A comparative analysis: health data protection laws in Malaysia, Saudi Arabia and EU General Data Protection Regulation (GDPR)

Jawahitha Sarabdeen
College of Law, Prince Sultan University, Riyadh, Saudi Arabia, and

Mohamed Mazahir Mohamed Ishak
JS Law Firm, Pickering, Canada

Received 17 January 2024
Revised 22 February 2024
Accepted 14 March 2024

Abstract

Purpose – General Data Protection Regulation (GDPR) of the European Union (EU) was passed to protect data privacy. Though the GDPR intended to address issues related to data privacy in the EU, it created an extra-territorial effect through Articles 3, 45 and 46. Extra-territorial effect refers to the application or the effect of local laws and regulations in another country. Lawmakers around the globe passed or intensified their efforts to pass laws to have personal data privacy covered so that they meet the adequacy requirement under Articles 45–46 of GDPR while providing comprehensive legislation locally. This study aims to analyze the Malaysian and Saudi Arabian legislation on health data privacy and their adequacy in meeting GDPR data privacy protection requirements.

Design/methodology/approach – The research used a systematic literature review, legal content analysis and comparative analysis to critically analyze the health data protection in Malaysia and Saudi Arabia in comparison with GDPR and to see the adequacy of health data protection that could meet the requirement of EU data transfer requirement.

Findings – The finding suggested that the private sector is better regulated in Malaysia than the public sector. Saudi Arabia has some general laws to cover health data privacy in both public and private sector organizations until the newly passed data protection law is implemented in 2024. The finding also suggested that the Personal Data Protection Act 2010 of Malaysia and the Personal Data Protection Law 2022 of Saudi Arabia could be considered "adequate" under GDPR.

Originality/value – The research would be able to identify the key principles that could identify the adequacy of the laws about health data in Malaysia and Saudi Arabia as there is a dearth of literature in this area. This will help to propose suggestions to improve the laws concerning health data protection so that various stakeholders can benefit from it.

Keywords Privacy, Health data, Protection, Malaysia, Saudi Arabia, GDPR

Paper type Research paper

1. Introduction

With the advancement of technology, personal data has become the black diamond as data are most sought after for understanding customers' wants and needs and providing targeted solutions for their problems. With technologies in the health sector, patients' data are

The authors would like to acknowledge the support provided by the Prince Sultan University (PSU) and the Governance and Policy Research Lab, PSU.

International Journal of Law and Management
Vol. 67 No. 1, 2025
pp. 99-119

1754-243X
DOI 10.1108/IJLMA-01-2024-0025

collected in digital format, stored and accessed to provide better care. With the help of advanced technologies, health service providers could assess a patient from various dimensions as a large amount of data could be easily accessed and assessed. The connectivity and availability of the patient's data through a network of providers like insurers, medical practitioners, pharmacies, laboratories and health-care administrators allow quick diagnoses, approval and treatment. The use of technology in the diagnosis, assessment and treatment of patients relies on enormous health data. The reliance causes concern over the privacy, security, confidentiality and safety of health data. Overreliance on technology may also create issues related to control over health data, fairness and equity as health-related decisions could be automated without human interference. Further, providing health-care services not only relies on technology but also on various parties. The involvement of various parties and technologies requires adequate legal protection to ensure sensitive medical data are protected from unauthorized access, use and misuse by various parties. Inadequate legal protection will deter people from seeking health care and leave them without any legal ramifications in cases of misuse or abuse (Sarabdeen and Moonesar, 2018).

Privacy that includes data privacy could be defined as a right that grants value to individuals to decide the way they want to handle their privacy (Hynes, 2021). The Universal Declaration of Human Rights (UDHR), 1948, recognizes the right to privacy. Article 12 of the General Data Protection Regulation (GDPR) encompasses protection against violation of privacy, home, correspondence, honor and reputation. Individuals may opt to give away their privacy or hold tightly to it. Many countries, including Malaysia and Saudi Arabia, adopted the UDHR in 1948. In 2010, after years of contemplation, the Malaysian legislature passed the Malaysian Personal Data Protection Act (PDPA) and implemented it in November 2013 by giving a three-month grace period to private sectors to adopt. Unfortunately, the law excluded the public sector, which is the biggest blow to the protection of personal data that includes health data. Currently, the PDPA seems to lack comprehensiveness and needs updating as it is based on the old European Union (EU) data protection regulation. The vacuum in the current legislation could, to some extent, be mitigated through other existing legislation. Saudi Arabia, on the other hand, passed a legislation called Data Protection Law 2021 modeling the amended EU Data Protection Regulation 2018. However, the implementation of the Data Protection Law was postponed to 2024. Until the law is implemented, existing laws like the Basic Law of Governance 1992, E-commerce Law 2019, the Cloud Computing Regulatory Framework 2019, Data Protection Law 2021 and Telecommunication Law 2001 could be used to protect health data. Malaysian and Saudi Arabian law may have some weaknesses; nonetheless, the Malaysian PDPA and the Saudi Arabian Personal Data Protection Law (PDPL) have incorporated data protection principles enunciated in the EU GDPR, though they have some weaknesses that need legislative interference.

2. Objective of the study

Protection of privacy in general and health data privacy in particular have been discussed in many jurisdictions with the advent of the internet, technology and international trade. Countries like Germany followed by the EU Commission tried to provide comprehensive laws or regulations to regulate privacy. The Data Privacy Directive 2006 followed by the GDPR 2018 created a benchmark in regulating data privacy. The unfortunate effect of the EU Directive and the Regulation is that the business establishments selling goods and services, or monitoring consumer behavior should adhere to the GDPR and when the EU

residents' data are transferred to a third country, it is necessary to ensure that the third country has adequate law on data protection (GDPR, 2018).

This prompted lawmakers around the globe to come up with laws similar to EU Directive or GDPR. Malaysia passed the Data Protection Law following the 2006 Directive while Saudi Arabia enacted a law like the current GDPR. This research is an attempt to explore the data protection regime of the aforementioned two countries and draw a comparison with GDPR to see the adequacy of the law using systematic literature review (SLR), legal content analysis (LCA) and comparative analysis (CA). The contribution of this article is significant as there is a lack of comprehensive comparative studies on health data. There is also no study on the adequacy of Malaysian and Saudi Arabian laws to meet the requirement of Articles 45–46 of GDPR. Thus, this study contributes to extending the existing theoretical insights to understand the application of data protection laws in Malaysia and Saudi Arabia to meet the "adequacy" requirement under GDPR. This study further contributes to understanding the level of protection of data, efficiency, transparency and accountability of data processing. It will show how the Malaysia and Saudi Arabian laws meet the "adequacy" requirement under GDPR. The study provides short- and long-term initiatives to improve health data protection. The suggestion will help to amend the law and implement strategies to meet the needs of the stakeholders and to get access to data from EU countries.

3. Methodology

The research used SLR, LCA and CA to critically analyze the health data protection in Malaysia and Saudi Arabia in comparison with GDPR to see the adequacy of health data protection that could meet the requirement of EU data transfer requirement. Malaysia and Saudi Arabia were selected to study due to the government's action in passing data protection laws that are similar to GDPR. SLR was chosen as it allowed us to assess the available literature on the research topic and find the gap in the literature so that the article could fill the gap in the literature. The LCA was adopted in this research to assess all the possible legislation that could be applied to protect health data. This analysis helped in finding the strengths and weaknesses of the existing laws, and it became the basis for recommendations for the improvement of the legislation. Finally, the CA method was used to compare the laws of the selected countries so that the best available legislation could be taken as a benchmark to recommend legislative amendments. All these methodologies helped to achieve the objective of the study: identify the gaps in the literature, the adequacy of the law relating to health data protection and to provide suggestions to amend the law to meet the international standard on health data privacy.

The researchers systematically reviewed the literature and mapped the literature using visualization similarities. Once the literature was mapped, a scoping review framework was applied to review in detail the content of the literature to understand the nature, scope, limitation, gap and gray areas (Arksey and O'Malley, 2005). For SLR, the literature in this research was collected from journals listed in Web of Science, Scopus, Emerald, ScienceDirect, IEEE Xplore and Directory of Open Access Journals (DOAJ). Some of the literature was also collected from Google Scholar and library sources. The keywords or combination of keywords used in collecting literature are "Data Protection," "Privacy law," "Heath data," "GDPR," "Personal Data Protection Act Malaysia," "Personal Data Protection Law Saudi Arabia" and "Health Laws." The databases were searched till the year 2023 to collect data regarding the research topic. This meticulous process led to the identification of 152 scholarly publications. By using further inclusion criteria, the search was subsequently narrowed down to "privacy," "health data," "Malaysia," "Saudi Arabia" and "GDPR."

