Malaysian Journal of Syariah and Law
مجلة الشريعة والقانون بماليزيا

**Vol. 12, No. 3, pp. 550-561 | DECEMBER 2024**
**DOI:** https://doi.org/10.33102/mjsl.vol12no3.572

# BIG DATA AND THE DETERIORATION OF CONSENT PRINCIPLE TO PROTECT HEALTH DATA PRIVACY IN MALAYSIA

[i]Nazura Abdul Manap, [i]Mohd Rizal Ab Rahman & [i,*]Siti Nur Farah Atiqah Salleh

[i]Faculty of Law, Universiti Kebangsaan Malaysia, 43600 Bangi, Selangor, Malaysia

*(Corresponding author) e-mail: sitinurfarahatiqah@gmail.com

***Article history:***
Submission date: 3 October 2023
Received in revised form: 28 June 2024
Acceptance date: 17 October 2024
Available online: 6 December 2024

***Keywords:***
Consent, big data, health data privacy, GDPR, Personal Data Protection Act 2010

***Funding:***
The authors would like to acknowledge the financial support from the Ministry of Higher Education, Malaysia. This article is funded under the Fundamental Research Grant Scheme FRGS/1/2020/SSO/UKM/01/2 under the project title "Perlindungan Data Kesihatan dalam Pemakaian Teknologi Data Raya di Malaysia".

***Competing interest:***
The author(s) has/have declared that there are no competing interests.

***Cite as:***
Abdul Manap, N., Ab Rahman, M. R., & Salleh, S. N. F. A. (2024). big data and the deterioration of consent principle to protect health data privacy in Malaysia. *Malaysian Journal of Syariah and Law, 12*(3), 550-561. https://doi.org/10.33102/mjsl.vol12no3.572



## ABSTRACT

It is part of the legal requirement for an individual to be conferred the right to consent when it involves the processing of their health data. However, with the advent of big data in healthcare, consent principle as a lawful basis for data processing and as a tool for data privacy in healthcare is being challenged. In this article, big data refers to the processing and analysis of large data sets to find new correlations—for example, for decision-making purposes and improving health delivery of health bodies. While big data may be beneficial, it also imposes certain legal complications regarding the sufficiency of the Malaysian Personal Data Protection Act 2010 in implementing consent. This article aims to analyse consent principle under the PDPA 2010 as a tool for health data privacy and its sufficiency in big data. We adopt a doctrinal qualitative analysis as the methodology in this paper. It is found that the consent principle under the Act must be revisited because it is lacking in its suitability and functions in dealing with big data and the practical demonstration of explicit consent in protecting privacy. Therefore, it is suggested that Malaysia could look to the European's Union General Data Protection Regulation as a potential model for enhancing its consent standards, with careful consideration of the existing constraints under the PDPA.

## Introduction

The principle of consent, as a means of protecting privacy, is currently going through a process of changes. The instrument in question serves to acquire legal authorization for the processing of health data. With consent, the utilization of health data is facilitated in a manner that aligns with the requirements of the health sector. This facilitates access to the collecting, analysis, and use of data. Considering the advancements in technology, particularly the use of big data for data collection, processing, and analysis, the question arises as to whether obtaining consent is still a necessary requirement?

Big data is relatively a new technology in Malaysia. The application of this technology is gaining its currency through various applications and projects in healthcare. In 2017, the Ministry of Health introduced the Malaysian Health Data Warehouse (MyHDW). This warehouse is an official healthcare information gathering and reporting system which applies big data technology (Azmi et al., 2022). Other than MyHDW, big data could be found in health-related applications such as *MySejahtera, SeLangkah* that were used during COVID-19 for the purpose of close-contact tracking and tracing (Batumalai, 2020; Azmi et al., 2022).

As compared to other available sector, the healthcare sector generates a massive amount of data every day from many different sources, such as healthcare treatment, patient admissions, medical images, patient medical records, and others (Azmi et al., 2022). This data may be mixed in with an individual's personal information (Torra & Navarro-Arribas, 2017). With this huge amount of data collected or integrated from different sources, the potential for this data to be infringe or misuse is at risk, even though the data has been anonymised or aggregated (Torra & Navarro-Arribas 2017; Price II & Cohen 2019).

