Malaysian Journal of Social Sciences and Humanities (MJSSH) (e-ISSN : 2504-8562)
2022, Volume 7, Issue 9, e001776
DOI: https://doi.org/10.47405/mjssh.v7i9.1776

The Magnitude of GDPR To Malaysia

Mohd Bahrin Bin Othman[1*], Muhammad Faiz Bin Abu Samah[2]

[1]Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia.
Email: mohdb916@uitm.edu.my
[2]Faculty of Law, Universiti Teknologi MARA, 40450 Shah Alam, Selangor, Malaysia.
Email: faiz.abusamah@gmail.com

CORRESPONDING AUTHOR (*):
Mohd Bahrin Bin Othman
(mohdb916@uitm.edu.my)

KEYWORDS:
GDPR
Data Privacy
Data Protection
PDPA

CITATION:
Mohd Bahrin Othman & Muhammad Faiz Abu Samah (2022). The Magnitude of GDPR To Malaysia. *Malaysian Journal of Social Sciences and Humanities (MJSSH), 7*(9), e001776.
https://doi.org/10.47405/mjssh.v7i9.1776

ABSTRACT

The European Union ("EU") General Data Protection Regulation ("GDPR") governs any individuals or companies that stores or processes personal information about EU citizens within EU states even if it does not involve a business presence within the EU. Malaysian businesses need to comply with the GDPR as failure to comply will cause disruption or discontinuance of business. This paper aims to understand and evaluate the scope of the GDPR and its effect on personal data protection in Malaysia. It employs a doctrinal qualitative approach by examining the GDPR and the Malaysia Personal Data Protection Act 2010. This paper suggests that the GDPR provides a more comprehensive law with its holistic principles and rights which may provide lessons for Malaysia in protecting personal data as the area covered by the GDPR is broader specifically the non-commercial transactions, its wider range of rights and the extraterritorial applicability.

Contribution/Originality: The paper contributes to the existing literature on protecting data privacy in Malaysia. Specifically, the impact of GDPR on Malaysian businesses dealing with their European Union counterpart and the understanding of the scope and application of the GDPR needs to be considered in the review of the Data Protection Act 2010.

1. Introduction

The European Union ("EU") GDPR ("GDPR") came into force on 25 May 2018. The GDPR replace the old 1995 Data Protection Directives 1995 ("DPD"). This Regulation is enforced on all members of the EU. However, the PDP was not fit for purpose in the digital age where most businesses and organisations are doing online transactions, and across borders. As such, something else was needed to deal with the modern digital needs of businesses and processes. In addition, DPD imposes lesser fines as it is restricted to their jurisdiction. Because of that, something else was needed to deal with the modern digital needs of businesses and processes of that, the EU went on their way

in introducing the GDPR. The GDPR is a major update to the DPD, which is before the proliferation of cloud platforms and social media, let alone the scale of today's data usage (Nguyen & Gyu, 2020). Osborne (2020) applauded the GDPR as a new version of data protection as older laws are not suitable for modern technology and online business practices.

Significantly, the GDPR applies extraterritorially to cover personal data in business within and outside the EU. This means that EU citizens' personal data is protected when they transfer their business outside of the EU, unlike Malaysia's Personal Data Protection Act 2010 ("PDP") which is inapplicable outside of Malaysia (Section 3(2) of PDPA). This highlights the insufficiency of PDPA in today's technological advancements (Fauzi, 2019).

2. Literature Review

Linden et al. (2019) explain that the GDPR defines four entities, that are, data subjects, data controllers, data processors, and third parties. The data subjects are the users of the information systems from which data is collected. The data controller is typically the service provider (for example, website or mobile app) with a vested interest in receiving and processing the user data. A data controller might employ a processor to process the data on its behalf. Finally, the data controller might authorize a third party (for example, an analytics agency) to process some of the user's data. While serving as better privacy and security framework, the GDPR also aims at protecting data ownership by obligating data controllers to provide fundamental rights for data subjects to control over their data (Nguyen et al., 2021).