The refined search in the English language yielded a total of 52 relevant literature that were found to be relevant to the research. Later, three research materials were added to complete the analysis.

The search technique and criteria for source ensured rigorousness and high-quality search (Khan *et al.*, 2020). In the second phase of the analysis, the collected research materials were sorted, and abstracts were scanned for relevancy. If it was relevant, then full publications were logged. In the final phase, a detailed reading of 52 research materials was carried out. For LCA and LA, the researchers looked at all the relevant laws, cases, regulations and policies relating to health data privacy. Further, working papers from government and international organizations were studied to understate the development of the law and to interpret the law (Srinivasan, 2024).

4. Literature review

Technology and global connectivity create greater opportunities to advance health care. Machine learning and deep learning AI techniques are used by health-care providers, diagnostic centers and pharmacies to diagnose, conduct surgery and track patients and medications. Machine learning, for instance, is used to track medical stock and predict patients' needs based on electronic health records (EHR) (Peng *et al.*, 2021 Paul *et al.*,2023). Deep learning is highly used in diagnosing tumors and lung diseases (Ahuja, 2019, Jyotiyana and Kesswani, 2020). It is also used in cancer (lymph node metastasis and mammography malignancy) detection (Golden, 2017, Suh *et al.*, 2020, Marie-Sainte *et al.*, 2019). AI is used in detecting diabetic retinopathy (DR) among diabetic patients (Sandhu *et al.*, 2018). In the pharmaceutical industry, AI is used in drug development in the shortest period by discovering relevant molecules and determining the drug components (Gallego *et al.*, 2021; Paul *et al.*, 2021). Technology is also used to conduct robotic remote surgery and follow-up for monitoring (Papa *et al.*, 2020). Technology is found to be efficient in diagnosing the symptoms that could lead to preventing disease and reducing the cost and mortality rate. However, many users and legal advocates are concerned about the protection of patients' health data, even though the use of technology is inevitable in health care.

The EU amended its data protection regulation and came up with GDPR to protect personal data, including sensitive data like health data. In the process of providing comprehensive protection for EU residents, the GDPR imposes restrictions on non-EU organizations on data collection, access, use and transfer across borders. The previous Directive 95/46/EC regulates companies based on the territoriality principle where the only reason to be bound by the data protection directive is the physical location of an establishment or object in the EU. The GDPR, however, focuses more on the effect principle rather than the geographical location of data processing. Under the GDPR, data controllers and processors who are stationed outside the EU but offering goods or services to EU data subjects [A.3(2)(a) or monitoring people's behaviors (targeting) ((A.3(2)(b))] could be subjected to the GDPR. The interconnectivity of countries through trade, technology and corporate extension due to globalization has increased the possibility of data transfer and processing data in different countries than the country of origin of an organization. Hence, GDPR requirement is costly to many organizations.

Article 3 of the GDPR imposes an obligation on those who are processing EU citizens' data to follow the GDPR even though these companies are non-EU companies and the size, or the revenue of those companies does not count. Article 3(1) states that EU rules apply even if the processing does not take place in the EU. With the new law, the EU Commission does not need to show the link between EU establishment and the processing of data in the third country as it was shown in *Google Spain*. In *the Google Spain* case, the court stated that

the company profited through the activities in *Google Spain*, and the processing carried out in the USA was conducted in the context of the activities of *Google Spain*. Under GDPR, it is enough to show that some real activities like the sale of goods or services or the minoring of consumers are happening in the EU through stable arrangements (Azzi, 2018).

Article 3(2), which cannot be circumvented by the agreement, covers cookies, spyware, banners and tracking devices under "monitoring" of the behavior of EU people. To establish liability under this provision, it should be shown that there is data processing about goods or service offerings or monitoring of consumer behaviors (Beauvais, 2020). The monitoring activities should be apparent according to Recital 23 of the GDPR. However, it is not required to show that processing took place in an EU country (Blyth and Yazbek, 2020). Perhaps, the EU Commission or court might look at the accessibility, language and currency used in ordering goods and services to analyze the intention of the parties. It may also assess the technical steps used like the use of geolocation technologies taken by the establishment to prevent people of the EU from accessing the website (Azzi, 2018). "Monitoring" according to the GDPR involves tracking a natural person to track and predict or analyze personal attitude, behavior and preferences. Applying this provision to business activities, most businesses need to adhere to GDPR as the processing of data in their business operation could be considered monitoring because IP addresses and cookie identifiers are classified as personal data.

The extraterritorial jurisdictional effect of Article 3(2) was considered new in the area of data protection. Extraterritorial jurisdictional application of the law was not practiced, except in criminal cases or antitrust cases. International law recognizes the extraterritorial application of laws under Article 38 of the Statute of the International Court of Justice if the international convention, international custom or principles of recognized law allows such application (Svantesson, 2014). Though privacy protection has been mentioned under the UDHR and the International Covenant on Civil and Political Rights (ICCPR), it is unclear if GDPR could be considered an acceptable basis for extraterritorial application of laws (Prinsley *et al.*, 2021). It is argued that "effects doctrine" under international law could be used as a justification to extend jurisdiction beyond borders as in the antitrust cases. The court in antitrust cases accepted the arguments if it could be shown that the act has a detrimental effect (Kuner, 2010).

Some literature tends to suggest that the judiciary in applying the extraterritorial jurisdictional provisions could opt to choose the "territorial approach" or "balancing approach" besides the "effect approach" (Dodge, 1998). Application of the territorial approach requires showing that the lawfulness depends on the law of the country where the offense was committed (*American Banana Co. v United Fruit Co. "Banana"* 213 U.S. 347, 1909) and (*E.O.C. v Arabian American Oil Co*, 499 U.S. 244 (1991). Conversely, the effect approach requires showing that an offense or action committed should have a consequence to the country that is trying to extend its power beyond borders (*United States v Aluminum Co. of America ("Alcoa")* (148 F.2d 416, 65 U.S.P.Q. (BNA) 6, 1945 Trade Cas. (CCH) P57,342 (2d Cir. N.Y. Mar. 12, 1945). The balancing approach looks at the effect of an act on the state and the interest of the third country (*Timberlane Lumber Co. v Bank of America,* (574 F. Supp. 1453 (N.D. Cal. 1983) (Hixson, 1988). The GDPR approach seems to follow the balancing approach as it listed certain criteria under Art. 3 (2) to extend jurisdiction beyond borders.

The High Court of England and Wales in *Soriano v Forensic News LLC and Others* [2021] EWHC 56 (QB) analyzed Article 3 of the GDPR about a US website. In this case, a UK claimant brought an action against a US website by invoking Article 9 of the GDPR for harassment, falsehood, misuse of private information and defamation. He argued that the

"data controllers" violated his data privacy when it published articles about him. He claimed that the data was inaccurate, and the processing was unfair. The High Court approved his request for permission to serve notice to the US website for misuse of private information and defamation though it was not convinced of the prospect of success under Articles 3(1) and 3(2). In allowing notice to be served, the court mentioned that the "establishment" requirement should have a more stable arrangement like having employees or representatives or some customers. By considering Recitals 23 and 24 and the EDPB Guidelines, the website was not targeting UK customers to provide goods or services with the defendant's "core" activity. However, the English Court of Appeal disagreed with the High Court and allowed the service of notice in the USA for violation of Article 3 too. The Court of Appeal mentioned that the research about the claimant and steps taken before publishing could be considered as monitoring as such it comes within the ambit of A. 3(2)(b) (De Freitas and Matthews, 2022, Prinsley *et al.*, 2021). The extra jurisdiction effect of GDPR could be justified by looking at some international practices. However, the investigation and enforcement would be challenging. There is a need for consent and cooperation of foreign states for investigation and enforcement of non-compliance even though the companies have consented to such investigation. The absence of mutual legal assistance (MLA) will make it difficult to investigate and enforce judgment in foreign states. For instance, when the German DPA audited the credit card data of Germans in the USA, and when the Spanish DPA audited data related to data processing equipment in Colombia, it obtained the consent of the USA and Colombian governments, respectively (Kuner, 2010). After investigation, for any enforcement of sanction to be effective, the DPA needs to show the existence of a treaty, agreement or reciprocity. Further, it should also show that it is fair to enforce the sanction as per "obligation theory" under international law.

