Sheraton Surabaya Hotel & Towers, October 17th - 19th, 2019
International Joint Conference on Science and Technology
Chapter ICST (International Conference on Science and Technology)

The Past, Present, and Future of Awareness and Preparation Toward General Data Protection Regulation (GDPR)

Ariana Tulus Purnomo[1] and Navara Seetee[2]

[1] National Taiwan University of Science and Technology, Taipei, Taiwan
[2] Srinakharinwirot University, Bangkok, Thailand

Email: [1]d10602808@mail.ntust.edu.tw, [2]suwapid@g.swu.ac.th

Abstract. General Data Protection Regulation (GDPR) is a new law of privacy that influences companies having a presence both in European Union (EU) and outside. There are many research studies published on knowledge, awareness, and preparation related to the GDPR. Understanding awareness and readiness of any company toward GDPR will be a benefit for planning, implementing, and achieving compliance with the regulation. However, research studies examining the awareness and preparation toward the GDPR is less discussed. Therefore, this paper presents a detailed review of the awareness and preparation from the past, present, and future. We have reviewed and analyzed research reports from 2016 to 2018. The implication for the future research, scholar, and practitioner are discussed.

Keywords: awareness; data privacy regulation; readiness.

1. Introduction

GDPR is an attractive topic that has attracted the attention of the people all around the world. The GDPR presents the set of rules that composed of data protection, individuals' right, and legal obligations in order to protect the personal data of people on a digital platform [1][2] . The GDPR is designed to create a unique standard that will govern the way personal data collected, used, and shared [3]. Our society is driven by technology and it is hard for people to control their own private data or limit the recording by companies especially in the online space that knows no territorial or regional boundaries [3].

Since 25th May 2018, all personal data acts of countries in EU were substituted by the GDPR [3]. By implementing GDPR, more than 40 existing laws also need to be changed. GDPR is the most significant change in the data protection space in the last 20 years, and it has an extensive impact. Although the GDPR is only applied to people having a residence in EU, it affects companies/organizations throughout the world. The organizations that process data of persons in the EU, and do business in EU have to comply with the GDPR [4].

After the implementation of GDPR, it will affect both citizens, as well as companies and organizations. In person level, they will be more aware of their privacy rights. The GDPR give the consumer control over their personal data collected by the company. For the companies, they need to

have responsibility for collecting privacy data of their customers [3]. In another word, the company has to comply with the GDPR. The regulation change is an opportunity but also a challenge of the companies in EU when complying with GDPR [5]. The challenges can be related to different factors, such as the interpretation of the new regulations, the motivation for organizational change, and the management of collecting and storing personal data [6].

Several reports are published on the awareness and preparation of GDPR [3][7]. For example, Dell software (2016) [7] did survey and found that digital/IT companies lacked a general awareness on GDPR; 97% of companies did not have a plan of GDPR preparation, and 9% of business professionals were confident for readiness in May 2018. Nielsen and Wind (2018) [3] study comparative legal research to identify the new requirements as a consequence of GDPR launching and to explore the preparation of ICT companies for the new requirements. They found that the ICT companies are preparing by piloting a new process and study about GDPR. However, the companies cannot complete a compellability due to lack of resources and vagueness of the regulation.

Understanding past and present progression of companies' awareness and preparation to compliance with the GDPR is useful both for researcher and practitioner in planning their next steps. The review is aimed to report on awareness and preparation from the past, present, and future using published reports from 2016 to 2018. Additionally, we discussed and suggested the implication for further research and practice.

