NAVIGATING THE DICHOTOMY BETWEEN BIG DATA AND HEALTH DATA PRIVACY IN THE PURSUIT OF SDG

[i*]Siti Nur Farah Atiqah Binti Salleh & [ii]Nur Mohd Iqzuan bin Samsudin

[i*]Jabatan Undang-undang, UiTM Cawangan Melaka, Kampus Alor Gajah, 7800 Alor Gajah, Melaka, Malaysia.

[ii]Fakulti Undang-undang, Governan dan Hubungan Antarabangsa, Universiti Islam Melaka, 78200 Melaka, Malaysia.

*Corresponding author: sitinurfarah@uitm.edu.my

ABSTRACT

The dichotomy between big data technology and the protection of health data privacy arises when the extensive use of big data becomes essential for innovation and economic development in achieving the Sustainable Development Goals (SDGs). While big data has been recognised as a critical tool in advancing healthcare delivery and public health decision-making, its application has simultaneously generated legal concerns relating to the protection of sensitive health data. In Malaysia, the implementation of large-scale health data initiatives, such as the Malaysian Health Data Warehouse, has intensified public and civil society concerns regarding the adequacy of existing data protection safeguards. This article examines the tension between the right to health data privacy and the application of big data technologies through a doctrinal legal research methodology grounded in a human rights perspective. The study adopts a structured doctrinal approach comprising: (i) a historical analysis of the evolution of data protection law in response to technological developments; (ii) a jurisprudential examination of privacy and data protection as fundamental rights; (iii) a statutory analysis of Malaysia's Personal Data Protection Act 2010 (PDPA) to assess its capacity to protect health data in the context of big data processing; and (iv) a comparative legal analysis of the European Union's General Data Protection Regulation (GDPR) as a reference framework for health data governance. This article finds that the current Malaysian data protection framework exhibits structural limitations in addressing large-scale and data-driven health technologies, particularly in relation to sensitive health data. It concludes that core principles of data protection law—such as lawfulness, purpose limitation, transparency, accountability, and risk-based governance—offer a practical legal model for harmonising health data privacy with big data applications. These principles, as reflected in the GDPR, may serve as a useful reference for Malaysia and other jurisdictions in resolving the legal dichotomy between technological advancement and the protection of fundamental rights in pursuit of the SDGs by 2030.

Article history:
Submission date: 27 November 2025
Received in revised form: 30 December 2025
Acceptance date: 08 April 2026

Keywords:
Big Data, health data privacy, SDG, data protection law, Malaysia, GDPR.

Funding:
This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Competing interest:
The author(s) have declared that no competing interests exist.

Cite as:
Salleh, S. N. F. A., & Samsudin, N. M. I. (2026). Navigating the Dichotomy between Big Data and Health Data Privacy in the Pursuit of SDG. *Current Legal Issues*, *8*(1), 6-18.

INTRODUCTION

Big data has been part of the sustainable development agenda. The importance of big data, i.e., the analytical processing of various data for the purpose of development and preparing for the upcoming global challenges, has been made clear in various papers prepared by the United Nations (UN), such as Big Data for Development: A

Primer, Big Data for Development: Challenges & Opportunities and Big Data for Development and Humanitarian Action: Towards Responsible Governance. From the technological perspective, big data is currently the new way to gain insights that can accelerate progress toward the SDGs. The UN started working on big data and has been promoting data revolution ever since.

Although Malaysia has not expressly framed its engagement with big data as part of a formal commitment to the United Nations' big data agenda, its policy initiatives and institutional actions demonstrate a clear governmental commitment to data-driven development in support of the SDGs. This is evidenced by the integration of big data analytics into the public healthcare sector, including national initiatives such as the Malaysian Health Data Warehouse, as well as broader governmental efforts to modernise data governance and digital infrastructure in pursuit of sustainable development objectives. Nevertheless, it is unclear whether the data protection law is ready to face this challenge. In particular, concerns arise from the limited applicability of the PDPA 2010 to public sector entities, the absence of specific provisions governing large-scale and secondary uses of health data, and the lack of enforceable data subject rights and oversight mechanisms in public health data processing. This has resulted to the conflict of dichotomy between big data and health. It arises when the application of big data is needed for innovations and the economy to achieve the SDGs. Health data is not only a powerful tool, but it is also very helpful in decision making by governments, health care providers and researchers.