Though there might be challenges in enforcing non-compliance decisions in foreign jurisdictions, the companies are willing to comply with orders related to data protection violations. In *Aggregate IQ Data Services Ltd (AIQ) v UK's Information Commissioner's Office (ICO)*, AIQ complied with the order to cease processing of UK and EU citizens' data for political campaigns [67]. The businesses were afraid that the EU countries could implement market-destroying measures for business establishments if they failed to comply with data protection measures. These measures could include trade bans, penalization of representatives or prohibition for the use of data by way of judicial injunctions. Though the GDPR may face problems in investigation or enforcement in foreign states, GDPR has a quality that cannot be and should not be ignored (Azzi, 2018). Because such a measure would impact the reputation of the establishment negatively, the business organizations rectify the non-compliance speedily to avoid repetition of downfall. This could be seen in the *Google Spain* case as well as Facebook where they implemented GDPR in their worldwide operations. With the Cambridge Analytica scandal, many companies tried to adopt GDPR provisions to meet the market demand and create consumer trust (Pramesti and Afriansyah, 2019). Compliance with GDPR will be very challenging for small and medium industries to adopt GDPR in their operation.

Besides Article 3, which requires compliance with full data protection requirements, Chapter V rules of data transfer require an adequate level of protection. Article 45 under Chapter V of the GDPR allows the transfer of personal data to a third country with the approval of the European Commission if the third country has taken adequate measures to protect personal data. Articles 3, 45 and 46 of the GDPR provision are said to force many countries to adopt laws like GDPR so that the law could meet the requirements related to adequate law. Article 45 states that personal transfer to a third country or international organization may take place if the Commission has decided that the third country or

organization has an adequate level of protection. Subsection 2 states that the factors/requirements that the Commission will consider in assessing an adequate level of protection include the rule of law, human rights-related issues, relevant legislation, independent supervisory authority and international commitment. Article 46(1) states "that a controller or processor may transfer personal data to a third country or an international organization only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available." The appropriate safeguards are mentioned in Subsection 2. Many developing and underdeveloped countries might find resource constraints to amend the existing law or pass a data protection law that could be considered adequate. The resource constraint could take many years for these countries to meet the adequacy requirement. Applying the spirit of Article 50, the EU may assess the impact of GDPR on these countries and provide some leeway (Kuner *et al.*, 2017). Nonetheless, some other countries passed or are in the process of passing data privacy legislation to facilitate access to the EU market and meet the local needs for comprehensive legislation on data privacy. Malaysia and Saudi Arabia have passed laws that are like data protection laws in the EU.

In Saudi Arabia, Saudi Vision 2030 focuses on the diversification of the economy by achieving greater participation from local and international industries. In the process, the government has passed many laws to ensure that the law in Saudi Arabia is comprehensive. One such law is the Data Protection Law 2021. The law will protect personal data, including sensitive data like health data, while meeting the requirement of "adequate" law under Articles 45–46 of the GDPR.

In the context of health data protection, a survey conducted among 186 health practitioners working in four hospitals in Riyadh, Saudi Arabia, showed that more than 60% of the participants were using AI-related technology at work, and 90% of them confirmed the accuracy of diagnosis using AI technologies. Some of the participants in this survey expressed concern about the accuracy of data, protection of data privacy and ethical use of health data. According to the participants in the survey, when AI, deep learning or machine learning are used, large amounts of data are used to analyze, and the data input and analysis should ensure privacy. The use of anonymized data to blur data to avoid tracking the individual could be beneficial. However, transparency, purpose limitation and data minimization could be challenging to achieve if AI and other new technologies are used in providing health-care services (Chikhaoui *et al.*, 2022). Another similar survey conducted in neighboring Dubai, United Arab Emirates, found that even if there was no comprehensive legislation on health data protection, more than 80% of respondents who participated in the survey felt that data protection principles like choice, disclosure, notice, access, security, data integrity and the enforcement principles were voluntarily adopted by health care providers to build trust and confidence among the patients and other stakeholders (Sarabdeen and Moonesar, 2018).

In Malaysia, the need for comprehensive legislation to regulate personal data and sensitive data has been discussed by researchers. Regarding the need for comprehensive legislation on operationalized telehealth flagship applications, Mohan and Raja Yaacob (2004) stated that the protection of privacy could be considered one of the challenges when electronic lifetime health records are used at hospitals and homes. They stated that ensuring privacy through adequate laws and policies is necessary. The law should regulate data access and use, to detect and penalize violations. Sarabdeen *et al.* (2008) analyzed the laws regulating electronic health data protection before the passing of PDPA and found that the protection available under the Federal Constitution and other related laws could be extended to protect health data to some extent. Nevertheless, there is a need to have comprehensive

legislation on data protection. The need for separate data protection laws triggered the passing of the PDPA in 2010 and implemented in 2013. The law tends to follow the EU (2016) Directive on data protection, and the literature on health data protection shows that the PDPA lacks explanation in certain areas; as such, the law needs updating. Salleh *et al.* (2021) analyzed Sections 6 and 40 of the law and found that the consent requirement needs to be looked at in the era of the advancement of technologies. Similarly, Cieh (2013) looked at all the provisions of the PDPA to see what is covered and what is not covered under the PDPA. The analysis of the literature suggests that the consent, scope, privacy protection assessment and clarity about automation need to be updated. Sarabdeen and Mohamed Mazahir (2024) analyzed the applicability of Islamic law to protect data. They concluded that Islamic law is broad and protects all the data and confidential information. As such, passing laws to protect data privacy is in line with Islamic principles. The literature also asserted that by applying public interest policy, the governments in Muslim countries like Saudi Arabia and Malaysia are duty-bound to provide appropriate laws to protect the rights of individuals. The data protection laws are initiatives to meet the mandate of responsible government, which requires certain conditions to be fulfilled for processing of personal data (Neogi, 2021). Additionally, Articles 45–46 of GDPR push the countries to pass adequate legislation. Saudi Arabia and Malaysia responded by passing laws to meet the GDPR requirements so that local companies will have access to consumer data from EU member countries (Kuner, 2010, Almarzoqi and Albakjaji, 2021).

The literature review shows that the 2016 Directive and GDPR have a greater effect on measures taken to protect the personal data of EU residents. Some researchers studied the impact of the EU regulatory regime on businesses, the EU and other countries. Others looked at the legality and validity of the extraterritorial-jurisdiction effect of EU Directive and Regulations. The researchers also looked at the impact of the Directive and Regulation in non-EU countries. Malaysian literature looked at the current law and the problems with it, while Saudi Arabian literature tends to look at the government initiatives in providing laws to move Saudi Arabia from an oil reliance economy to a diversified economy. The literature also looked at the health practitioners' view on health data privacy in the context of technology adoption.

5. Analysis

5.1 The Malaysian health data protection laws

AI, big data, ambient intelligence, ubiquitous computing, cloud computing, international trade and globalization created vast opportunities for the health sector like any other sector. At the same time, they created some uncertainty as to data protection. Some argue that coordination with new computing technologies in a globalized environment with personal data protection became a challenge as both do not intersect well (Kuner *et al.*, 2018). Bias and discrimination in the algorithm, for instance, are difficult to eliminate as training data might have some cultural or racial information that may lead to bias or discriminatory decisions. Literature supports the proposition that the usage of newest technologies like AI locally or internationally should be used as a support system in decision-making rather than an autonomous decision-making tool that could affect human self-determination (Hoeren and Niehoff, 2018). Otherwise, it may be difficult to meet the requirements of data protection laws. As technologies in the health sector could uplift the diagnosis, delivery, research and development, appropriate transparent and resilient data protection and management systems should be developed to meet legal requirements and create trust among the patients. Such a system is necessary as the exponential data accumulation affects the trust, reliability and security of the health-care system.