2. Literature Review

2.1 General Data Protection Regulation (GDPR)

2.1.1. Definition of GDPR

The framework of data protection regulation has existed for a long time [2]. The GDPR was born in 2012. After four years of discussion, it was improved in April 2016 and was in force on May 25, 2018. This is the set of rules to protect the data of residence in 28 countries in EU [1][2]. The GDPR give the way for companies to collect and control the personal data. It covers the handling of personal data, including high penalties for non-compliance, and can execute any company in the world that process data of EU citizen [8]. The GDPR regulation comprised of 11 chapters including, general provisions, principles, rights of the data subject, controller and processor, personal data to third countries of international organizations, independent supervisory authorities, co-operation and consistency, remedies, liability and sanctions, provisions relating to specific data processing situations, delegated acts and implementing acts, and final provisions [9][10]. Each chapter has many articles such as Article 89 in chapter 9, the organization is obliged to ensure the data security process inappropriate way. In this Article, the data controller needs to apply an anonymized data system if the data subject is no longer needed [11].

The GDPR is basically about protecting and activating individual privacy rights [12]. The regulation gives certain individuals or subject data rights regarding their personal data processing. This right includes the right to correct inaccurate data, delete their data or limit processing, receive their data and fulfil requests to send their data to the other controllers. Citizens have the right to access, change and delete their personal data at certain times from the company's customer data. Companies are also asked to be transparent about why they collect data and how they will use it [13][14].

The regulation which was formulated for four years and was only approved on April 14, 2016, has four main points. First, the companies must notify users if a data leak occurs on their system, a maximum of 72 hours since the leak is known. Second, the companies must give full freedom to control the data belonging to their users from the EU. EU citizens have the right to allow, allow part of, or not allow data to be used by the companies. Third, is the right to be forgotten, which allows EU citizens to erase all their digital footprint from the companies used. Fourth, EU citizens are also given

the power to have data portability rights, namely, data formatted to be read easily on computer machines. This right allows EU citizens to transfer their data to other computer machines [9][10].

2.1.2. Urgency of GDPR

Before the GDPR is implemented, in our daily life, some of the following often occur. For example, a consumer wants to buy a new stove for his kitchen. This consumer does the surveys through a web browser. Without the knowledge of the consumer, several parties use customer's behaviour to learn about what customer needs. This is a big opportunity for the merchant promoting their product to the customer. In some case, several people disturbed by the advertisement for the product. Because by using individual privacy data as a media campaign, it is something that disturbs the customer's convenience [5]. Sometimes after buying an item from a certain store, usually the consumer will also get the advertisement from the current brand she purchased. Sometimes the consumer also gets the pop-up message or advertisement in their browser. After using our telephone number for ordering hotel or food, the telephone number data will be stored by certain parties to carry out the product promotions. These simple example is disturbing the consumer privacy and the consumer has their right to refuse such misappropriation privacy data [5]. A company that store private data of many people have an obligation to protect the user data. In the worst case, if one day the data is inadvertently used by other parties, the company must report this to the authorities and also notify the user. Because the user has the right to get informed about her privacy security[5].

2.1.3. Impact of GDPR

The GDPR was considered to be an impact on companies especially ICT-based industries because they usually use a variety and lots of personal information. Based on GDPR Article 4, personal information means all information that can identify a subject [11]. In addition, it also influenced new technologies such as the internet of things, cloud computing, and big data technologies. These technologies related to data protection [4][15]. Large corporate companies can analyse large amounts of behaviour information of their users. By using this kind of data, the system can find out the relationship between user behaviour and the patterns of their consumer. Companies are considered to have a lot of customer information. Because of that reason, the company that uses the ICT need to comply with this GDPR. Hopefully, the industry can significantly transfer control information to each [11]. By complying with GDPR, it makes customer appreciate companies that give better information into their products or services before buying or using their product and services [16]. Three things that customer perceive a company's trustworthiness are company's ability, benevolence, and integrity [16].

2.1.4. The Challenges and Opportunities after Implementing GDPR

Implementation of GDPR is a quite big challenge for the companies. Opportunities are less than challenges [5]. The challenges and opportunities faced by companies when implementing GDPR are summarized as shown in Table 1.