Malaysia is actively involved with the mission to achieve SDG by 2030. The application of big data and data had already penetrated the Malaysian health sector. Among the earliest initiatives highlighting the use of big data in Malaysia's healthcare sector is the Malaysian Health Data Warehouse (MYHDW) established by the Ministry of Health in 2017. While MYHDW represents a significant move towards data-driven healthcare governance, it raises substantive legal concerns rather than merely social or public apprehension. From a legal standpoint, the primary issue lies in the limited scope of the Personal Data Protection Act 2010 (PDPA), which does not apply to federal and state government authorities. As MYHDW operates within the public healthcare system, the large-scale collection, aggregation, and secondary use of sensitive health data fall outside the statutory safeguards imposed on private sector data controllers.

This exclusion creates a regulatory and accountability gap, whereby health data processed by public authorities are not subject to equivalent legal standards concerning consent, purpose limitation, data minimisation, transparency, and enforceable data subject rights.[8,22] Moreover, the centralisation of health data under MYHDW heightens legal risks associated with re-identification, function creep, and secondary use of data, in the absence of a comprehensive statutory framework governing oversight, remedies, and proportionality. Accordingly, MyHDW is legally problematic not merely because it has generated public concern, but because it operates within a fragmented data protection regime that lacks uniform and enforceable legal safeguards for sensitive health data. Since there is a need to develop a centralised health analytic system for analysis and reporting. However, issue arises as to whether data will not be compromised.

Data protection law is known as branch of law that deals with personal data protection which relates to personal data processing and as a legal standard in matters related to personal data processing. The Malaysian data protection law known as Personal Data Protection Act 2010 (PDPA) is the sole Act to regulate the processing of personal data involved in commercial transactions. When it was first

gazetted in 2010, it was considered as a comprehensive law dealing with personal data. Moreover, the spirit of PDPA was influenced by Data Protection Directive and incorporates the human rights value and jurisprudence of the European Union (EU) data protection law. However, the main question here is does the health data privacy of data subjects as a consumer and individuals will be protected? Is it comprehensive enough to tackle big data?

Thus, this study, which is mainly motivated by the concern of data privacy rights and the usage of big data, would like to address this legal issue accordingly. Whilst big data has been considered the right technology to be applied in health sector, health data became the main sources to ignite this technology. It is essential for improving healthcare delivery and healthcare development in the health sector. Big data and health data are become the vital element to big data can be used to process health data and obtain the results needed in healthcare. It draws the attention of different groups from healthcare companies, organisations and individuals to extract its potential or harms specifically to the privacy of individuals.

This research aims to analyse the dichotomy between the rights to privacy of health data within the application of big data. The methodology applied in this study is the doctrinal legal analysis based on a human rights perspective. For this purpose, the EU's General Data Protection Regulation (GDPR) will be analysed to determine the legal approach taken in the attempt to harmonise this new technology and privacy. This jurisdiction was chosen as a case study based on two important facts: i) the jurisprudence framework on data protection law is proven to be suitable as a model for other countries including Malaysia, and ii) the preparation taken by the EU in terms of its legal approach could be adopted in facing the advancement of big data technology and its application in health. The main contribution of this study is to address the needs to improve the data protection law in Malaysia to strengthen data subjects' protection of their health data privacy.

LITERATURE REVIEW

Big data has started as a phenomenon associated with the exponential data productions through various sources. Big data is large volumes of high-velocity, complex, and variable data that require advanced techniques and technologies to capture, store, distribute, manage, and analyse information. The three V's that stands for the extreme volume of data, the wide variety of data types, and the speed with which the data can be processed, have always been used to define big data in the form of characters. The Big Data Value Association defines big data in health as "high volume, high diversity biological, clinical, environmental, and lifestyle information collected from single individuals to large cohorts in relation to their health and wellness status at one or more time points." As more data is generated and referred to as big data in popular literature, its application becomes more widespread.[2]

Big data in healthcare could be concluded as a growing collection of data from various sources, technologies techniques and procedures rather than a mere phenomenon. It is not just a single concept where data is rapidly collected and produced.[12]

The United Nations has addressed the application of big data and emphasised on the significance of big data, highlighting how it aids in decision-making to better gauge progress towards the SDGs and provides insight into the well-being of individuals and vulnerable groups.[1] The implementation of big data and health-monitoring technologies is actually in line with the SDG 3 relating to good health and well-being.[2] The significance of health and well-being can be evaluated owing to the extensive implementation of large-scale health data platforms and intelligent health

monitoring equipment. Numerous research in the literature have examined the strong integration between big data related technologies and health and well-being.