The Malaysian PDPA applies to entities that process data for commercial purposes, not for government departments or public entities. The PDPA includes seven different data principles, namely, the general principle, notice and choice principle, disclosure principle, security principle, retention principle, data integrity principle and data access principle. Under PDPA, consent requirements should be met before processing data for lawful purposes. Section 6 of the PDPA further states that the data collected should be for a specific purpose. This requirement eliminates the possibility of collecting excessive data for future use. Health data is classified under Sections 3 and 6 of the PDPA as sensitive data as such collecting and processing of health data needs explicit consent to control unwanted exposure of health data that could cause irreversible harm to individuals. However, PDPA mentions that there is no need to obtain consent if the health data is processed due to a contract, for fulfilling a task assigned by the data subject, for the protection of the data subject's interest or for the administration of justice or application of law [Section 6 (2)]. If any of the data subjects want to withdraw the consent given previously, Section 38 of the PDPA allows such withdrawal if it is made in writing. The data processor or controller must stop processing data and delete all the data related to the concerned data subject if the consent is withdrawn. The technology that is used by the data controller or the health-care provider in the health-care system should cater to this adjustment or deletion of the data upon request. If the system does not facilitate it, technology could continue to use the data after consent is withdrawn. This could be considered a violation of data privacy law. Some argue that meeting the legislative requirement of consent in the face of AI, neural technologies and similar advanced technologies is very challenging (Mitrou, 2019). What is going to be even more challenging is getting explicit consent for health data as it falls within sensitive data and updating all the data if consent is withdrawn [Sections 6 (1) and 40(1)(a)] (Kesa and Kerikmae, 2020).

Minimalization is required under Sections 6(3)(c) of the PDPA as part of the personal data protection principle. Accordingly, the data processed should be adequate, not excessive for the purpose for which they were collected. This provision is concerned about the quality and the quantity of data to achieve the purpose. Technologies like AI, big data and ambient intelligence may tend to collect data on a large scale; if those data are relevant to achieving the purpose and benefiting health-care users, such collection could be considered legal. Section 7 of the PDPA of Malaysia implements a written notice requirement before collecting or processing personal data. The notice should also include the choice to opt-out if the health-care users are not willing to participate. If the processing of health data is through technologies, the explanation about the use of technology should be given clearly. However, meeting this requirement in complex technologies will be a foible, until the explainable technological system is developed. The feasible option to meet the notice principle about technology use is having appropriate and elaborative organizational measures (Belle and Papantonis, 2021).

Further disclosure of personal data for purposes other than the initially stated purpose or to any other third party is not allowed under the PDPA. However, Section 6(3)(b) allows the processing of health data for related purposes by considering the purpose of the original purpose, the expectation of the parties, the type of data and the impact of the data processing on the data subjects. The purpose limitation principle is argued to be impractical in the data-driven service sector as it limits the use and further use of data for the benefit of the patients and society. Some argue that the application of this data principle is not feasible with technologies as such legitimate interest should be the only principle that should be used as part of data processing (Moerel and Prins, 2016). Though it is challenging to meet the legal requirements in data data-driven economy, the data principle cannot be ignored.

Under PDPA, retention of data for necessary purposes is allowed. Section 10 of the PDPA imposes the retention period; however, there is no mention of the permissible retention period. What could be a reasonable period shall depend on the type of data, the purpose of collection and the need for longer retention of the data. Longer retention is only allowed for necessary purposes like public health, research and statistical purposes (Section 45, PDPA). It also requires the deletion of the data after certain use. It could be assumed to be reasonable for the purpose for which it has been collected. Though the deletion of certain data may interrupt data analytics usage in diagnosis or decision-making, it is necessary to customize the data inputs so that deleted data are not used in the final output and decision-making (Kesa and Kerikmae, 2020).

The data integrity principle in Section 11 of the PDPA requires ensuring the completeness of data when it is collected. The data collected should be current so that the data process yields accurate and fair results about a patient. Section 12 of the PDPA introduced the access principle where the data subject is given the right to access data and the right to correct inaccurate data, subject to the law. Right to information is included in Section 30 of the PDPA, and the data subject could request a copy of the personal data in intelligible form. However, the right to access a copy of legal analysis that was derived from personal data may not be considered as part of the requirement of Section 12 [*YS* v *Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel* v *M, S, Joined Cases* C141/12 and C372/12, (2014) (ECLI:EU: C:2013:838)]. However, the right to access should be read along with Section 45(2)(b) of the PDPA. Accordingly, the right to access may be denied if such access causes serious harm to the physical or mental health of the data subject or any other individual. The health minister could come up with guidance on access to data by patients, a health-care provider or any authorized representative [the Private Health-care Facilities and Service Act 1998, section 107(2)(g)].

Aside from the PDPA, the Malaysian Constitution in Articles 5(1) and 8(1) provides privacy as a fundamental right. The rights under these provisions are not absolute but qualified rights where various limitations and restrictions could be imposed. It is also possible to abolish or suspend these types of rights. For example, the protection of all health-related data during the COVID-19 pandemic was limited as part of emergency public measures, and such measures are considered constitutional under these provisions. Article 5 (1) spells out that there is no deprivation of life and personal liberty, except per the law. The judiciary in applying this provision tends to show leniency toward individual rights, freedom and the rule of law, as the meaning and value of life cannot be achieved without fundamental rights. It also ensures that any restriction on the rights, in general, should only be allowed per the law [*Andrew s/o Tamboosam v Superintendent of Pudu Prisons, Kuala Lumpur* [1976] 2 MLJ 156, 158., *Che Ani bin Itam v Public Prosecutor* (1984) 1 MLJ 113,114].

Article 8(1) of the Constitution talks about equality before the law and equal protection of the law. This provision simply means any discrimination and unequal treatment should be as per the law. Equal treatment means treating everyone in the same class the same [*Public Prosecutor v Datuk Harun bin Haji Idris* (1976) 2 MLJ 116, 118]. The combined effect of Articles 5(1) and 8(1) is that the right to privacy as a fundamental right could be recognized, and any violation should be sanctioned by law without any discrimination. Anyone who alleges discrimination should show that the discrimination alleged is unfair and brought harm to the victim [*Ahmad Tajudin bin Ishak v Suruhanraya Pelabuhan Pulau Pinang* (1997) 1 MLJ 241]. There should be fairness in the substantial and procedural law when a decision affects people's lives [*Lembaga Tatatertib Perkhidmatan Awam Hospital Besar Pulau Pinang and Anor v Utra K Permal* (2000) 3 CLJ 224].

Applying this elaboration of law in terms of freedom, fairness and non-discrimination to health data protection, it could be assumed that health data protection is one of the means that affects life, and any restriction of its protection should be by the law. The court stated that deprivation of reputation and dignity is equivalent to deprivation of life because reputation/dignity is an integral part of life. Life does not refer to mere existence, rather it includes all qualities, including the protection of personal data that ensure life is holistic *[Tan Tek Seng v Suruhanjaya Perkhidmatan Pendidikan and Anor* (1996) 1 MLJ 288].

Besides the Federal Constitution, the Telemedicine Act 1997, the Medical Act 1971 and Related Regulations can be used to protect health data in Malaysia. The decades-old Telemedicine Act covers a very narrow practice of health care, and therefore, it may protect health data collected using audio, visual and data communication only. The core principle related to health data protection is obtaining informed consent under Section 5 of the Act. The consent should be obtained after explaining the purpose of the telehealth exercise and the risk involved. The patient is given the option to opt out before and after giving the consent. Any information collected in the process of telemedicine will be kept confidential and cannot be used for purposes other than the original purpose. The use of health data for secondary purposes like medical research would require new consent from the patients. The Act imposes criminal liability for violation of the provisions related to the consent requirement. However, there is no provision under the law for civil liability.

The Medical Act 1971, which governs all medical practitioners, does not directly address the issue related to medical data protection. However, the reading of Section 34B shows that this section may be relied on in seeking some level of protection for medical data or health data privacy. According to this section, the government could be made liable for the wrongs committed by non-government medical practitioners while practicing medicine at the request of the government. This provision is very restrictive and only covers non-government medical professionals who are hired by the government and does not apply to government medical professionals. As such, this law provides immunity from legal action against a larger group of medical practitioners who are prone to breach the health data privacy of patients. Nonetheless, the *Malaysian Medical Council Code of Professional Conduct* provides some reprieve to hold all medical practitioners liable for breach of confidential information.