Table 1. Opportunities and Challenges of Implementing GDPR

Opportunities	***Challenges***
1. GDPR provides a competitive advantage for the company [5].	1. GDPR will change the procedures and routines of the company [5].
2. GDPR give an opportunity to clean the company's data. Data cleaning is related to the	2. Understanding the rules and their consequences [5].

disposal of unnecessary data and makes data to be more consistent. The data cleaning needs to be done by all employees with each manager in his department [5]. 3. Company data have excellent transparency. Companies will have cleaner data and have a more straightforward business process [5]. 4. The company will have a good reputation in the eyes of its customers. So that between some companies will have a better competitive value in serving their customers [5].	3. Companies need to determine which data needs to be secured, decide where it should be stored and limit the person who has access to the data [5]. 4. IT department and management department need determining the priority list and also the company's budget whether the technology in the company needs to be replaced or not [5]. 5. Change the legal requirements of GDPR to be a suitable and sustainable operational behavior of the company. Preparation in the face of GDPR relates to how far stakeholders in the organization are ready to face GDPR [17]. 6. Company costs are increasing 3 to 4 times [18].

The challenges faced by companies after May 2018 are not only limited to IT. In the case of business, it is also necessary to ensure that the process designed will produce results as expected. Regarding the subject of data, the crisis of violations and the audit process are essential in the implementation of GDPR [17].

2.1.5. Meet the GDPR Compliance

It is crucial for senior business stakeholders to understand and be aware of all GDPR requirements. The financial sanctions imposed on the company are quite expensive if the company cannot comply. The most severe GDPR violations can be fined of 20 million or 4% of a firm's global turnover [18]. The first step that needs to be taken through the journey of compliance with GDPR is the company's readiness. The first parameter of GDPR readiness is about how far the stakeholder of the company understand GDPR [17]. In order to have good readiness, it is critical for companies to conduct training and education regarding the importance of GDPR [17]. Most of the companies surveyed chose to change their business strategies so they could meet GDPR [18]. ICT companies are preparing by piloting new processes and study the results to check to comply with the regulation.

MetaCompliance (2018) [17] suggested the way to meet the GDPR compliance as follows: (1) Make the GDPR readiness team that have clear roles good skill, and the good ability of member, and management of budget according to the company resources. If the GDPR readiness team is ready to carry out the mission, the journey for implementing GDPR can begin smoothly; (2) Identify and review relevant business function. By having a proper business function, if a problem occurs, tracking the matter will be easy. (3) Identify and assess the process of third-party activities; (4) Make personal data centrally. Companies need to determine what kind of data that needs to be collected, where the data is coming from, why the data is collected, how the data is processed, what is the legal basis of each operation process, where data is stored, how long the data is held, who have access to the data, where are the data transferred. Data is then neatly arranged so that it becomes a comprehensive personal data register. This data will be stored centrally and checked periodically to ensure integration over time. In addition, data flow maps are also needed. It will help to provide visual and flow forms internally and externally so that anyone easily understands them; (5) Distribute data protection policies and privacy notices every time. Transparent privacy notices to the customer is an obligation that must

be done by the company [19]. By using this kind of privacy notices, consumers are expected to know how the company will use their data. Furthermore, updating the data protection policies and privacy notices needs to be done regularly; (6) Educate personal data holders and data processors. Provide education to the data holders and data processors is necessary to ensure that they truly understand the rules for achieving compliance with GDPR. The quality of personal data holders and processors is representing the reputation of the company. This is a valuable asset for the company.

2.2. Awareness and Readiness before Implementing GDPR

Before implementation of GDPR, many research studies made a survey on awareness and readiness with employees in companies from various countries such as UK [4], England [7], German [7], Dutch [7], Norway [5]. The samples are senior managers [4], a person who works on data privacy [7] or data protection experts [4]. It was found that most of them had a lack of awareness about GDPR [4]. The companies did not inform or train their staff [4]. 45% of Norwegian companies claimed to have good knowledge about this [5]. The reason of lack of awareness is that they had limited understanding of GDPR [5].