Nevertheless, literatures also suggested that the application of big data will jeopardise health data privacy. Based on research conducted by Information Commissioner Officer (ICO) in 2013 to 2014, the processing of personal data in big data, in the manner of data processing including collections and analysis, there are risk that could triggered the privacy of such data. Big data has made it possible to re-identification, making the data identifiable again. In research published in Nature, the researchers successfully re-identified an individual's identity using a statistical model. The research demonstrated that more than 95% of reidentified data is accurate and leads directly to individuals' identifiable information.[3] Finding a balance between big data utilisation and health data privacy is legally challenging due to doctrinal limitations within existing data protection frameworks. Traditional data protection principles such as informed consent, purpose limitation, and data minimisation—are premised on identifiable, finite, and purpose-specific data processing. In contrast, big data analytics in the health sector rely on continuous data aggregation, secondary use, and predictive analysis, often beyond the original context of data collection. This creates legal uncertainty as to the validity of consent, the scope of lawful processing, and the effectiveness of safeguards such as anonymisation, particularly where re-identification remains technically feasible. As a result, existing legal doctrines struggle to reconcile the demands of data-driven innovation with the protection of fundamental privacy rights in healthcare.[4]

The existing data protection law in Malaysia is primarily addresses the relatively stable phases of data.[5] However in the realm of big data, data undergoes a continual cyclical process. This process involves the interconnection, aggregation, anonymization, de-anonymization, and subsequent pseudonymization of data.[6] This implies that data are not collected and processed at the individual level, but rather processed by aggregating the data to establish generic patterns for statistical and group profiles.

Big data also helps data users to detect prototypes and inclinations to health data. The advent of big data makes it possible for companies to make sense of data that was previously invisible or not explicitly intended in the original data source.[7] Big data application could be making use of data while becoming a re-user of data. This has challenged the purpose limitation principle under data protection law.[8] Under this principle, companies employing collected personal information for predictive analysis must ensure that such analysis is consistent with the purpose for which the data was initially collected.

Rubinstein also argued that big data had challenged the very core principle of data protection law through re-identification of data because it will not only weaken the practice of anonymisation of data, which is a security measure applicable to not only personal data but also sensitive personal data.[9] She added that big data had broader impact towards data protection law by disrupting the core principle of consent and transparency.

Other scholars demonstrate that anonymisation alone is increasingly insufficient to exclude data from the scope of data protection law, especially where data processing creates specific risks to fundamental rights through the purpose or result of processing rather than merely its content.[9]

The human-rights approach is similar to the concept of human-rights based approach by the UN. This is because the European Union (EU) and the UN share the same fundamental values and goals.[10] In the context of SDGs, the EU countries are independent members of the UN. Initially, the human-rights approach only covers

matters relating to human rights in the context of privacy and access to health. The challenge to data privacy is different from what we have today, especially in the context of big data and health data privacy.

The EU and the UN realised that new technologies had become a challenge and that it was important to safeguard and use data in a secure manner.[1,2] This approach has crept into the context of humans and data. Hence, the human-rights based approach to data was introduced in 2018 with a set of principles namely, participation, data disaggregation, self-identification, privacy and accountability.[11] Therefore, it is of utmost importance for healthcare organizations to effectively handle and secure personal information, as well as fulfil their obligations and legal liabilities for the processing of personal data, to navigate through the complicated structure of data protection laws and to improve the protection of privacy of data subject.[12]

METHODOLOGY

This study employs a doctrinal legal research methodology centred on the legal doctrine of data protection law, complemented by a thematic analysis of big data and health data privacy. The thematic analysis is conducted through a library-based and document-based search, whereby relevant literature is organised into three key themes: big data and privacy law, health data privacy and the Sustainable Development Goals (SDGs), and big data and health data privacy.

In line with the doctrinal research method, the study undertakes a statutory analysis and interpretation of the PDPA 2010 to determine the extent to which existing legal provisions safeguard health data privacy in the context of big data processing. This analysis is further supported by a comparative legal examination of the General Data Protection Regulation (GDPR), which serves as a benchmark for contemporary data protection standards. Relevant judicial decisions and regulatory principles are also examined to elucidate the application of data protection doctrines to large-scale and technologically driven health data processing.

FINDINGS AND DISCUSSIONS

Sustainable development has gained popularity in policy-oriented research as an expression of what public policies should accomplish. It is a concept that refers to meeting the needs of the present without compromising the ability of future generations to meet their own needs. The concept of sustainable development has related to the long-term stability of the economy and environment. It is a holistic approach that seeks to strike a balance between economic, social, and environmental factors, which form the pillars on which the concept of sustainable development was built to create a sustainable future for all. The sustainable development goals can only be realised by incorporating and acknowledging the three pillars throughout the decision-making process.