Section 2.22 of the Malaysian Medical Council Code of Professional Conduct states that no medical professionals shall disclose patients' data without the consent of the patients or legal justification (Puteri Nemie, 2006). Obtaining consent is not required if the disclosure is necessary for the public interest [*Public Prosecutor v Dato' Sri Anwar bin Ibrahim @ Anor* (2001) 3 MLJ 193]. The use of health data for secondary purposes like medical research, public health investigation and fund allocation is not addressed under the Code like the Medical Act 1971. The Malaysian Medical Council Code of Professional Conduct could be used to say that consent is necessary for any secondary usage if it is justifiable under the law. Section 3.6 of the Code requires medical practitioners to be careful and protect the life, dignity, health and privacy of the patients when conducting medical research (Quan *et al*, 2004). However, there is an absence of guidance on the requirements, conditions and allowable usage of health data under the Code, and there is no judicial precedent on this issue. Detailed guidance on this issue is warranted as the common law allows the ownership of medical reports to medical institutions in the absence of any contractual obligation. This position was asserted by the Canadian court, one of the common law countries, where the highest court of Canada stated that the medical records ownership vested in the medical practitioner and the medical institution [*Mclnerney v MacDonald* (1992) (2 S.C.R) 138].

The PDPA covers many aspects of health data privacy like the GDPR, though it lacks some elaboration. It could be said to be similar in content to GDPR in regulating the private health sector. However, if the health data are collected and processed by the state and federal government entities or hospitals, the data protection provided by PDPA will not be available. As such, the seven different data protection principles, namely, the general principle, notice and choice principle, disclosure principle, security principle, retention principle, data integrity principle and data access principle, will not be available for patients who are using government/public health facilities. Article 5(1) and Article 8(1), the Telemedicine Act 1997, the Medical Act 1971, related regulations and the *Malaysian Medical Council Code of Professional Conduct* could be used to protect privacy in the public sector that lacks comprehensiveness. Extending the scope of the PDPA to cover public sector organizations could provide better protection as it could protect patients in both public and private health sectors in terms of rights, and empowerment of data subjects with various rights, it will create great standardization in data protection that will lead to more accountability and trust among various stakeholders. This will also ensure that the companies gain a competitive advantage while meeting legislative requirements (Taylor, 2023). However, it is to be noted that adequate legislation and compliance with data protection come with cost and complexity in operation.

While waiting for the legislative amendment, the organizations should adopt governance to ensure health data privacy, accountability and transparency measures so that they will be able to gain patients' trust. The governance also should dictate possible risk mitigation strategies and liabilities of various parties in case of occurrences of risks (PDPC Singapore and IMDA, 2020).

5.2 The Saudi Arabian health data protection laws

Health data privacy is protected by various legislation in Saudi Arabia like Malaysia. Data Protection Law 2021 enunciates protection for data privacy. The Data Protection Law 2021 followed the EU Data Protection Regulation 2018 and integrated data protection principles for the processing of normal and sensitive personal data. Accordingly, the processing of data should be lawful, fair and transparent. The purpose should be regarded as lawful if it is necessary to protect an essential interest. In the case of sensitive data like health data, lawful purpose could mean protecting the life and vital interests of data subjects and others. Certain processing of data may serve both important grounds of public interest and the vital interests of the data subject like humanitarian, public health monitoring and natural and man-made disasters (Articles 1 and 2).

Consent is necessary for personal data collection or processing. However, obtaining explicit consent is an important criterion for health data collection. Before health-related data are collected, consent should be obtained. The consent cannot be said to be valid if the details of the data collector, the purpose of data collection, the process, storage and further processing are not explained. Because privacy is concerned about self-integrity, determination and dignity, consent to use health data will ensure that disclosure was made voluntarily with a clear understanding of the process and consequences of their action (Van Kolfschooten, 2019). The consent requirement is exempted in cases of public health, security and other related purposes (Gerke *et al.*, 2020). The data collection purpose should be directly related to the activity of the data collector and cannot be for a secondary purpose unless those secondary purposes are allowed under the law (Article 1). This requirement infuses accountability in data processing and prevents misuse. The data minimization principle allows the collection of relevant data, adequate to the activities of the data collector. Excessive collection of data is prohibited under the law, and such collection should be done

directly from the data subject unless the collection is authorized by the patients or in compliance with the law (Article 11). The law states that the data shall be accurate so that the quality of the data being collected could be ensured and inaccurate data should be corrected. When sensitive data like health is processed, the element of proportionality should be considered, and any data processing should minimize intrusion into privacy rights. The processing should be necessary, useful or beneficial for the patients (Office of Privacy Commissioner of Canada, 2017).

The collected data should be stored for a limited period and cannot be kept for longer than necessary. The data collector should be able to justify the timescale that they have put in place. However, an exception could be applied if the data will be used for archiving purposes in the public interest; statistical purposes or scientific or historical research purposes [GDPR, 5(1)(e) and Article 18 of PDPL]. Any data held in the systems requires regular updating to be current and accurate. Technologies like AI require huge amounts of data feeds for analysis, diagnosis and prediction. Amending and updating the data in those data sets will be challenging or may not be feasible. The PDPL also mentions principles related to the security, integrity and confidentiality of data; as such, it requires the adoption of appropriate security measures to control any misuse, abuse or intrusion (Article 19). To meet this requirement, it is expected to have suitable security policies and procedures and audit them at regular intervals. Anonymization is considered one of the methods where personal data may be used without compromising data privacy. However, when anonymization is applied, it should be ensured to eliminate the possibility of linking back to the data subject.

The health data should be collected directly not through a third party. This principle reflects transparency in data collection that is reflected in Article 5(1), GDPR. Transparency could be considered as part of the fairness principle, and health institutions should not ignore transparency and fairness for their asymmetric power (Aden, 2022). Transparency could help to create public agility as it shows responsible behavior of health institutions toward data privacy. Along with data principles, various rights are given to data subjects so that checks and balances can be maintained. The right to be informed, the right to access data and the right to have the data rectified play crucial roles in ensuring a balanced use of sensitive data because the data subject keeps the right to live away from intrusion to their privacy without justifiable reasons (Article 4 of PDPL). The data collector should avoid any biased decisions. If any of the decisions tend to compromise the interest of the data subject, there should be an appropriate explanation with reasons (Martinez-Martin, 2019).

While waiting for the implementation of the PDPL, the health data could be protected through the Basic Law of Governance 1992, which is considered as the Constitution of Saudi Arabia. The Basic Law protects identifiable individuals' data in Article 40. Accordingly, any illegal use or misuse could be penalized unless authorized by law. The Saudi Health-care Practice Code also could be used to protect health data. According to the code, patients' data, which was acquired during work, cannot be used without the written approval of the relevant patient. The only exception is that such use or disclosure is authorized by law. Violation of the Code is criminal, and the law is not elaborative on civil liability for misuse of health data. The Telecommunications Act 2001 and its bylaws ensure privacy by prohibiting interception and disclosure of identifiable personal information without consent [Article 37(7), (13)]. Article 23 requires the use of data for the purpose for which the consent was given. The service providers are required to take all reasonable steps to protect the privacy of data [Article 57 (1)]. The bylaw in Articles 58(2) and (3) imposes restrictions on data collection, use and process. Accordingly, the service providers cannot use the personal data without consent. Network and service providers could act as processors when

health-care providers use them. It prohibits the misuse of information or disclosure of information without prior consent. The health professionals who are working with government health-care facilities are also bound by the Civil Service Regulation 1977 where maintaining the confidentiality of information is mandatory. Whoever gets access to any information, including health data, in the course of their work should keep it confidential.

The Electronic Transaction Law 2007 and the Electronic Commerce Law 2019 could be applied to protect health data too. According to Article 1(11), electronic data include texts, codes, images, graphics, sounds or any other electronic form. All electronic data should be kept confidential according to Article 18(5), and disclosure of the data is only permitted if consented. The Electronic Commerce Law 2019 ensures personal data protection. The law imposes an obligation on the service providers to use the data for the purpose for which it was consented and collected. Further consent is necessary to process the data for other purposes. Likewise, consent is necessary to transfer data to other organizations. The need for the safekeeping of data is also emphasized under Electronic Commerce Law 2019. In addition, the retention period should be reasonable to achieve the purpose of data collection, and it should not be retained more than necessary. The law also mentioned the issues related to safe data management.