An important aspect of data protection is purpose limitation, meaning users must consent about a particular and specific purpose for processing data (Nouwens et al., 2020). Thus, Article 4 of the GDPR defines consent more definitively, to mean 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by clear affirmative action, signifies agreement to the processing of personal data relating to him or her. Therefore, when an organisation relies on consent as the basis for processing in a big data context, they must inform the data subjects how they will use their personal data and there must be a clear indication that the data subject consent to the processing. The basics of valid legal consent are defined in Article 7 of the GDPR. Consent must be given freely, specific, informed, and unambiguous voluntarily.

The GDPR outlines six principles for the controller to adhere to when processing personal data. Firstly, is lawfulness, fairness, and transparency. GDPR requires personal data to be processed lawfully, fairly and in a transparent manner.

Secondly, is a purpose limitation. This means that personal data may only be collected for a specific purpose and not processed data beyond the organization's purpose.

Thirdly, is the data minimisation principle, which states that the data that is processed must be adequate, relevant and limited to what is necessary about the purposes for which they are processed.

Fourthly, is the accuracy principle, which requires all personal data that are processed to be accurate and kept up to date. Further, every reasonable step must be taken to

ensure that inaccurate personal data, having regard to the purposes for which they are processed, are erased or rectified without delay.

Fifthly, is the storage limitation principle which mandates that personal data are to be kept no longer than is necessary for the purposes for which the personal data are processed unless for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

The sixthly is the security principle which provides that personal data must be processed in a manner that ensures appropriate security, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

3. Methodology

This paper applies a doctrinal methodology. It involved a comparative study between the GDPR and the PDPA. It analyses a set of secondary data obtained from the statutes, books, journals, online articles and viewpoints on the studies in personal data protection. It focused on the unit of analysis which consists of the principles of data principles and data rights.

4. Result and Discussion

4.1. The 8 Basic Rights of the General Data Protection Regulation

Under the GDPR, individuals have the right to access, right to be forgotten, right to data portability, the right to be informed, the right to have the information corrected, the right to restrict processing, the right to object and the right to be notified.

4.1.1. The Right to Access

The right to access under GDPR means that individuals have the right to request access to their personal data and to ask how their data is used by the company after it has been gathered (Article 15). For example, individuals have the right to access data concerning their health such as medical records, examination results, assessments and any treatment provided. However, this right must not affect the rights of others, including trade secrets or intellectual property.

Article 15 of the GDPR60 expressly stated that:

a. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:-

i. the purposes of the processing;
ii. the categories of personal data concerned;
iii. the recipients or categories of recipients to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
iv. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

v. the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
vi. the right to complain with a supervisory authority; where the personal data are not collected from the data subject, any available information as to their source;
vii. the existence of automated decision-making, including profiling, referred to in Articles 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

b. Where personal data are transferred to a third country or an international organisation, the data subject shall have the right to be informed of the appropriate safeguards under Article 46 relating to the transfer.

c. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject requests by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

d. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others."

4.1.2. The Right to Erasure

The right to be erasure ('forgotten') is provided under Article 17 of the GDPR. If consumers are no longer the customers, or if they withdraw their consent from a company to use their data, then they have the right to have their data deleted. Article 17 of the GDPR provides for the right to be forgotten which gives data subjects the right to have their data erased for example where the data is no longer necessary for the purpose for which it was collected or the data subject withdraws his consent. It means that GDPR gives individuals the right to request organizations to delete or erased data.

Article 17 of the GDPR provided that:

a. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:-

i. the personal data are no longer necessary about the purposes for which they were collected or otherwise processed;
ii. the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
iii. the data subject objects to the processing under Article 21(1) and there are no overriding legitimate grounds for the processing or the data subject objects to the processing under Article 21(2);
iv. the personal data have been unlawfully processed;"

In the case of *Google Spain SL and Google Inc. V Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2012]*, a ruling by the EU Court of Justice found that

European data protection law gives individuals the right to ask search engines like Google to delist certain results for queries related to a person's name. Another similar case is the case of *Google Inc. v Commission Nationale de l'informatique et des libertés [2017]*, in deciding what to delist, search engines must consider if the information in question is "inaccurate, inadequate, irrelevant or excessive," and whether there is a public interest in the information remaining available in search results. However, this is limited to countries within the EU only.