Two significant keywords contained in the phrase sustainable development brings different definitions if it were to be define separately. Sustainable refers to studying the relationship between economic development, environmental quality, and social equity.[13]

On the other hand, development is etymologically defined as the internal process of expanding and growing. [14] The Brundtland Commission is frequently cited for a more definitive definition of sustainable development. According to the commission, sustainable development must be based on governments' political will as critical economic, environmental, and social decisions are made.[15]

The SDGs are inextricably linked to the concept of sustainable development.[16] They represent a shared vision for a sustainable future and provide a framework

for action to promote sustainable development. The SDGs are a set of 17 global goals established by the UN to promote sustainable development by addressing global challenges.[17] Generally, it covers a range of areas, including poverty, hunger, health, education, gender equality, clean water and sanitation, affordable and clean energy, decent work and economic growth, industry, innovation and infrastructure, reduced inequalities, sustainable cities, and communities, responsible consumption and production, climate action, life below water, life on land, peace, justice, and strong institutions, and partnerships for the goals.[18]

Goals pertaining to health is placed under SDG 3. SDG 3 focuses on well-being and good health, which include using health data to achieve the goals. To attain the overarching objective of good health, it is imperative to accomplish universal health coverage (UHC) and ensure access to high-quality healthcare. This helps them to monitor progress and implement targeted interventions to achieve the outlined objectives of Goal 3 of the SDGs. The effective use of health data is therefore crucial for promoting worldwide health and ensuring well-being for all people. The UN recognised that the application of big data is significant for the development of health globally.[19] As a result, the UN has highlighted the need for a balance between the risks and benefits of big data and data privacy.[20]

In Malaysia, the effort is currently taking place to achieve the goals of SDG and balancing the dichotomy between health data privacy and big data.[21] The PDPA is applicable to health sectors but not extended to the government and state health sectors.[22] For instance, Although the PDPA applies to the processing of personal data in the health sector, section 3 of the PDPA expressly excludes its application to the Federal Government and State Governments. As a result, public healthcare institutions, which function as primary collectors and processors of large volumes of health data, are not subject to the statutory obligations imposed on private sector data users.

This statutory exclusion has attracted legal criticism because it creates an uneven regulatory framework in which private healthcare providers are bound by consent, purpose limitation, and accountability requirements, while public healthcare authorities operate outside these enforceable legal safeguards. Given the scale and sensitivity of health data managed by government and state healthcare institutions, this legislative gap raises serious concerns regarding the adequacy of Malaysia's data protection framework in addressing big data–driven health initiatives.

This limitation has also drawn criticism because the government and state healthcare manage massive amounts of data and serve as the primary data collector.[23] The Malaysian Health Data Warehouse 2017 is a living proof of an imbalance protection of privacy for health data. The justification behind this due to the fact that health data is not only collected from government healthcare sector but also private healthcare sector.[24] While the PDPA is applicable to the private healthcare sector, this indicate there is unfair treatment towards how the data will be protected. The lack of legal standard in Malaysia with regards to data protection law has called for a reference to be made to the closest example of law in the EU.

The Data Protection Directive has traditionally rooted its human-rights obligations within its legislative framework. This human rights obligation has become essential in dealing with human rights matters.[25] It is a conceptual framework for the process of human development that is operationally oriented toward human rights protection and promotion.[26] Privacy rights have been elevated to fundamental human rights in most international laws, including the 1948 Universal Declaration of Human Rights and the 1966 International Covenant on

Civil and Political Rights. Article 8 of the European Convention on Human Rights establishes that the EU is one of the few governments in the world that protects individuals' rights to privacy, particularly regarding personal data.

Data Protection Directive with the GDPR, which came into force in 2018 in response to emerging challenges posed by advanced digital technologies. Under the GDPR, personal data including sensitive categories such as health data, are afforded enhanced protection through stricter obligations imposed on data controllers and processors.

Although international case law specifically addressing big data analytics in the health sector remains limited, the jurisprudence of the Court of Justice of the European Union (CJEU) has consistently affirmed that data protection constitutes a fundamental right, particularly where data processing poses risks to individual autonomy and dignity. In *Digital Rights Ireland Ltd v Minister* for Communications, the Court emphasised that large-scale and systematic data processing may seriously interfere with the rights to privacy and data protection, even in the absence of direct individual harm.[26] Similarly, in *Breyer v Bundesrepublik Deutschland*, the Court adopted a broad interpretation of identifiability, recognising that data may remain personal where re-identification is reasonably possible through technological means.[26]

More recently, in *Nowak v Data Protection Commissioner,* the CJEU confirmed that the concept of personal data must be interpreted expansively to include information that may affect an individual's rights or interests, thereby reinforcing the relevance of data protection law beyond traditional notions of secrecy or confidentiality.[26] Collectively, these cases provide an important jurisprudential foundation for the application of the GDPR to health data, particularly in contexts involving large-scale data aggregation and analytics.