6. Results

The Malaysian PDPA and Saudi PDPL largely mirror the GDPR provisions because the GDPR and its previous directive set the benchmark for the protection of data privacy, including health data privacy. The PDPA and PDPL discuss many data principles like the need for consent, the necessity of processing data for lawful purposes, collecting data for a specific purpose and disclosure of collection. Consent is a precondition for the collection and processing of data. Before getting consent, necessary information related to data collection, processing and the use of data should be explained together with security measures taken for data safety. Though the Malaysia PDPA requirement reflects the GDPR requirements under Article 4(11), it is not detailed as the GDPR. However, this gap has been addressed in Saudi PDPL in Articles 6,10, 13 and 15. The PDPA prohibits excessive data collection under Section 6 of PDPA. The Saudi PDPL also imposes similar conditions for the collection and processing of personal data.

The consent requirement is different for sensitive data. Sections 3 and 6 of the PDPA and Article 1 of the PDPL include health data as sensitive data. The Malaysian legislation requires explicit consent to process the sensitive data. However, Article 5 of the Saudi PDPL left an explanation of the requirement of explicit consent to the regulation. The requirement of explicit consent for processing sensitive data is somewhat similar to Article 9 of GDPR, which states that health data is sensitive data, and exposure of the health data could cause the data subject to various risks. Because they are specific data, they would need special protection. The PDPA, PDPL and GDPR mention that there is no need to obtain consent if the health data is processed due to a contract, or for fulfilling a task assigned by the data subject, for the protection of the data subject's interest, the administration of justice and application of law [Section 6, PDPA, Article 6 (1–6), PDPL and Article 9 GDPR]. Article 27 of Saudi PDPL also exempts consent requirements if the data are to be used for scientific, research or statistical purposes, and the data controller meets the conditions listed under the said provision. In Saudi Arabia, it is interesting to note that the consent required could not be waived for sensitive data if the data is to be processed for the legitimate interest of the data controller [Article 6(7)].

In processing data, if automation in decision-making is implemented, this should be disclosed to the data subject. The GDPR in Articles 22, 13(2)(f) and 14(2)(g) together with

Recital 71 cover this right to information regarding automation. Additionally, it includes the right to have human interference in decision-making and the right to explanation and refusal. The PDPA does not cover automation; however, the requirement of practical and due diligence measures could be used to demand appropriate safeguards when automation is used as part of health care. The Saudi PDPL in Article 22 could be implied to cover automation as it requires the implementation of impact assessment on personal data before adopting any product or service. The challenge in the use of advanced technologies in health care is that providing detailed information on the processing of huge health data will be impractical, and the users may not be able to understand the technical information provided. Therefore, the organizational measures should provide general information that affects the patients and ensure that there is human interference in decision-making. To protect sensitive data from various risks, it is suggested that de-identification and anonymization should be used. However, de-identification and anonymization may not be fully achieved unless it is planned properly with technology and data management.

The withdrawal of consent and the aftermath of the withdrawal have been elaborated in PDPA and PDPL as in GDPR. Sections 6 and 40 of the Malaysia PDPA and Saudi PDPL in Article 5(2) allow the withdrawal of previously given consent. Section 38 of the PDPA allows such withdrawal if it is made in writing, whereas Saudi legislation leaves the details of withdrawal of consent and related issues to implementing regulation. Under PDPA, PDPL and GDPR, the data processor or controller must stop processing data and delete all the data related to the concerned data subject if the consent is withdrawn. The data protection principles try to establish accountability on the part of the data controller and processor. To meet the requirements, it became imperative for them to have the right policy for collection, processing and disclosing data.

Written notice of data collection is another requirement under Section 7 of the PDPA of Malaysia. This provision like Article 12 of the GDPR requires that the data collector, user or controller should inform the data subject that data are processed, the nature of the data and the purpose of the data processing. The Saudi PDPL in Article 13 also requires notice to be given though it did not mention if it is necessary to be written. Besides notice principles, security principles are given importance in PDPA and PDPL as in GDPR. This requires the implementation of security measures in each stage of system development so that correct action can be effectively implemented. The measure should be an acceptable international standard so that a tested and accepted system is adopted to control misuse and abuses. The appropriate technical and organizational measures should include a requirement to access data including the requirement of passwords and secure storage.

Article 35 of the GDPR mandated such measures if the processing of sensitive data has an adversarial effect on the data subject's rights. The PDPA has no explicit provision about privacy by design (PBD) or Privacy Impact Assessment (PIA); nonetheless, Sections 9(1) and 133(1)(b)(ii) could be interpreted to include privacy by design or PIA as part of practical or due diligence measures. Article 19 of the PDPL explicitly mentions that necessary organizational, administrative and technical measures should be implemented to protect personal data, which could include the implementation of privacy by design. The PDPL imposes another layer of organizational measure in terms of accessing and processing health data in Article 23. It states that the data controller shall limit the number of employees who can access the health or medical data and the access shall be allowed for necessities only. To ensure the health data are collected, processed and used as per the legal requirement, it becomes necessary to implement appropriate privacy management measures like PIA, PBD or anonymization of data. Section 48(f) of the PDPA requires the Commissioner of Data Protection to monitor the current development and develop ways to

assess the impact of data protection. Similarly, the security principle also mandates the data user, collector and processor to take the appropriate technical and organizational measures. Section 22 of the PDPA introduced a data user forum that could be monitored by the Commissioner. The data users under Section 23 are encouraged to develop a code of practice for data use. The Saudi PDPA in Article 22 also requires the implementation of impact assessment on personal data when a product or service is introduced. This measure is to see possible privacy or data protection concerns before and after adoption. Any privacy or data protection measures should be audited regularly to assess their effectiveness.

The minimization principle in PDPA like Article 5(1)(c) of the GDPR requires the collection of data for the purpose consented to, and there should not be excessive data collection. The Saudi PDPL is more detailed in this regard. Any disclosure of personal data to any party other than originally disclosed is prohibited under the PDPA, PDPL and GDPR. Article 11 of the PDPL states that the collection of data should be for a specific legally allowed purpose, and the controller should use direct, clear and secure methods in collecting data directly from the data subject. The use of data collected should not identify the data subject. Transferring data to any third party is not allowed unless a third party is assigned to do work related to the original purpose of the collection of data. This provision reflects Article 5(1)(b) of the GDPR. The Saudi PDPL, in Article 13(4) imposes additional conditions for the transfer of data to a third party who uses or processes it outside Saudi Arabia. Accordingly, it is necessary to disclose the capacity of the third party to whom the personal data are to be transferred, disclosed or processed. This will require the data controller and processor to have a detailed record of the transferee and technical, and organizational records of data collection and processing. This seems to be in line with the Recital 78 of the GDPR guidelines.

The retention principle is another principle that has been advocated as important under the data protection laws. It mandates that retention is only allowed to achieve the purpose for which the data was collected. Any extended retention should be for an allowable cause like research and statistical purposes [Article 5(1)(e), GDPR and Section 45, PDPA]. Article 18 of Saudi PDPL permits extended retention and use of the collected data provided it is allowed under the law or it is being used for a case that is being considered by the judiciary. The same provision mandates the data controller to destroy the data once the reason for the extension ceases to exist. According to Article 4, the data subject has the right to access data, correct and ask for destruction of the data if he/she does not want his/her data to be used.

7. Conclusion and recommendation

The analysis shows that the data principles and protection articulated by EU regulators have an impact on the legislative initiatives of non-EU countries. Many countries reacted by passing laws emulating the EU data protection regulation. For instance, Malaysia passed the PDPA in 2010 to address various data protection principles relating to notice, choice, disclosure, security, retention, data integrity and data access. Though the Malaysian legislation is based on the EU Directive 2006, it covers many important principles. The major drawback of the legislation lies in its scope. The legislation is only applicable to the private sector, whereas the public sector has been excluded from its coverage. Unlike Malaysia, Saudi Arabia passed the PDPL in 2021, reflecting on the GDPR 2018. The law currently covers various data principles and includes comprehensive rights to data subjects. Though the law is not elaborative on the issue of automation, a closer analysis shows that the provisions could be easily extended to cover technological means of processing data and decision-making. The Saudi 2021 law mentions the PIA in adopting or implanting products

and services. The law is set to come into force in 2024, and until then, the existing law will be able to protect personal data, including health data.