4.1.3. The Right to Data Portability.

Individuals have a right to transfer their data from one service provider to another. And it must happen in a commonly used and machine-readable format. GDPR provided this under Article 20:-

a. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:-

i. the processing is based on consent under point (a) of Article 6(1) or point (a) of Article 9(2) or a contract under point (b) of Article 6(1); and
ii. the processing is carried out by automated means.

b. In exercising his or her right to data portability under paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

c. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or the exercise of official authority vested in the controller.

d. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others."

4.1.4. The Right to be Informed

This is governed under Article 13 of GDPR. Simply means that any gathering of data by companies, and individuals must be informed before data is gathered. Consumers have to opt-in for their data to be gathered, and consent must be freely given rather than implied.

Article 13 of the Regulations stated that:

"a. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

i. the identity and the contact details of the controller and, where applicable, of the controller's representative;
ii. the contact details of the DPO, where applicable;
iii. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

iv. where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;
v. the recipients or categories of recipients of the personal data, if any;
vi. where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and how to obtain a copy of them or where they have been made available.

b. In addition to the information referred to in paragraph 1, the controller shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

i. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;
ii. the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to the processing as well as the right to data portability;
iii. where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
iv. the right to complain with a supervisory authority;
v. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and the possible consequences of failure to provide such data;
vi. the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

c. Where the controller intends to further process the personal data for a purpose other than that for which the personal data were collected, the controller shall provide the data subject before that further processing with information on that other purpose and with any relevant further information as referred to in paragraph 2.

d. Paragraphs 1, 2 and 3 shall not apply where and insofar as the data subject already has the information."

4.1.5. The Right to Rectification

Article 16 of GDPR also provides the right to rectification ('have the information corrected') which ensures that individuals can have their data updated if it is out of date or incomplete or incorrect. In the GDPR, Article 16 explained that the data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including using providing a supplementary statement.

Article 18 of the GDPR also provides the right to restrict processing. Individuals can request that their data is not used for processing. Their record can remain in place, but not be used.

According to Article 18 of the GDPR:

a. The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

i. the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
ii. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
iii. the controller no longer needs the personal data for the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
iv. the data subject has objected to processing under Article 21(1) pending the verification of whether the legitimate grounds of the controller override those of the data subject.

b. Where processing has been restricted under paragraph 1, such personal data shall, except storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or reasons of important public interest of the Union or a Member State.

c. A data subject who has obtained restriction of processing under paragraph 1 shall be informed by the controller before the restriction of processing is lifted.

4.1.6. Right to Object

Article 21 of the GDPR provides the individual right to object. This includes the right of individuals to stop the processing of their data for direct marketing. There are no exemptions to this rule, and any processing must stop as soon as the request is received. In addition, this right must be made clear to individuals at the very start of any communication.

Article 21 provides that:

a. The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to the processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

b. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to the processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

c. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
d. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

e. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.

f. Where personal data are processed for scientific or historical research purposes or statistical purposes under Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to the processing of personal data concerning him or her unless the processing is necessary for the performance of a task carried out for reasons of public interest."

4.2. The General Data Protection Regulation was Created to Revise and Control Businesses Way of Handling Information and Data of Their Customer

Any organization or business that deals with data of EU citizens such as banks, insurance companies, telcos, and other financial companies. Coming into force, GDPR improves the protection of individual data and clarifies what companies can or cannot process personal data of the subject. With the emergence of technologies and communication, online transaction is common. Individuals send emails, shared online documents, pay bills, and purchase goods online by entering personal details without a second thought. These individuals have no idea how much personal data they have shared online and what happens to the personal data that they have entered. When an individual intends to make a transaction online, the companies will inform you to enter your email address, phone number, name and address to collect individual information and inform the individual about their services or better offer. However much to our ignorance, some companies sell their customer data to another service. Hence the new GDPR was enforced and permanently changed the way businesses collect, store and use customer data.

4.3. The General Data Protection Regulation Protects Right and Information of the European Union Citizens (Not Only Within the European Union but Also Data of the European Union Citizens Exported Out of the European Union)

Article 3 of the GDPR explained about territorial scope of the law.

a. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.

b. 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:-

i. 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
ii. the monitoring of their behaviour as far as their behaviour takes place within the Union.

c. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by public international law".