Due to the emerging challenges from new technologies, the EU took the steps to amend the directives and releasing General Data Protection Regulation (GDPR) in 2018. Under this new regulation, the law can be used in various ways to protect the safety and privacy of personal information, including health.

The GDPR appears to be significantly more equipped to address the issues of protecting personal health data in the digital health era.[27] It aims to define the rights and protection of personal health data in digital healthcare and gives people better rights and more control over their health data. For example, the GDPR initially provides a more detailed definition of "data concerning health" than was previously provided, referring to personal information about a natural person's physical or mental health, including information about that person's past, present, or future health status that was gathered during the registration process for or delivery of healthcare services to that person.[28] Most crucially, it creates new health-related data protection rules and toughens the obligations of data controllers and processors.

Before processing sensitive health information, data controllers must perform data protection impact assessments to identify any potential hazards and create solutions. Some rules under Articles 12, 13, 22, and 29 attempt to make patients more aware of the logic behind data processing and the decisions taken by automated processing, including profiling, as well as the results.[29]

In the application of big data in processing health data for the purpose of decision-making, it is important for patients or individuals to be informed as to what extent their data will be subjected to algorithms. It is usually hard to tell because of the uncertainty of such decision-making techniques. However, under the GDPR, patients are given this opportunity to exercise human intervention in the decision-making process because the risks

associated with using decision-making algorithms are transparent to them.[30]

Confidentiality and privacy are critical to developing and sustaining a successful and respected treatment relationship. It has societal value because it promotes open discussion of health-related issues between professionals and patients.

Physicians must maintain the confidentiality of information provided by patients or obtained during professional interactions with patients. The GDPR laid out the general principle of confidentiality, and integrity stated in Article 5. In the event of a data breach, and if the breach poses a high risk to patients For example, in the event of a personal data breach involving health data, Articles 33 of GDPR, imposes explicit notification obligations on data controllers under Articles 33 and 34. Article 33 GDPR requires the data controller to notify the competent supervisory authority without undue delay and, where feasible, not later than 72 hours after becoming aware of the breach, unless the breach is unlikely to result in a risk to the rights and freedoms of natural persons. The notification must include, inter alia, the nature of the personal data breach, the categories and approximate number of data subjects affected, the likely consequences of the breach, and the measures taken or proposed to mitigate its adverse effects.

Article 34 GDPR further strengthens the protection of data subjects by mandating that, where a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data controller must communicate the breach directly to the affected data subjects without undue delay. This communication must be clear and plain, describing the nature of the breach, its potential consequences, and the remedial actions taken, including advice on steps that individuals may take to protect themselves. In the context of health data, these two articles mandate that the data controller notify the supervisory authority when there is a breach of data.

The EU realised the challenge brought by new technology to the data protection law, including privacy in health.[31] The GDPR could become a standard for data protection law in Malaysia in facing the legal challenge of health data privacy to achieve SDGs. The human-rights approach applied and embedded within the legal framework of data and the shared understandings of the EU, and the United Nations could be an example.

The GDPR could be a relevant reference for Malaysia. Based on the discussion, we found that the GDPR prioritises the legal use of health data in big data which involves implementing strict privacy protections and data governance frameworks to ensure that individuals' data is used legally, and the risk of privacy harm is lessened.

CONCLUSION

The United Nations has increasingly relied on big data as a strategic tool to support the achievement of the Sustainable Development Goals (SDGs) by 2030. Nevertheless, the utilisation of big data in the healthcare sector has exposed persistent legal challenges relating to the protection of health data privacy. Given the sensitive nature of health data, which often involves intimate and identifiable personal information, the extensive processing and aggregation of such data pose heightened risks to individual privacy and autonomy. This study demonstrates that the application of big data in healthcare inevitably intensifies privacy concerns, as health data constitutes a core component of data-driven healthcare systems.

The preceding analysis underscores the need to strengthen legal and regulatory safeguards to address the unresolved tension between health data privacy and big data utilisation. In the Malaysian context, this necessitates a reassessment of the existing data protection framework to ensure that it is capable of responding to large-scale, technology-driven data

processing in the healthcare sector. In particular, clearer legal standards on the processing of sensitive health data, enhanced accountability obligations for data controllers, and improved transparency mechanisms are essential to reinforce the protection of data subjects' rights in an increasingly data-intensive environment.