The following long- and short-term recommendations should be considered for better protection of health data privacy. The long-term recommendations are:

- The Malaysian legislature should amend the existing law so that the scope of the PDPA could be extended to include the public sector. Such an extension will provide comprehensive health data protection to all the parties. Presently, personal and health data in the public sector can only be protected through the provisions of the Federal Constitution, the Telemedicine Act and the Medical Act. However, the protection may not be similar to the one that is afforded by the PDPA 2010.
- The Malaysian legislation should also seek to accommodate technological advances and automation. It should provide express provisions on various rights of the data subject when automation. It also should require the introduction of the practice of PBD and PIA.
- The Saudi Arabian legislation should be implemented soon to provide comprehensive protection for health data.

While the laws are waiting for update and/or implementation, the following should be taken as short-term and continuous improvement measures to meet the "adequacy" requirement of GDPR *vis-à-vis* data protection laws:

- All the health-care providers, controllers and processors of health data should ensure accountability and transparency in handling and processing health data.
- Technical and organizational measures should be implemented in collecting, processing and transferring health data. These measures should help to map the data process journey.
- Organizations should also use technologies like blockchain to secure communication and data transfer in an encrypted format (Gordon and Catalini, 2018).
- To ensure accuracy, when an automated decision process is implemented, the data process should be assessed by a designated individual. Error rates across various groups should be assessed too so that bias in automation about health data could be controlled. As suggested by Gahntz (2020), it is also advisable to use a multi-stakeholder regulatory framework where various stakeholders' opinions and advice could be considered in the collection, use and processing of health data. There should be a committee that decides by a majority on critical issues related to the data process. There should be a clear policy on how consent will be solicited, the ways of collection of health data, the purpose of use, the retention period and the way the data will be destroyed.
- There should be an organizational policy on data processing and the policy should include all the requirements and conditions of data processing. They should also include the rights and liability of all the parties involved in handling health data.
- In ensuring the security of the health data, system, process and repositories, organizations should use internationally acceptable measures as systems and repositories are susceptible to malicious attacks from inside and outside. The measures should also impose an administrative requirement to train personnel who handle health data (Mikkelsen *et al*, 2020). Part of the administrative requirement includes access control, data access, encryption and anonymization. A periodical data life cycle analysis should be introduced so that weak spots and operational

risks can be detected, and measures should be taken to eliminate them (Taranto *et al*, 2020).

- Health-care providers, controllers and processors should guarantee these rights even if they process the data in a third country (Ducato, 2020). The overseas processing of data should be regulated through contractual terms and technology like blockchain, which could monitor data use and processing in real time. If the country that processes data does not have an adequate data protection law, the health-care provider or data controller should include all transfer details, transfer tools should be precise, clear and accessible data protection measures (The Guidance by the European Data Protection Board EDPB).
- The data processing measures should be implemented in proportionate to the nature of the data, and they should be audited periodically (Paulley and Kim, 2020).

The implementation of long- and short-term recommendations could cause some challenges in terms of cost and resources. Amending legislation requires a thorough study and support of various stakeholders. To overcome this, it is important to organize various awareness workshops, information sessions and support strategies that could garnish the support of various parties and could help move forward with the required amendment, implementation and adoption of the data protection law.

Implementation of comprehensive data protection measures requires an organizational change in terms of policy, design and organizational structure. Therefore, there should be adequate time given to the organization to adopt and implement all the measures. Additionally, the organization in coordination with regulators and industrial experts should organize regular training sessions to help them adopt, implement and update the legislative or policy requirements. With the technology change, there will be challenges regarding the safety measures implemented in an organization. There should be a regular review of these measures so that all the possible risks can be eliminated.

References

Aden, H. (2022), *Ethical Issues in Covert, Security and Surveillance Research, Advances in Research Ethics and Integrity*, Emerald Publishing, Vol. 8, pp. 119-129.

Ahuja, A.S. (2019), "The impact of artificial intelligence in medicine on the future role of the physician", *PeerJ*, Vol. 7, p. e7702, doi: 10.7717/peerj.7702.

Arksey, H. and O'Malley, L. (2005), "Scoping studies: towards a methodological framework", *International Journal of Social Research Methodology*, Vol. 8 No. 1, pp. 19-32, doi: 10.1080/1364557032000119616.

Azzi, A. (2018), "The challenges faced by the extraterritorial scope of the general data protection regulation", *J. Intell. Prop. Info. Tech. and Elec. Com. L*, Vol. 9, p. 126.

Beauvais, M. (2020), "GDPR brief: understanding the extraterritorial effect of the GDPR for genomic and health-related research", available at: www.ga4gh.org/news_item/ga4gh-gdpr-brief-understanding-the-extraterritorial-effect-of-the-gdpr-for-genomic-and-health-related-research-july-2020/

Belle, V. and Papantonis, I. (2021), "Principles and practice of explainable machine learning", *Frontiers in Big Data*, Vol. 4, p. 688969, doi: 10.3389/fdata.2021.688969, PMID: 34278297; PMCID: PMC8281957.

Blyth, T. and Yazbek, J. (2020), "Does the EU's general data protection regulation have extra-territorial effect?", Digital Governance, Cyber and Privacy, available at: www.cbp.com.au/insights/insights/2020/november/does-the-eu%E2%80%99s-general-data-protection-regulation-h

Chikhaoui, E., Alajmi, A. and Larabi-Marie-Sainte, S. (2022), "Artificial intelligence applications in healthcare sector: ethical and legal challenges", *Emerging Science Journal*, Vol. 6 No. 4, pp. 717-738.

Cieh, E.L.Y. (2013), "Personal data protection act 2010: an overview analysis", in Edwing L., Yong, I. and Noriswadi, C. (Eds), *Beyond Data Protection*, 1st ed., Springer, pp. 55-58.

De Freitas, I. and Matthews, A. (2022), "Ruling threatens to extend the extra-territorial reach of GDPR", Insight, available at: www.farrer.co.uk/news-and-insights/ruling-threatens-to-extend-the-extra-territorial-reach-of-gdpr/

Dodge, W.S. (1998), "Extraterritoriality and conflict-of-laws theory: an argument for judicial unilateralism", *Harvard International Law Journal*, Vol. 39, available at: https://ssrn.com/abstract=2712013

Ducato, R. (2020), "Data protection, scientific research, and the role of information", *Computer Law and Security Review*, Vol. 37, pp. 1-16.

Gahntz, M. (2020), "Regulating the use of facial recognition technology Kennedy school review", available at: https://ksr.hkspublications.org/2020/09/02/regulating-the-use-of-facial-recognition-technology/1/1

Gallego, V., Naveiro, R., Roca, C., Ríos Insua, D. and Campillo, N.E. (2021), "AI in drug development: a multidisciplinary perspective", *Molecular Diversity*, Vol. 25 No. 3, pp. 1461-1479, doi: 10.1007/s11030-021-10266-8.

Gerke, S., Shachar, C. and Chai, P.R. (2020), "Regulatory, safety, and privacy concerns of home monitoring technologies during covid-19", *Nat Med*, Vol. 26 No. 8, pp. 1176-1182.

Golden, J.A. (2017), "Deep learning algorithms for detection of lymph node metastases from breast cancer helping artificial intelligence be seen", *JAMA*, Vol. 318 No. 22, pp. 2184-2186, doi: 10.1001/jama.2017.14580.

Gordon, W.J. and Catalini, C. (2018), "Blockchain technology for healthcare: facilitating the transition to Patient-Driven interoperability", *Computational and Structural Biotechnology Journal*, Vol. 16, p. 224.

Hixson, K. (1988), "Extraterritorial jurisdiction under the third restatement of foreign relations law of the United States", *Fordham International Law Journal*, Vol. 12 No. 1, p. 128, available at: https://ir.lawnet.fordham.edu/ilj/vol12/iss1/6

Hoeren, T. and Niehoff, M. (2018), "Artificial intelligence in medical diagnoses and the right to explanation", *European Data Protection Law Review*, Vol. 4 No. 3, pp. 308-319.

Hynes, M. (2021), "The social, cultural and environmental costs of hyper-connectivity: sleeping through the revolution", Emerald Publishing, pp. 85-102, available at: http://creativecommons.org/licences/by/4.0/legalcode

Jyotiyana, M. and Kesswani, N. (2020), "Deep learning and the future of biomedical image analysis", in Dash, S., Acharya, B., Mittal, M., Abraham, A. and Kelemen, A. (Eds), *Deep Learning Techniques for Biomedical and Health Informatics. Studies in Big Data*, Vol 68, Springer, Cham, doi: 10.1007/978-3-030-33966-1_15.