The Personal Data Protection Act 2010 encompasses a range of privacy protection measures and legal protocols that serve to prevent and address instances of data privacy violations (Cieh, 2013; Munir et al., 2012; Walters et al., 2019). In the context of data processing, obtaining consent was established as the primary legal foundation before the processing of health data using technological means. In section 40 of the Personal Data Protection Act 2010 (PDPA 2010), it was stated as followed:

> (1) Subject to subsection (2) and section (5), a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions:
>
> (a) The data subject has given his explicit consent to the processing of the personal data.

As per Section 40 of the PDPA 2010, which is contingent upon the provisions outlined in Section 2 and Section 5, it is prohibited for a data user to engage in the processing of sensitive personal data pertaining to a data subject, unless it aligns with the requirements specified in Section 40 (Cieh, 2013; Pointon & Phuoc, 2012). The processing of health data without obtaining authorization is strictly prohibited due to the highly sensitive nature of such information. However, is the notion of consent still valid under the Act, particularly in situations involving big data?

This paper posits that privacy protection of health data via consent, as outlined in the Personal Data Protection Act (PDPA), is currently facing challenges in relation to the protection of health data privacy and consent within the realm of big data. This article attempts to address this issue and to primarily examine the potential risks posed by big data to consent and the privacy health data. It will explore the role of consent as a mechanism for securing the privacy of health data and discuss how the use of big data is compromising the privacy of such data. It is argued that the ability to exercise control over personal privacy affords individuals the autonomy to determine the extent of information disclosed to others, the level of intimacy desired in connections, and the way one's own identity is constructed (Cate & Mayer-Schoberger, 2013; Cormack, 2016; Froomkin, 2019; Ioannidis, 2013). In addition, we will propose appropriate approaches by examining the European Union's disposition with respect to this issue.

## Methodology

This article is conducted using doctrinal legal analysis study centralising on data analysis, that deliberates on the development of this issue, construes and organises laws relevant to health data privacy and big data. The aim of the study is to analyse the privacy through consent under the Act in providing privacy protection for health data. A legal analysis is the most suitable method to apply since the adequacy aspect is evaluated from the main data protection law in Malaysia, the Personal Data Protection Act 2010. There are two main stages in conducting this study. The first stage is data collection. We employed a library-based search, conducted by categorising the literature into two important themes: 1) big data and health data privacy and, 2) data protection laws and consent. Reference was also made to legal documents and policy papers from Malaysia and the European Union that were relevant to the issue beforehand. The second stage in data analysis, carried out throughout this paper to acquire an in-depth understanding relating to the consent principle, which will be elaborated in every part of this article.

## The Significance of Consent for Health Data Privacy and the Challenge of Big Data

### *Consent and Health Data Privacy*

Health data is inherently sensitive and frequently classified as a separate category of data. The scholarly literature in Malaysia does not provide any explicit definition or explanation of the concept of sensitive data (Cieh, 2013; Jahn Kassim, 2019; Munir et al., 2012; Pointon & Phuoc, 2012; Walters et al., 2019). The definition and elaboration of health data in the Personal Data Protection Act 2010 (PDPA 2010) in Malaysia are not clearly stated. However, it may be inferred that health data is encompassed within the category of sensitive data, as outlined in section 4 of the Act. However, the concept of health data can be characterized by its personal nature, as it possesses the capacity to identify specific individuals. Additionally, its sensitivity arises from its emphasis on the diverse aspects of individuals' health, as well as their medical treatments and services (OECD, 2015).

The sensitivity of the information resides in its capacity to ascertain the identities of persons and its emphasis on matters pertaining to personal health and healthcare interventions and provisions. Health data is classified as sensitive information according to the regulatory framework established by the Organization for Economic Cooperation and Development (OECD) for safeguarding personal data. Consequently, strict safeguards are required to ensure its safety. Moreover, Article 9 (1) of the European Union General Data Protection Regulation, a definitive list of special categories of personal data has been established, thereby expanding the extent of protection to encompass various significant domains, including healthcare.

In the medical practice, for example, consent must be first obtained before any medical treatments or procedures could be conducted upon the patient (Jahn Kassim, 2019). Medical treatment requires information collected from patients for the purpose of understanding the health condition of a patient (data subject) or for the physicist to be able to give suggestions for treatments or relevant medical procedures. In this situation, the physicists have the obligation to give sufficient information to enable the patients to make an informed decision that leads to informed consent. As for the latter, when there is research involving individuals (data subjects), consent needs to be explained in a form prepared by the researcher to inform data subjects regarding the purpose of such research, the relevant collection, storing, and using of data, including the extent of data usage (Abdul Aziz & Mohd Yusof, 2019; Dove & Chen, 2020a).