At the international level, the findings of this study suggest the importance of adopting a rights-based and risk-oriented approach to health data governance. The General Data Protection Regulation (GDPR) provides a useful reference point in this regard, particularly through its emphasis on data protection principles such as lawfulness, purpose limitation, proportionality, and accountability. Internationally, greater regulatory coherence, cross-border cooperation, and the development of harmonised standards for health data processing would contribute to addressing privacy risks arising from global data flows and advanced analytics.

Taken together, these measures highlight the necessity of aligning data protection laws with technological realities while safeguarding fundamental rights. While this study offers a general legal analysis of the dichotomy between big data and health data privacy, future research may further explore the development of enhanced and context-specific data protection frameworks, both in Malaysia and internationally that support innovation in healthcare while remaining consistent with the objectives of the Sustainable Development Goals by 2030.

NOTES

[1] Pulse, U. G. (2018). Big data for sustainable development. United Nations.

[2] Hossein Hassani, X. H., Steve MacFeely & Mohammad Reza Entezarian. (2021). Big Data and the United Nations Sustainable Development Goals (UN SDGs) at a Glance.

[3] Wiper, C. (2014). *Big data and data protection*.

[4] Gastin, L. O. (1995). Health Information Privacy. *Cornell Law Review*, 80(3).

[5] Mohd Amiruddin Hamzah, S. F. M. Y., Maisahara Yusof, Tunku Sofiah Larasih T. Zainol Rashid, Hasnah Shuhaimi, Abu Bakar Suleiman, Ahmad Nazri Mansor & Khairul Mizan Taib. (2020). Big Data Implementation in Malaysian Public Sector: A Review. *International Journal of Academic Research in Business and Social Sciences*, 10(11).

[6] Abu Bakar Munir, S. H. M. Y. F. M.-S. (2015). Big Data Big Challenges to Privacy and Data Protection. *International Journal of Social, Education, Economics and Management Engineering* Vol. 9(1), 355-363.

[7] Atiqah Binti Azman, N. S. A. B. A., Nurul Sahira Binti Kamal Azwan, Sherie Aneesa Binti Johary Al Bakry, Wan Nur Afiqah Binti Wan Daud, Hartini Saripan, Nurus Sakinatul Fikriah B.T. & Mohd Shith Putera. (2021). Privacy in the Era of Big Data: Unlocking the Blue Oceans of Data Paradigm in Malaysia. *Malaysian Journal of Social Sciences and Humanities*, 6(5).

[8] Norjihan Abd Ghani, S. H. N. U. U. (2016). Big data and data protection: Issues with purpose limitation principle. *International Journal of Advances in Soft Computing & Its Applications*, Vol. 8(3), 116.

[9] Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, *3*(2), 74-87. SEE ALSO: Rupp, V. & M.V.G. (2024). Clarifying "personal data" and the role of anonymisation in data protection law: Including and excluding data from the scope of the GDPR (more clearly) through refining the concept of data protection. *Computer Law & Security Review* Vol.52, 105392.

[10] Europe, U. N. R. I. C. f. W. (2007). How the European Union and the United Nations cooperate.

[11] Rights, U. N. H. (2018). *A Human Rights Based Approach to Data - Leaving No One*

Behind in the 2030 Agenda for Sustainable Development: Guidance Note to Data Collection and Disaggregation. SEE ALSO: Rights, U. N. H. (2018). A Human Rights-Based Approach. 1-24.

[12] Karim Abouelmehdi, A. B. H. H. K. (2018). Big healthcare data: preserving security and privacy. Journal of Big Data, 5(1), 1-18.

[13] Ben Purvis, Y. M. D. R. (2019). Three pillars of sustainability: in search of conceptual origins. *Sustainability Science*, Vol.14, 681–695.

[14] Dictionary, O. E. (2023). Development.

[15] Sachs, W. (2001). *The Development Dictionary: A Guide to Knowledge as Power*, Withwaterstrand University Press.

[16] Sachs, W. (2001). *The Development Dictionary: A Guide to Knowledge as Power*, Withwaterstrand University Press.

[17] Statistics, D. o. (2018). Sustainable Development Goals (SDG) Indicators. In M. o. Economy (Ed.). Malaysia: Department of Statistics.

[18] Statistics, D. o. (2018). Sustainable Development Goals (SDG) Indicators. In M. o. Economy (Ed.). Malaysia: Department of Statistics.