Kesa, A. and Kerikmae, T. (2020), "Artificial intelligence and the GDPR: inevitable nemeses?", *TalTech Journal of European Studies*, Vol. 10 No. 3, pp. 67-90.

Kuner, C. (2010), "Data protection law and international jurisdiction on the internet", *International Journal of Law and Information Technology*, Vol. 18 No. 3, pp. 227-247, doi: 10.1093/ijlit/eaq004.

Kuner, C., Cate, F.H., Lynskey, O., Millard, C. and Ni Loideain, N. (2018), "Expanding the artificial intelligence-data protection debate", *International Data Privacy Law*, Vol. 8 No. 4, pp. 289-292, doi: 10.1093/idpl/ipy024.

Kuner, C., Dan Jerker, S.B., Cate, F.H., Lynskey, O., Millard, C. and Ni Loideain, N. (2017), "The GDPR as a chance to break down borders", *International Data Privacy Law*, Vol. 7 No. 4, pp. 231-232.

Marie-Sainte, S.L., Saba, T., Alsaleh, D. and Alamir Alotaibi, M.B. (2019), "An improved strategy for predicting diagnosis, survivability, and recurrence of breast cancer", *Journal of Computational and Theoretical Nanoscience*, Vol. 16 No. 9, pp. 3705-3711, doi: 10.1166/jctn.2019.8238.

Martinez-Martin, N. (2019), "What are important ethical implications of using facial recognition technology in health care?", *AMA J Ethics*, Vol. 21 No. 2, pp. 180-187.

Mikkelsen, D., Soller, H. and Strandell-Jansson, M. (2020), "Privacy, security and public health in a pandemic year", available at: www.mckinsey.com/business-functions/risk/our-insights/privacy-security-and-public-health-in-a-pandemic-year#

Mitrou, L. (2019), "Data protection, artificial intelligence and cognitive services: is the general data protection regulation (GDPR), artificial Intelligence-Proof"?", *SSRN Electronic Journal*, available at: https://papers.ssrn.com/abstract=3386914 (accessed 4 July 2023).

Moerel, L. and Prins, C. (2016), "Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of big data and the internet of things", *SSRN Electronic Journal*, available at: https://ssrn.com/abstract=2784123 (accessed 10 July 2023).

Mohan, J. and Raja Yaacob, R. (2004), "The Malaysian telehealth flagship application: a national approach to health data protection and utilisation and consumer rights", *International Journal of Medical Informatics*, Vol. 73 No. 3, pp. 217-227.

Office of Privacy Commissioner of Canada (2017), "16-17 Annual report to parliament on the personal information protection and electronic documents act and the privacy act", available at: www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1

Papa, A., Mital, M., Pisano, P. and Del Giudice, M. (2020), "E-health and wellbeing monitoring using smart healthcare devices: an empirical investigation", *Technological Forecasting and Social Change*, Vol. 153, p. 119226, doi: 10.1016/j.techfore.2018.02.018.

Paul, D., Sanap, G., Shenoy, S., Kalyane, D., Kalia, K. and Tekade, R.K. (2021), "Artificial intelligence in drug discovery and development", *Drug Discovery Today*, Vol. 26 No. 1, pp. 80-93, doi: 10.1016/j.drudis.2020.10.010.

Paul, M., Maglaras, L., Ferrag, M.A. and Almomani, I. (2023), "Digitization of healthcare sector: a study on privacy and security concerns", *ICT Express*, Vol. 9 No. 4, pp. 571-588, doi: 10.1016/j.icte.2023.02.007.

Paulley, S.J. and Kim, K.H.A. (2020), "Why the guidance on international transfer of data post schrems II doesn't offer as much comfort as we'd hoped", available at: www.mondaq.com/canada/privacy-protection/1016664/why-the-guidance-on-international-transfer-of-data-post-schrems-ii-doesn39t-offer-as-much-comfort-as-we39d-hoped

PDPC Singapore and IMDA (2020), "Model artificial intelligence governance framework second edition", 129, available at: www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf

Peng, X., Long, G., Shen, T., Wang, S. and Jiang, J. (2021), "Self-attention enhanced patient journey understanding in healthcare system", *Lecture Notes in Computer Science*, pp. 719-735, doi: 10.1007/978-3-030-67664-3_43.

Pramesti, I. and Afriansyah, A. (2019), "Extraterritoriality of data protection: GDPR and its possible enforcement in Indonesia", Advances in Economics, Business and Management Research, 3rd International Conference on Law and Governance (ICLAVE 2019), pp. 3-130, doi 10.2991/aebmr.k.200321.012

Prinsley, M.A., Yaros, O., Vanryckeghem, V., Randell, R., Hajda, O. (2021), ("English high court considers limits of the extraterritorial reach of the GDPR in relation to an overseas website", available at: www.mayerbrown.com/en/perspectives-events/publications/2021/02/english-high-court-considers-limits-of-the-extraterritorial-reach-of-the-gdpr-in-relation-to-an-overseas-website

Puteri Nemie, J.K. (2006), "Medical confidentiality against disclosure in the public interest: should such protective privilege end when public peril begins?", *Malayan Law Journal*, pp. xxxv- xliii.

Quan, Y.K., *et al* (2004), *The Essential of Medical Law*, Sweet &Maxwell Asia, Singapore, p. 21.

Salleh, S.N.F.A., Manap Naura, A. and Rahman, R. (2021), "Big data in Malaysia: the adequacy of consent principle under data protection act 2010", International Tuanku Jaafar Conference 2021, *Universiti Kebangsaan Malaysia*.

Sandhu, H.S., Eltanboly, A., Shalaby, A., Keynton, R.S., Schaal, S. and El-Baz, A. (2018), "Automated diagnosis and grading of diabetic retinopathy using optical coherence tomography", *Investigative Ophthalmology and Visual Science*, Vol. 59 No. 7, pp. 3155-3160, doi: 10.1167/iovs.17-23677.

Sarabdeen, J. and Moonesar, A.I. (2018), "Privacy protection laws and public perception of data privacy: the case of Dubai e-health care services", *Benchmarking: An International Journal*, Vol. 25 No. 6, pp. 1883-1902.

Srinivasan, R. (2024), "Content analysis technique in legal Research- A critique", available at: www.commonlii.org/in/journals/NLUDLRS/2012/66.pdf#:~:text=Content%20Analysis%20is%20a%20scientific%20study%20of%20the,particular%20subject%20and%20reading%20it%20consistently%20and%20systematically

Suh, Y.J., Jung, J. and Cho, B.J. (2020), "Automated breast cancer detection in digital mammograms of various densities via deep learning", *Journal of Personalized Medicine*, Vol. 10 No. 4, p. 211, doi: 10.3390/jpm10040211.

Taranto, L., De Ampuero, S., Navarro, P. and Wenzel, A. (2020), "Key privacy considerations for covid-19 clinical trials", *COVID-19 Exit Strategy. A Global Privacy and Cybersecurity Guide*, Hogan Lovells.

Taylor, E. (2023), "Advantages and disadvantages of GDPR. The knowledge academy", available at: www.theknowledgeacademy.com/blog/advantages-and-disadvantages-of-gdpr/

Van Kolfschooten, H. (2019), "EU coordination of serious Cross-Border threats to health: the implications for protection of informed consent in national pandemic policies", *European Journal of Risk Regulation*, Vol. 10 No. 4, pp. 635-651.

Svantesson D.J.B. (2014), "The extraterritoriality of EU data privacy law – its theoretical justification and its practical effect on U.S. Businesses", *Stanford Journal of International Law*, Vol. 50, pp. 53-102.

Further reading

Kim, H.S., Kim, D.J. and Yoon, H.K. (2019), "Medical big data is not yet available: Why we need realism rather than exaggeration", *Endocrinology and Metabolism*, Vol. 34 No. 4, p. 349, available at: http://pmc/articles/PMC6935779/ (accessed 21 July 2023).

Regulation (EU) (2016), "679 Of the European parliament and of the council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing directive 95/46/EC (general data protection regulation), OJ 2016 L 119/1".

Sarabdeen, J. and Ishak, M.M. (2024), "Compliance of Saudi Arabian personal data protection law 2021 to Islamic principles of privacy", *Migration Letters*, Vol. 21 No. 4, pp. 726-737, available at: https://migrationletters. com/index.php/ml/article/view/7684

Corresponding author

Jawahitha Sarabdeen can be contacted at: jsarabdeen@psu.edu.sa