It must be noted that the act of giving consent is not merely a legal procedure, but it is also one of the most profound elements in medical ethics, the principle of autonomy. It is a fundamental concept in medical ethics, underpinning the notion that individuals have the right to make informed decisions about their own health and medical treatments (Brazier et al., 2023; Tharini & Low, 2021). It was asserted that autonomy is understood as the capacity for self-governance and decision-making, is fundamental to the concept of morality itself (Walker, 2018). Consent ensures that patients are adequately informed about the nature, benefits, and risks of medical procedures and research before agreeing to participate (Ahlin, 2017). It is not merely a formal requirement but a process that involves continuous communication and reassessment to ensure that the individual's autonomy is respected throughout their engagement with healthcare services.

In medical practice, consent is usually understood as a form signed by a patient prior to a medical procedure to confirm that he or she agrees to the procedure and is aware of any risks involved (Faden & Beauchamp, 1986). The primary purpose of the consent form is to provide evidence that the patient gave consent to the procedure in question. Consent is also considered the act of providing extensive information to a person who benefits from such information to execute the intended specific act. The interpretation is derived from the relationship of a doctor or physicist with their patients (Faden & Beauchamp, 1986). The practise of obtaining information by a doctor from a patient customarily involves consent that shows the significance of consent in such a relationship. It is safe to say that consent evolved from medical or health practices.

From the data protection law perspective, consent is one of the important principles before any sensitive personal data could processed. Consent and data are two important aspects that are interrelated in providing protection for data privacy for individuals in healthcare. According to (Cate & Mayer-Schoberger, 2013), consent is required because it empowers individuals or data subject to exercise privacy rights as they see fit. Unfortunately, the visions of privacy architects when they imagined empowered individuals making informed decision about the processing of their personal data is disrupted with big data (Cate & Mayer-Schoberger, 2013). Data protection law aims to provide for adequate protection upon individual data privacy. From the perspective of data protection law, consent is the core principle for data privacy. This aim is expected to be established in every field including healthcare (OECD, 2015). Meanwhile, Section 6 of the PDPA 2010 provides as followed:

> (1) A data user shall not —
>
> (a) In the case of personal data other than sensitive personal data, process personal data about a data subject unless the data subject has given his consent to the processing of the personal data; or
>
> (b) In the case of sensitive personal data, process sensitive personal data about a data subject except in accordance with the provisions under section 40.

The general rule under section 6 of the PDPA 2010 clearly stated that any personal data that needs to be processed must first obtained the consent from data subject. It is the main legal tool that allows for data to be processed in a legal manner. Furthermore, the reason behind consent as the main condition before any data could be processed is to ensure that the process will be done in the spirit of protecting the privacy of data subject who is the source of health data.

### *Big Data and Its Challenges*

There has been argument on how big data is killing consent as a form of privacy protection mechanism (Cormack, 2016; Froomkin, 2019; Ioannidis, 2013; Price II & Cohen, 2019). It kills the element of informing the data subject regarding the scope of consent and put privacy at risk since data re-identification could lead to the identification of the identity of the data subject (Froomkin, 2019). Consent requires for the data subject to fully understand how or why their data will be utilised, what are the advantages and disadvantages and address the achievable outcomes associated with the use of their data. Accordingly, there are two levels of risk caused by big data, and one of them is known as link-ability (Andreotta et al., 2022; O'Connor et al., 2017). It is common for big databases to link databases to increase the amount and quality of information. Because there is more information about everyone, linking databases increases the risk of identification. It's worth noting that the more information we have on people, the easier it is to re-identify them and the more difficult it is to protect them.

In defining what is big data, the definition is never definite. What makes it interesting is that the term itself could be comprehended by those two words, *"big"* and *"data"*. When combined, the definition is never easy to grasp. In other words, there is no definite or agreed-upon definition of big data. This is because big data is usually defined by these three important characteristics: volume, velocity, and variety. The characteristic has grown extensively in terms of its character to include the element of variety and veracity (Chen et al., 2014). In other words, big data is a large-scale dataset, complex and possesses specific characteristics with the ability to process different types of data from structured, semi-structured to unstructured data.