For GDPR compliance, Companies did not prepare for GDPR compliance, only 17% of England, German, and Dutch companies have fully ready for the GDPR [7]. 57% of respondents had prioritized GDPR during the last year [5]. The organization in the UK have still focused on the initial stage of implementation [4]. Many companies are still late in starting this GDPR [17]. The implementation of technology that adheres to GDPR is still in the process [17]. However, the companies cannot complete a compellability because of lack of resource and vagueness of the regulation [3]. The impact of the GDPR is not clear [7]. The companies did not have enough budget [5]. They lacked the required technology [5]. The companies have a low level of implementation due to a low level of awareness [4].

Nevertheless, it was found that different sizes of company, different in preparation. The large companies informed their staff and up to date [4]. The online market was in advance, a big bank has had GDPR programmes [4]. For Brexit, which is the UK exit the EU, almost half of people both in the UK and outside the UK feel not clear on the impact of Brexit on GDPR [7]. For Asian companies that locate outside of the EU but their target is EU customers or monitor behaviour of the EU people, it was found that only 11% of companies were ready for the effect of GDPR. However, they still have a lot of work to do. Most the companies in Asia were found unprepared for complying with the regulation or far from GDPR compliance. These might be they are suffering to interpret, measure, and monitor compliance with GDPR [19].

There is a big misunderstanding. Some companies assumed that their company does not have essential user data because they do not deal with customer personal data. Even though the company does not handle the user's data, the company still has the employees who have personal data that needs to be protected by GDPR [5].

2.3. Awareness and Readiness after Implementing GDPR

After May 25, 2018, many companies use temporary controls and manual processes to ensure compliance with GDPR in their company. Furthermore, if the system already stables, the company will apply more permanent technology for the coming year [17].

A few research studies report the data after implementing the GDPR. TrustArc [21] conducted a survey one month after May 25, 2018, on 600 IT and legal professionals of privacy data from companies in the United States (US), United Kingdom (UK), and EU. The results showed that only 20% of companies surveyed had complied GDPR. Meanwhile, 53% are still in the implementation stage, and 27% of companies have not even started implementation (Fig. 1).

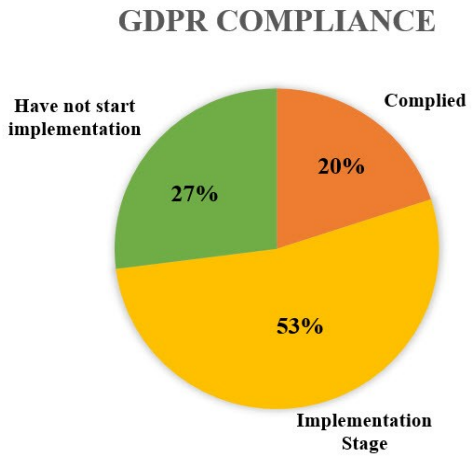

Fig. 1 GDPR compliance after May 25, 2018, in EU, UK, US [21].

The percentage of the company that compliance with GDPR can be seen in Fig. 2. It was found that 27%, 21%, and 12% of companies in EU, UK, and the US, respectively comply with GDPR. The readiness of companies in EU was higher than UK and US.

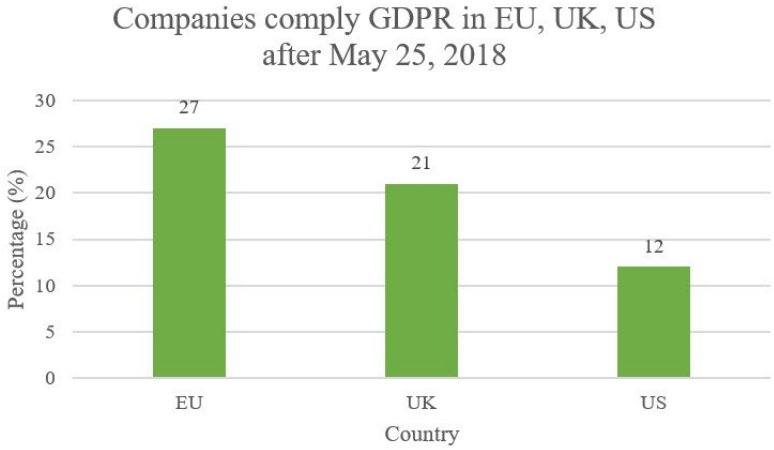

Fig. 2 GDPR compliance after May 25, 2018, in EU, UK, US [21].