Regardless of where the EU citizens are physically located at the time of processing whether in or outside of the EU, GDPR protects their data being processed. For example, if a Malaysian company is selling services to someone out in the EU, that Malaysian company is still required to comply with GDPR because of the European data being involved. This is the way of EU protect its citizens' data. All companies and business that deals with data relating to EU citizens must comply with the GDPR. GDPR introduce stringent fines if companies fail to adhere to the regulation.

4.4. Businesses and Organizations Are Bound by The Same Rules Hence Transparent Trust Network

The GDPR impose obligations on organisations that process personal data and requires all members of the EU to comply with the regulations hence there are no loopholes for them to avoid. Instead of each country having its data protection regulation, the GDPR set the rules for them so that each country under the EU can follow single regulation. This significantly streamlines the regulatory environment for businesses across the EU. A company operating in different countries no longer need to comply with multiple regulations, instead, they only need to comply with GDPR to offer their services anywhere in the EU. Single regulation makes it more simple and cheaper for companies to do business in the EU. It also ceases any double standard or unfairness in the event they were to follow different regulations for different countries before GDPR. The regulation designed in GDPR fits all obligations of the EU countries.

5. Conclusion

The GDPR is designed to protect EU citizens' personal data by defining how organizations process, store, and destroy it. It is evinced that the main purposes of the GDPR are to ensure data protection laws are standardized across all member states and to expand the rights of data subjects. The six principles of lawfulness, fairness, transparency, purpose limitation, data minimization principle, accuracy principle, storage limitation principle and security principle must be followed by a data user to ensure the personal data that is being processed complies with the GDPR. The GDPR also recognized eight basic rights that aim to ensure the data subjects have greater control over who collects their data, how the information is used, and its duration. The rights set under the GDPR also play an important role in ensuring the regulation's effectiveness in protecting personal data.

It is suggested that the GDPR is the world's most comprehensive data privacy law. It also can be seen that GDPR applies a very strict approach to ensure an individual's personal data is being protected correctly, and to ensure there should be no risk of a data breach. Hence, the GDPR can be seen as a model for Malaysia to emulate its PDPA.

Acknowledgement

Part of this article was extracted from a Master of Enforcement Law project paper submitted to Universiti Teknologi MARA, Shah Alam, Selangor.

Funding

This study received no funding.

Conflict of Interests

The authors reported no conflicts of interest for this work and declare that there is no potential conflict of interest with respect to the research, authorship, or publication of this article.

References

Fauzi, N. (2019, February 12). Data Privacy Laws: Malaysia Has a Long Way to Go, *New Straits Times Press.* https://www.nst.com.my/opinion/columnists/2019/02/459321/data-privacy-laws-malaysia-has-long-way-go.

Google Inc. v Commission Nationale de l'informatique et des libertés (CNIL) (2017) Case C-507/17 - Court of Justice of the European Union ('Google v CNIL'). https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:62017CC0507

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González (2012) Case C-131/12 – Court of Justice of the European Union ('Google v. Spain'). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131

Linden, T., Khandelwal, R. Harkous,H., & Fawaz.K. (2019). The Privacy Policy Landscape After the GDPR. arXiv:1809.08396v3 [cs.CR].

Nguyen, T, Kai, S, Gyu, M.L. & Yike, L. (2020). A Blockchain-Based Solution. *IEEE Transactions on Information Forensics and Security, 15*, 1746-1761.

Nguyen, T., Kai.S., Siyao, W., Florian, G., & Guo, Y.K. (2021). Privacy Preservation in Federated Learning: An insightful survey from the GDPR Perspective. *Arxiv*. arXiv:2011.05411v5 [cs.CR].

Nouwens, M., Liccardi., I, Veale.M., Karger.D, & Kagal. L. (2020). Dark Patterns after the GDPR: Scraping Consent Pop-ups and Demonstrating their Influence. *Proceedings of CHI '20 CHI Conference on Human Factors in Computing Systems, April 25--30, 2020, Honolulu, HI, USA*. https://hdl.handle.net/1721.1/129999.

Osborne, C. (2020). Australia Proposes Privacy Act 1988 Reforms Inspired by EU's GDPR. *Portswigger*. https://portswigger.net/daily-swig/australia-proposes-privacy-act-1988-reforms-inspired-by-eus-gdpr.