It was argued that the possible results of big data analysis are usually unknown. The PDPA 2010 is also silent on the legal status of predictions. Prediction is part of the important features of big data applications in health (San, 2020). The application of the consent principle in the case involving biomedical big data (sensitive personal data) would undermine the principle if it is to be implemented in the form of broad consent (Hallinan, 2020). Indeed, consent is one of the important mechanisms that gives the data subject autonomy in exercising their choice towards data processing, hence dynamic consent should be applied in obtaining consent from the data subject. Is the consent principle under PDPA ready for big data applications and protecting health data privacy?

Another issue is in the case of re-purposed data. The general problem of re-purposed data, then, is that data users have not always limited their use of personal data to the purpose for which the subjects' original consent was applicable (Andreotta et al., 2022). This is morally wrong because it does not consider the preferences and possibly the well-being of each person. The reason why informed consent should be sought in the first place is so that subjects have the information they need to decide if agreeing to something is in their best interests or if agreeing to it could hurt them.

In the context of big data, the traditional models of informed consent are challenged by the sheer volume, variety, and velocity of data processing. The need for a more flexible and responsive consent model becomes apparent, allowing individuals to modify their consent preferences in real-time and thereby enhancing their autonomy and control over their personal data (Cohen et al., 2018; Vayena et al., 2016). The complexity of big data, from data collection to data processing does giving a huge impact to consent as a tool to protect health data privacy. From the uncertainty of purpose, the unpredicted result of data processing and bias outcome had been influenced by big data and its complexity (Vayena & Blasimme, 2018).

As in the medical and clinical research setting, it is crucial to obtain an individual's informed consent prior to the use of big data, as failure to do so might cause harm to individuals. In such a setting, consent can be removed to facilitate major discoveries from readily available, rich databases. The practice known as "consent bias," where consent is placed as a legal requirement but has no significant impact on providing protection for data subjects' privacy, is relevant especially with regard to big data applications in health (Rothstein & Shoben, 2013; Terry, 2015).

Looking at the challenges brought by big data, addressed an approach to consent known as dynamic consent (Kaye et al., 2011; Prictor et al., 2019; Kaye & Prictor, 2021). The aim is to accommodate consent through more personalized, digital communication for researchers and participants (Kaye & Prictor, 2021). This approach has been tested on a few different projects in clinical research setting that involve big data (Kaye & Prictor, 2021). Abdul Aziz & Mohd Yusof (2019), were of the view that this approach is relevant. However, its position under the Malaysian data protection law must also be determined and discussed to see whether the law is sufficient and ready to face the challenges that have been highlighted.

## Legal Position of Consent under the Personal Data Protection Act 2010

### *Definition of Consent*

The legal handling of data has necessitated the inclusion of consent as a mandatory requirement. In the context of personal data processing, it is generally necessary to get consent prior to commencing such activities. The significance of consent as a fundamental principle within the framework of the Personal Data Protection Act (PDPA) of 2010 is worth considering. This legislation affirms consent as a legally valid foundation for the lawful handling of health information. Section 6 of the PDPA, which also serves as the general principle, forbids the processing of any data unless it is for a lawful purpose directly related to the data user. In contrast, section 40 delineated the circumstances under which the processing of personal data falling within the category of sensitive personal data was permissible. Further discussion on this topic will be presented in the subsequent section. Nevertheless, the Act does not provide a clear definition of consent (Munir et al., 2012; Cieh, 2013).

However, an effort was made to establish a definition for consent, which is described as the voluntary, explicit, and informed expression of the data subject's preferences, indicating their approval to the processing of their personal data. On the other hand, Cieh (2013) choose to define consent based on the EU Data Protection Directive, which states that "consent" of the data subject refers to any voluntary,

explicit, and informed indication of their wishes, through which they express their agreement to the processing of personal data related to them (Cieh, 2013).

This definition suggested by the EU Data Protection Directives that consent comprises of these element (Directive 95/46/EC, 1995). The situation encompassed a proactive and unequivocal action, the individual whose data is being processed must be provided with an authentic opportunity to exercise their autonomy in determining whether or not to grant consent, in order for the processing activity to take place, consent must be explicitly granted, and the individual whose data is being processed must be provided with comprehensive information regarding the processing activity in order to enable them to make a well-informed decision.