During the implementation of GDPR, 27% of the companies have spent more than 500.000 USD to comply with GDPR. 30% of companies said that they plan to spend this amount of money between June and December 2018 [21].

Sirur, Nurse, & Webb (2018) [8] found that large companies accomplishable to meet GDPR compliance. The small-to-medium companies are less focus on data protection. The companies face the problems such as too broad of the regulation, difficult to put the qualitative recommendations of the regulation in practice, and need to arrange their complex data networks [8]. Although implementing GDPR is very difficult, most of the company see that GDPR has a big positive impact on their business. The complexity of GDPR is the biggest challenge in complying with GDPR. Most companies argue that data privacy will be very important for the company and users [21].

3. Discussion

The present paper aims to discuss awareness and preparation of companies to comply with the GDPR in the past, present, and future. The literature review showed that the awareness before the GDPR

implementation was found most of them lacking knowledge and awareness about GDPR compliance. However, we have not found the report about awareness of GDPR after it is in force. In the future, it seems the awareness should be increased, due to it, they need to prepare their company to meet the GDPR compliance.

The readiness of the company in compliance with GDPR before implementing was found less than 17 %. Then, the readiness is up to 20% after implementing. It is higher and seems increasing in the future. It was found that the large companies were more readiness than medium to small companies.

We have found the three key factors from the literature that account for the readiness of the companies including reputation, money, and impact of the GDPR. The large companies have a lot of money. They have a direct impact of GDPR if they cannot comply with GDPR. It will also affect their reputation. Therefore, these companies are the first group that meets the regulation.

Contrary to the medium and small companies, which have not much money to invest in a short period to comply with the regulation. They need more time to manage their system to meet the GDPR compliance. In addition, these companies have not clear about GDPR impact the wonder whether it affects their company or not. Furthermore, if companies are small and regardless of the reputation, they will not attempt to comply with the GDPR.

Awareness of employees has influenced readiness. The medium to small companies has not trained their employee. Thus, the companies have not ready yet. Contrary to the large company they informed and trained their employee, as well as up to date. So they met the GDPR compliance.

It was found that the companies in the UK and outside EU such as Asia cannot insist on the implementation of GDPR because they have not realized the impact of GDPR itself. This is a misunderstanding. While from the user side, nothing should be worried. Although proposed by the EU, this regulation is applied internationally. As the user, we also get the same level data protection as EU citizen. Unfortunately, for residents outside the EU, if they get the disadvantages such as the data is being misused, they cannot complain to the company that is not obliged to implement GDPR. Therefore, we can only hope that the IT company can process user data properly. Because nowadays there are no other rules that are as strict as GDPR. In general, GDPR is stricter than previous regulations and makes users more bombarded by permission requests by data access services. On the positive side, this allows users to sort information that can be retrieved.

In addition, some companies assume that they do not store and process the personal user data. This is a big mistake and misunderstanding for the company. All companies must have at least the workers' data. It means that the companies also need to protect the private data of their employees. Indeed, the GDPR will only take effect after May 25, 2018, however, this does not mean that companies outside the EU only silent and consider GDPR as a wind. Companies outside EU must maintain personal data properly if they do not want to get a big sanction of fine.

Not only the companies but also the government of each country needs to take care of their citizen privacy data. It is good for the non-EU country to start creating similar rules with GDPR. This kind of privacy policy protection is very important because the protection of personal data maintaining the personal safety of the citizen. Besides that, data loss allows someone to be exposed to unnecessary risks such as money, safety, and reputation. The other thing that needs to be done by the government is providing the awareness education in security data protection for their citizen. During the time where the development of the digital world has also grown, the data privacy needs will increase. Data protection requires the commitment of every employee in the company and requires each of the employees to complete data security training on a regular basis to ensure the highest standards of data protection. The company also need a require vendors to meet their data privacy standards.

