Journal*, vol. 18, no. 283, 2018.
[21] J. Holvast, "History of Privacy, the Future of Identity in the Information Society," *Privacy and Identity, IFIP Advances in Information and Communication Technology,* Springer, Berlin, Heidelberg, 2017.
[22] Privacy Europe, *About the Network.* 2019. [Online]. Available: https://www.privacy-europe.com/european-privacy-framework.html. [Accessed: November. 14, 2019].
[23] H. P. Yuwinanto, "Privasi Online dan Keamanan Data," *Jurnal Palimpsest*, vol. 2, no. 2, 2011.
[24] Intersoft Computing, *GDPR: Right to be forgotten.* 2019. [Online]. Available: https://gdpr-info.eu/issues/right-to-be-forgotten/. [Accessed: November. 4, 2019].
[25] L. M. Jones, "The Right to be forgotten," *Proc. Assoc. Info. Sci. Tech*, vol. 52, no.1, 2019.
[26] G. Sartor, "The Right to be forgotten in the Draft Data Protection Regulation," *International Data Privacy Law*, vol. 5, no. 1, 2019.
[27] Google Inc., *Google Transparency Report.* [Online]. Available: https://transparencyreport. google.com/eu-privacy/overview. [Accessed: January. 23, 2020].
[28] Google Inc., *European privacy requests Search removals FAQs*. 2020. [Online]. Available: from https://support. google.com/transparencyreport/answer/7347822. [Accessed: January. 23, 2020].
[29] Y. H. Sirait, "General Data Protection Regulation (GDPR) dan Kedaulatan Negara Non-Uni Eropa," *Gorontalo Law Review*, vol. 2, no. 2, 2019.
[30] European Commission, *Binding Corporate Rules (BCR).* 2020. [Online]. Available: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en. [Accessed: January. 28, 2020].
[31] D. F. Masoch, *Why Should Companies Invest in Binding Corporate Rules*?. ICLG: Data Protection, 6th Edition, 2019.
[32] GDPR EU.ORG. (2020). *Fines and Penalties.* 2020. [Online]. Available: https://www.gdpreu.org/ compliance/fines-and-penalties/. [Accessed: January. 28, 2020].
[33] M. Foulsham, *GDPR: How to Achieve and Maintain Compliance.* London: Routledge, 2019.

[34] Anynomus, "General Data Protection Regulations," *Art,* vol. 83, no. 2, 2018.
[35] M. Samonte, "Google v. CNIL: The Territorial Scope of The Right to be forgotten under EU Law," *European Papers,* 2020.
[36] D. Erdos, *Google v CNIL – The EU Court of Justice Seeks a Via Media on Global Internet Publication and European Data Protection.* Faculty of Law and Trinity Hall, University of Cambridge, 2020.