There exist four crucial components that define the concept of consent: The individual whose data is being processed must be provided with a legitimate opportunity to exercise their discretion in determining whether or not to grant consent. Consent must be granted explicitly for the specific processing activity, and the individual must be provided with all essential information pertaining to the processing activity to make an informed decision (Cieh, 2013).

It has been determined that there exists a consensus about the definition of consent. Specifically, consent serves as a legal foundation for the legitimate handling of health data, and it plays a crucial role in safeguarding the privacy of such data (Cieh, 2013; Walters et al., 2019). There exists a contention that consent serves as a framework for data privacy, embodying principles such as individual autonomy, freedom of choice, and rationality. In essence, once an individual comprehends the underlying rationale for the use of their data, consent is deemed to be satisfied, hence enabling the processing to proceed as the information is effectively communicated.

***Requirements of Explicit Consent in Health Data Processing***

Section 40 of the Malaysian PDPA 2010 stated that the sensitive personal data shall not be process except in accordance with the conditions, explicit consent and necessary under the law. In other word, the processing for health data, considering its nature that is sensitive, could not be done only when explicit consent is obtained. There are three important procedures that must be followed under the provision; the personal information processor before collecting personal information must inform the data subject, the purpose of collection and use of personal information, particulars of personal information to be collected, retention period of personal information and any other fact which may deny the data subject from giving consent (Munir et al., 2014; Jahn Kassim, 2019; Walters et al., 2019). Further discussion will be elaborated in the next part.

In the case of *Lee Ewe Poh v Dr Lim Teik Man & Anor* (2011) 1 MLJ 835, it was highlighted how consent plays an important role in protecting a data subject's personal data, when related to sensitive personal data. The issue was whether consent was provided for the taking and using photographs by a surgeon and displaying these outside of the normal protocol (using the pictures for medical evidence only). The High Court observed that the first defendant argued that the act of capturing images during the surgery without the patient's consent was at issue.

In its deliberation, the court made reference to the Emergency Medical Journal and contended that the assertion regarding consent maintains that an image captured for clinical objectives is an integral component of a patient's medical dossier. Implicit consent is granted by patients when they undergo x-ray and ultrasound tests. In a similar vein, when the patient seeks medical care and undergoes examination and evaluation, they implicitly consent to the process of documenting, encompassing both visual representations and textual data. The utilization of a medical photograph captured with the intention of providing medical care to a patient is strictly prohibited for any alternative purposes unless explicit consent has been obtained.

According to Section 4 of the Personal Data Protection Act (PDPA), sensitive personal data encompasses four distinct categories of information, one of which pertains to personal data that reveals details regarding an individual's medical or mental health or condition. In the context of this article, the term "sensitive personal data" refers to information pertaining to an individual's health. It is important to note that this definition is closely aligned with the concept of health data. This data falls inside the classification of sensitive personal data.

Accordingly, section 6 of the PDPA encompasses the primary stipulations pertaining to consent within the framework of the PDPA. Within the framework of the PDPA, there are two distinct categories of consent, namely consent pertaining to personal data and explicit consent specifically pertaining to sensitive personal data. Both forms of permission serve to restrict data processing until explicit approval has been obtained (Pointon & Phuoc, 2012; Walters et al., 2019). In a broad sense, both forms of consent facilitate the legal processing of data. Nevertheless, the Act did not provide a precise definition of explicit consent. However, it is worth noting that the requirement for explicit consent is more stringent in comparison to general consent.

Section 7 of the PDPA also plays an important role in the execution of consent, which is the principles of notice and choice. Notice and choice give data subjects the realisation of consent. It requires notification in writing to data subjects to acknowledge the information to be considered by data subjects to give their consent (Pointon & Phuoc, 2012). Among the information that needs to be attached in the notice are data descriptions, the purpose of processing, information available, access rights, data limitation, consequences, and notifications.

The significance of obtaining consent for data processing has been emphasized by the Personal Data Protection Act (PDPA), which states that personal data may only be processed if the data subject has provided approval for such processing. In relation to the handling of sensitive personal information, it is necessary to consult section 6 (1) (b) of the legislation, namely section 40 of the PDPA. This provision underscores the necessity of obtaining consent prior to the processing of personal data or sensitive personal data, in order to ensure the protection of privacy for individuals whose data is being processed. Section 7 delineates the prerequisites necessary to establish consent as outlined in Section 6, namely through means of notification and decision-making.