Protection of personal user data has become a big issue lately discussed. Moreover, there is a lot of big company engaged in the digital world. To anticipate this problem, EU updates their regulations on personal data protection which are referred to as GDPR. The goal is protecting the user data and ensuring transparency of personal data usage. GDPR determines new regulations in companies, government agencies, and other organization that over goods and services to the EU, or collecting and analysing data that related to EU citizen. GDPR should be adhered by any organization around the

world that collects and processes data of EU citizen. If the company does not comply with this regulations, the company will get a substantial fine. It is big challenges and opportunities for the organization and the company to comply with GDPR. Preparation toward GDPR is really important for the organization and the company. How far and how good the company complying GDPR shows how good their awareness and readiness are facing GDPR.

The dramatically changes also occurred in the companies, regarding the data circulation behind the scenes, which are unknown to the user. For example, the information related to age, sex, location, and favourite topics of Facebook's user. This information can be an important treasure of the company, for estimating suitable ads to be displayed. Facebook can also share those data with the other companies.

In the end, GDPR should be treated as a good challenge to get a lot of opportunities in the companies. The companies should not regard GDPR as a threat to the company because a company will have a value added by the increasing of users trusted. In the other side, companies that do not comply with GDPR rules will get a big amount of fines, and it is not impossible to bankrupt just because they are affected by administrative sanctions.

4. Implication

4.1. For the Researcher

The regulation is rules about all process of personal data. It does not affect only the company that collected the data of people residence in EU. It also influences every work that related to the data of people. Therefore, research institutions, libraries, archive collectors, and researcher, who usually collect and use data containing personal data for any purpose such as researcher using for doing their experiment, should ask for consent form or permission of the user or use the old personal data [11]. In addition, to fulfill the obligations set by the GDPR, research institutions or organizations need to assess how far their data is used. This requires research institutions and organizations to update all processing records and review the protection measures taken by the organization [11]. In the case of data reuse for the scientific, historical research and the statistics purpose, the organization is also obliged to ensure the rights and the freedoms of the subject [11].

4.2. For a Practitioner

Based on the result that shows the lack of awareness of GDPR, the practitioner of the companies should attempt to train their employee to have a knowledge and realize on the GDPR as a consequence to meet the GDPR compliance quickly. In addition, planning GDPR as the priority of their plan is the most important thing. The most important things should be recognized are even though your company is in EU or outside, and your company is big or small, all company should comply with GDPR. Due to it, some company can use in accordance with the GDPR, the company can learn from that and adapt it for the application.

4.3. For the Future Research

This paper found that three factors (money, reputation, and impact of GDPR) affect the GDPR compliance of the company. The future research might study these factors or find the investigation amount of impact and its relationship to force the company to meet GDPR compliance as soon as possible. The size and area of a company were different results of GDPR compliance. Future research could investigate or compare the approach that is suitable for each size and area of the company.

5. Conclusion

The GDPR is a new regulation being implemented in EU, but the impact is around the world. This paper attempts to discuss the previous survey on the preparation of awareness and readiness of the

company both in EU and outside. It was found that it is too early for some companies in complying with GDPR. The literature showed a lot of companies still have not changed their privacy policy to comply with GDPR. The most important thing is that all companies in the EU have to comply with GDPR. Although the company does not hold personal data from customers, the company at least having the employee data, and supplier's data that need to be protected by GDPR. Besides that, non-EU company that handles EU citizen privacy data also have the responsibility to obey with the GDPR. Implementing and complying with GDPR is a managerial responsibility. However, each individual in the organization also needs to know about this issue. It is a quite big challenge and opportunity for the company toward GDPR. Nevertheless, complying GDPR will have a big added value to the company because it increases the credibility of their users and certainly increases a lot of benefit for a long term.