[19] Cannataci, J. A. (2019). Recommandation on the Protection and Use of Health-Related Data. U. Nations.

[20] Hossein Hassani, X. H., Steve MacFeely & Mohammad Reza Entezarian. (2021). Big Data and the United Nations Sustainable Development Goals (UN SDGs) at a Glance. *Big Data and Cognitive Computing*, Vol. 5(28).

[21] Health, M. o. (2020). Health in the Sustainable Development Goals and Universal Health Coverage: Progress Report for Malaysia 2016 – 2019 (MOH/S/RAN/197.20 (TR)-e). M. o. Health. SEE ALSO: Young, T. R. A. (2019). Data privacy in Malaysia with the emergence of big data and artificial intelligence. *Computer And Telecommunications Law Review*, Vol. 25(7), 181-186.

[22] Cieh, E. L. Y. (2013). Personal Data Protection Act 2010: An Overview Analysis. In N. I. E. L. Y. Cieh (Ed.), *Beyond Data Protection* (pp. 31-64).

[23] Mukhriz, J.-E. T. I. (2023). Challenges Arising from Digitalising Health Records. 1-9.

[24] Loh Fon Foong, H. S., Royce Tan & Desiree Tresa Gasper (2017). Data privacy a concern for many.

[25] Butler, T. A. I. d. J. (2006). The European Union and Human Rights: An *International Law Perspective. European Journal of International Law*, Vol. 17(4), 771-801.

[26] Europe, U. N. R. I. C. f. W. (2007). How the European Union and the United Nations cooperate. SEE ALSO: 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) [2016] OJ L119/1. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238. ALSO: Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779. Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994.

[27] Li, B. Y. J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. International Journal of E*nviromental Research and Public Health*, Vol. 16(6), 1070-1085.

[28] Ibid.

[29] Christofi, A., Dewitte, P., Ducuing, C., & Valcke, P. (2020). Erosion by Standardisation:Is ISO/IEC29134:2017 on Privacy Impact Assessment Up to (GDPR) Standard?. In M. Tzanou (Ed.), *Personal Data Protection and Legal Developments in the European Union* (pp. 140-168).

[30] Haug, C. J. (2018). Turning the Tables — The New European General Data

Protection Regulation. *The New England Journal of Medicine*, 379, 207-209.

[31] Supra 27. SEE ALSO: Menno Mostert, A. L. B., Monique C I H Biesaart & Johannes J M van Delden (2015). Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *24*, 956–960.

32.

REFERENCES

Abu Bakar Munir, S. H. M. Y. F. M.-S. (2015). Big Data Big Challenges to Privacy and Data Protection. *International Journal of Social, Education, Economics and Management Engineering Vo*, *9*(1), 355-363.

Atiqah Binti Azman, N. S. A. B. A., Nurul Sahira Binti Kamal Azwan, Sherie Aneesa Binti Johary Al Bakry, Wan Nur Afiqah Binti Wan Daud, Hartini Saripan, Nurus Sakinatul Fikriah B.T. & Mohd Shith Putera. (2021). Privacy in the Era of Big Data: Unlocking the Blue Oceans of Data Paradigm in Malaysia. *Malaysian Journal of Social Sciences and Humanities*, *6*(5). https://doi.org/https://doi.org/10.47405/mjssh.v6i5.780

Ben Purvis, Y. M. D. R. (2019). Three pillars of sustainability: in search of conceptual origins. *Sustainability Science*, *14*, 681–695. https://doi.org/https://doi.org/10.1007/s11625-018-0627-5

Butler, T. A. I. d. J. (2006). The European Union and Human Rights: An International Law Perspective. *European Journal of International Law*, *17*(4), 771-801. https://doi.org/https://doi.org/10.1093/ejil/chl029

Cannataci, J. A. (2019). *Recommandation on the Protection and Use of Health-Related Data*. U. Nations. https://www.ohchr.org/sites/default/files/Documents/Issues/Privacy/SR_Privacy/FINALHRDDOCUMENT.pdf

Christofi, A., Dewitte, P., Ducuing, C., & Valcke, P. (2020). Erosion by Standardisation:Is ISO/IEC29134:2017 on Privacy Im pact Assessment Up to (GDPR) Sta ndard?. In M. Tzanou (Ed.), *Personal Data Protection and Legal Developments in the European Union* (pp. 140-168). IGI Global.

Cieh, E. L. Y. (2013). Personal Data Protection Act 2010: An Overview Analysis. In N. I. E. L. Y. Cieh (Ed.), *Beyond Data Protection* (pp. 31-64). Springer.