Section 40 of the Personal Data Protection Act (PDPA) in Malaysia outlines the provisions pertaining to the incorporation of explicit consent in relation to health data. Section 40 primarily deals to the handling and management of sensitive personal data. According to Section 40 (1) of the legislation, it is stipulated that a data user is prohibited from processing sensitive personal data of a data subject unless explicit consent has been obtained from the data subject, as mandated by Section 40 (1)(a). According to Section 40 (1)(b), processing is deemed necessary for protecting the vital interests of the data subject in situations where consent cannot be obtained from the data subject or on their behalf.

***Loopholes of explicit consent provision and implications to healthcare practices***

Several studies shows that explicit consent is a crucial prerequisite for the processing of health data as stipulated by the Act. Munir et al. (2014), sought to establish a clear understanding of the concept of consent, as the meaning of this term is not explicitly provided in the Personal Data Protection Act (PDPA). Nevertheless, the proposed definition appears to have been derived from the EU Data Protection Directive (Cieh, 2013; Munir et al., 2014; Walters et al., 2019). It is important to adopt this definition given our PDPA was modelled after the EU data protection law. Nevertheless, there is currently no clear definition or explanation provided about the concept of explicit consent or the procedures via which it can be obtained under the Personal Data Protection Act (PDPA) of 2010. If assumption is to be made, the procedures is similar with section 40 of the Act.

In the context of big data, it is necessary to highlight the complications that might be faced by data subjects and data users due to the insufficiency of consent provisions. With the constant evolution of data-processing tools, such as data mining and profiling tools, predicting future data-processing techniques and the potential future use of personal data becomes exceedingly challenging (Custers et al., 2018; Dash et al., 2019). For instance, insufficient consent provisions can lead to unauthorized access and misuse of personal health data, violating individuals' privacy rights. Data subjects might find their sensitive health information being processed without their explicit consent, leading to significant privacy breaches. The PDPA 2010 includes several relevant provisions under Sections 30 to 44, which aim to protect the privacy interests of data subjects and assist data users in fulfilling their roles within the realm of data protection law (Cieh, 2013; Munir et al., 2014). However, it is still debatable whether such rights under the provisions are suitable given the current technological challenges.

Healthcare bodies, as data users, may encounter challenges in adhering to data protection laws. For example, the data integrity principle outlined in Section 11 of the PDPA 2010 states:

> (1) A data user shall by take reasonable steps to ensure that the personal data is accurate, complete, not misleading and kept up to date by having regard to the purpose, including any directly related purpose, for which the personal data was collected and further processed.

This section highlights one of the legal principles embedded under the PDPA 2010 to illustrate its role in safeguarding the privacy and the use of consent as a regulatory mechanism. Considering big data in this context, it is hard to say that it will be able to conform with the "accurate, complete, not misleading..." requirement when we look into the challenges that has been discussed and addressed in the previous section.

Based on research conducted, it was found that in Malaysia, there is currently limited availability of further interpretation about consent. Additionally, the absence of clear methods for obtaining explicit consent for the processing of sensitive personal data poses a potential disruption to the functioning of the consent principle, particularly in the context of applying big data in healthcare. It is anticipated that data users responsible for data collection, including hospitals, health institutions, researchers, and physicists, will exert considerable effort to ensure that individuals from whom data is collected possess a reasonably accurate comprehension and adequate information regarding the potential uses of the data.

## Learning from European Union: The legal approach on privacy through consent for health data and big data

### *The inadequacy of consent under PDPA 2010 in the context of big data*

The current consent concept outlined in the PDPA appears to be inadequate in protecting health data due to the sophisticated nature of big data in the healthcare domain. The current state of the COVID-19 epidemic has presented significant challenges in the effective execution of the data protection law in Malaysia, hence impeding progress in this sector (Institute for Democracy and Economic Affairs, 2022). The PDPA is subject to widespread criticism across different sectors. However, within the scope of this research, the most significant concern is in the usage of big data, and the practical demonstration of explicit consent. The effectiveness of the Personal Data Protection Act (PDPA) remains unproven despite its nearly eight-year implementation period. Nevertheless, Personal Data Protection Act 2010 is widely recognized for its foundation on the data protection frameworks established by the European Union (EU). The European Union has successfully enacted the General Data Protection Regulation (GDPR), a recent legislation aimed at safeguarding data privacy.