References

[1] C. J. Bennett, "The European General Data Protection Regulation: An instrument for the globalization of privacy standards?" *Information Polity*, vol. 23, no. 2, pp. 239–246, 2018.
[2] Y.-S. Martin and A. Kung, "Methods and tools for GDPR compliance through privacy and data protection engineering," *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2018.
[3] T. Neilsen and J. Wind, "GDPR – are we ready? a comparative and explorative study of the changes in personal data privacy and its impact on ICT companies," Bachelor Thesis, Malmö universitet/Teknik och samhälle, Swedia, 2018.
[4] C. Addis and M. Kutar, "The general data protection regulation (GDPR), emerging technologies and UK organizations: Awareness, Implementation and readiness," *UK Academy for Information Systems Conference 2018*, 2018.
[5] W. Presthus, H. Sorum, and L.R Andersen, "GDPR compliance in Norwegian companies," *Norwegian Conference for IT Use in Organizations (NOKOBIT)*, Savlbard, 2018.
[6] M. D. C. Freitas and M. M. D. Silva, "GDPR in SMEs," *2018 13th Iberian Conference on Information Systems and Technologies (CISTI)*, 2018.
[7] Dell, "GDPR: Perceptions and readiness. A global survey of data privacy professionals at companies with European costumers", Dimensional Research, 2016.
[8] S. Sirur, J.R.C. Nurse, and H. Webb, "Are we there yet?: understanding the challenges faced in complying with the general data protection regulation (GDPR)," *The 2nd International Workshop on Multimedia Privacy and Security*, 2018.
[9] Intersoft consulting. (2018) General data protection regulation GDPR, Deutsch. [Online]. Available: http://gdpr-info.eu.
[10] H. Schulze, "GDPR compliance report", Cybersecurity-Insiders, 2018.
[11] T. Katulic and A. Katulic, "GDPR and the reuse of personal data in scientific research," *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018.
[12] T. W. Kim and B. R. Routledge, "Informational privacy, a right to explanation, and interpretable AI," *2018 IEEE Symposium on Privacy-Aware Computing (PAC)*, 2018.
[13] V. Diamantopoulou, A. Androutsopoulou, S. Gritzalis, and Y. Charalabidis, "An assessment of privacy preservation in crowdsourcing approaches: Towards GDPR compliance," *2018 12th International Conference on Research Challenges in Information Science (RCIS)*, 2018.
[14] A. Skendzic, B. Kovacic, and E.Tijan, "General data protection regulation – protection of personal data in an organization," *The 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 2018.
[15] L. Elluri and K. P. Joshi, "A knowledge representation of cloud data controls for EU GDPR compliance," *2018 IEEE World Congress on Services (SERVICES)*, 2018.
[16] R. Crossler and C. Posey, "Robbing peter to pay paul: surrendering privacy for security's sake in an identity ecosystem," *Journal of the Association for Information Systems*, vol. 18, no. 7, pp. 487–515, 2017.
[17] Meta Compliance, "GDPR best practices implementation guide, transforming gdpr requirements into compliant operational behaviours", London, 2016.
[18] J. Seo, K. Kim, M. Park, M. Park, and K. Lee, "An analysis of economic impact on IoT under GDPR," *2017 International Conference on Information and Communication Technology Convergence (ICTC)*, 2017.
[19] K. Renaud and L. A. Shepherd, "How to Make Privacy Policies both GDPR-Compliant and Usable," *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, 2018.
[20] L. Karry. (2018) GDPR: Are Asian firms ready? International Financial Law Review, London. [Online]. Available: https://search.proquest.com/docview/2007905053?pq-origsite=gscholar.

[21] E. Gately (2018) 80 Percent of Companies Still not GDPR-Compliant. [Online]. Available: https://www.channelpartnersonline.com/2018/07/13/80-percent-of-companies-still-not-gdpr-compliant/.