Dictionary, O. E. (2023). Development. In https://www.etymonline.com/search?q=development&type=0.

Europe, U. N. R. I. C. f. W. (2007). How the European Union and the United Nations cooperate. Retrieved 6 June 2022, from https://unric.org/en/wp-content/uploads/sites/15/2021/02/Leporello_EU-VN_e.pdf

Gastin, L. O. (1995). Health Information Privacy. *Cornell Law Review*, *80*(3).

Haug, C. J. (2018). Turning the Tables — The New European General Data Protection Regulation. *The New England Journal of Medicine*, *379*, 207-209. Retrieved 25 March 2023, from

Health, M. o. (2020). *Health in the Sustainable Development Goals and Universal Health Coverage: Progress Report for Malaysia 2016 – 2019* (MOH/S/RAN/197.20 (TR)-e). M. o. Health. Dhttps://www.moh.gov.my/moh/resources/Penerbitan/Laporan/Umum/SDG_REPORT_FINAL_OCT2021.pdf

Hossein Hassani, X. H., Steve MacFeely & Mohammad Reza Entezarian. (2021). Big Data and the United Nations Sustainable Development Goals (UN SDGs) at a Glance. *Big*

Data and Cognitive Computing, *5*(28).

Karim Abouelmehdi, A. B. H. H. K. (2018). Big healthcare data: preserving security and privacy. *Journal of Big Data*, *5*(1), 1-18. https://doi.org/https://doi.org/10.1186/s40537-017-0110-7

Li, B. Y. J. (2019). The Policy Effect of the General Data Protection Regulation (GDPR) on the Digital Public Health Sector in the European Union: An Empirical Investigation. *International Journal of Enviromental Research and Public Health*, *16*(6), 1070-1085. https://doi.org/https://doi.org/10.3390/ijerph16061070

Loh Fon Foong, H. S., Royce Tan & Desiree Tresa Gasper (2017). Data privacy a concern for many. *The Star*.

Menno Mostert, A. L. B., Monique C I H Biesaart & Johannes J M van Delden (2015). Big Data in medical research and EU data protection law: challenges to the consent or anonymise approach. *24*, 956–960. Retrieved 16 May 2022, from https://www.nature.com/articles/ejhg2015239#citeas

Mohd Amiruddin Hamzah, S. F. M. Y., Maisahara Yusof, Tunku Sofiah Larasih T. Zainol Rashid, Hasnah Shuhaimi, Abu Bakar Suleiman, Ahmad Nazri Mansor & Khairul Mizan Taib. (2020). Big Data Implementation in Malaysian Public Sector: A Review. *International Journal of Academic Research in Business and Social Sciences*, *10*(11).

Mukhriz, J.-E. T. I. (2023). Challenges Arising From Digitalising Health Records. 1-9. Retrieved 15 Disember 2023, from https://www.krinstitute.org/assets/contentMS/img/template/editor/Challenges%20arising%20from%20digitalising%20health%20records.pdf

Norjihan Abd Ghani, S. H. N. U. U. (2016). Big data and data protection: Issues with purpose limitation principle. *International Journal of Advances in Soft Computing & Its Applications*, *8*(3), 116.

Pulse, U. G. (2018). *Big Data for Sustainable Development*. United Nations. Retrieved 23 Februari from https://www.un.org/en/global-issues/big-data-for-sustainable-development

Rights, U. N. H. (2018). *A Human Rights Based Approach to Data - Leaving No One Behind in the 2030 Agenda for Sustainable Development: Guidance Note to Data Collection and Disaggregation*. Retrieved 21 May from https://www.ohchr.org/en/documents/tools-and-resources/human-rights-based-approach-data-leaving-no-one-behind-2030-agenda

Rights, U. N. H. (2018). A Human Rights-Based Approach. 1-24. https://www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData.pdf

Rubinstein, I. S. (2013). Big Data: The End of Privacy or a New Beginning? *International Data Privacy Law*, *3*(2), 74-87.

Sachs, W. (2001). *The Development Dictionary: A Guide to Knowledge as Power*. Withwaterstrand University Press.

Statistics, D. o. (2018). Sustainable Development Goals (SDG) Indicators. In M. o. Economy (Ed.). Malaysia: Department of Statistics.

Wiper, C. (2014). *Big data and data protection*. https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220

Young, T. R. A. (2019). Data privacy in Malaysia with the emergence of big data and artificial intelligence.

Computer And Telecommunications *Law Review*, *25*(7), 181-186.