The General Data Protection Regulation (GDPR) implemented significant provisions aimed at addressing legal privacy concerns arising from emerging technologies, such as big data (Vayena & Madoff, 2019). In 2020, the European Union (EU) published a legal policy paper named "Big Data and Artificial Intelligence" to address the considerable opportunities and challenges associated with the use of large-scale data in the field of healthcare. The document also seeks to facilitate the involvement of patient organizations in EU policy deliberations relating to digital health. The goal of data collection must be clarified when seeking consent in order to ensure that data subjects are adequately informed and authorize the use of their data for these purposes (Cieh, 2013; Munir et al., 2014).

### *GDPR's approach to consent and data protection*

The use of big data in healthcare has also posed a threat to the notion of consent and its implementation, a matter that has been duly acknowledged in the European Union's General Data Protection Regulation (GDPR) (Tzanou, 2021). Despite the potentially limited legal efficacy of consent as a basis for data protection, it remains deserving of consideration and significance. Prior to engaging in lawful data processing, it is necessary to do the primary and basic stage ( Mostert et al., 2017; Dove & Chen, 2020b). This practice demonstrates a level of regard for the individual whose data is being processed and establishes a sense of fairness between the data subject and the data controller in terms of information and communication.

It has been asserted that big data applications frequently carry a degree of uncertainty regarding the outcomes subsequent to their processing (Andreotta et al., 2022). This situation has undermined the fundamental principle of consent and the intended purpose of consent as a mechanism to grant individuals sovereignty over their data and ensure privacy for health-related information. In the context of seeking consent from data subjects, it is imperative for data users to furnish comprehensive information regarding the procedures employed and the potential implications involved (Mostert et al., 2017). This practice is integral to the ethical review process, as it ensures that consent is obtained with a thorough understanding of the pertinent details. However, when it comes to the context of big data, specifically the collection and analysis of health data to identify potential hypotheses, neither of these methodologies can be employed (Andreotta et al., 2022). During the period of data collection, the potential outcomes remained uncertain.

To address this concern, the European Union (EU) has proposed that the most effective approach is to acquire supplementary and unambiguous consensus for the use of data, therefore mitigating the problem of uncertainty. The European Union, by means of the European Data Protection Board, has implemented a particular directive referred to as Guideline 05/2020 on Consent under Regulation 2016/679, which establishes the concept of explicit consent and provides guidance on the process of obtaining consent. There exist two methods for acquiring explicit consent from a data subject. The first method entails the data subject providing a clear and unambiguous statement of consent in written form, accompanied by their signature at the bottom of the document, in order to pre-empt any potential complications in the future (Working Party 259, 2016). Alternatively, the data subject may fulfil the necessary requirement by completing an electronic form through means such as email, electronic signature, or scanned document.

***Assessment of GDPR effectiveness***

To assess the effectiveness of data protection legislation in the European Union (EU), particularly concerning sensitive personal health data, the implementation of a compulsory data protection impact assessment has been implemented. This assessment is required for processing operations that pose a significant danger to the fundamental rights and freedoms of individuals. Three specific elements will be evaluated, encompassing extensive "special categories" of personal information. It is reasonable to conclude that large-scale data encompasses applications related to big data (Yuan & Li, n.d.). The practices seen within the European Union (EU) can serve as an instructive example for addressing the shortcomings of the consent principle outlined in the Personal Data Protection Act 2010. By drawing inspiration from the EU's approach, Malaysia can enhance the protection of privacy for health data and effectively mitigate the potential risks associated with the utilization of big data applications in the healthcare domain (Dhali et al., 2022).

In addition, it has been proposed that, in accordance with data protection legislation, the research committee engaged in any project that necessitates the use of personal information should establish a clear differentiation between informed consent for participation in an experiment and consent as the legal foundation for the processing of personal data (Cate et al., 2017) . Conceptual clarity is of utmost importance in this context (Dove & Chen, 2020a, 2020b). In the context of ethical consent, it is likely that the research ethics committee will mandate the researcher to obtain informed consent from participants prior to conducting the research. One potential approach to accomplish this objective is providing individuals with an information sheet and afterwards requesting their signature on a consent form, as an illustrative instance. Furthermore, it should be noted that in many jurisdictions, granting consent to participate in specific forms of medical research, such as clinical trials involving pharmaceuticals or medical equipment, may be legally mandated.

It was recommended to obtain a broad consent, particularly for research projects requiring large or extensive datasets (Hallinan, 2020; Andreotta et al., 2022; Zenkera et al., 2022). In the context of scientific study pertaining to genomics, the inclusion of a wide permission is deemed essential as it facilitates the researcher's ability to ethically and lawfully carry out a project with potential benefits. Article 9 of the General Data Protection Regulation (GDPR) outlines the specific instances in which justification is necessary. The explanations provided are comprehensive in nature, and their relevance lies in the assurance of privacy protection when handling sensitive personal data. This attempt aims to demonstrate that, in accordance with the principles of permission and privacy protection, the collection and processing

of sensitive personal data may still be permissible under the provisions of the General Data Protection Regulation (GDPR).

Given that big data frequently require the extraction of new information from "data exhaust," it becomes imperative to obtain consent to ascertain the aim, establish legitimacy, and substantiate the requirement of processing (Dove & Chen, 2020a). In the event that a data user detects potential adverse effects on data subjects during the data processing phase, it is advisable for them to intervene and proactively communicate the findings to the impacted individuals. This is particularly crucial when there exists a possibility that the identified outcome may cause harm to the data subject. Even in cases when no harm is observed and the advantages of such processing are demonstrated, data users should nonetheless have the ability to notify data subjects.

The adoption of GDPR consent mechanism in Malaysia could possibly enhance health data protection significantly. However, the authors are aware that the implementation should first be tailored to fit Malaysia's legal context. Initial steps could involve adopting the explicit consent requirement and supplementary consent provision to ensure data subjects are fully informed and involved in the process. While waiting for the formal amendment to be done to the Act, legal guideline is suggested to be developed by data users and stakeholders. A phased and carefully regulated approach may enhance health data privacy in facing the unique challenge posed by big data in Malaysia.

## Conclusion

The current consent concept outlined in Malaysia's Personal Data Protection Act (PDPA) is inadequate for protecting health data due to the sophisticated nature of big data in the healthcare domain. COVID-19 has presented challenges in executing data protection laws in Malaysia, exposing gaps in the PDPA, especially concerning big data and explicit consent. Despite its implementation, the PDPA's effectiveness remains unproven. In contrast, the European Union's General Data Protection Regulation (GDPR) has implemented provisions to address privacy concerns arising from big data, emphasizing clear and unambiguous consent in data collection.

Big data in healthcare threatens the notion of consent due to uncertainties during data collection. To mitigate this, the European Union proposes supplementary, unambiguous consent and has implemented guidelines for obtaining explicit consent through written or electronic means. Additionally, the EU requires a data protection impact assessment for operations posing significant risks to individuals' rights and freedoms. Malaysia can learn from the EU's approach to enhance health data privacy protection and mitigate risks associated with big data applications.

It is crucial to differentiate informed consent for research participation from consent as the legal foundation for personal data processing. Broad consent is recommended for research projects requiring large datasets. The GDPR allows for collecting and processing sensitive personal data under specific justifications. Consent is necessary to establish the aim, legitimacy, and requirement of processing in big data applications, with data users proactively communicating findings and potential harm to data subjects. Malaysia has the opportunity to draw valuable insights from the EU's approach, bolstering privacy protections for health data and addressing PDPA limitations. It is suggested for further research to be made on the guidelines for the protection of health data in the application of big data in Malaysia.

## References

Abdul Aziz, M. F., & Mohd Yusof, A. N. (2019). Can dynamic consent facilitate the protection of biomedical big data in biobanking in Malaysia? *Asian Bioethics Review, 11,* 209–222.

Ahlin, J. (2017). *Personal autonomy and informed consent: Conceptual and normative analyses* [Doctoral dissertation, KTH Royal Institute of Technology].

Andreotta, A. J., Kirkham, N., & Rizzi, M. (2022). AI, big data, and the future of consent. *AI & Society, 37,* 1715–1728.

Azmi, N. A., Mohd Noor, N., Muhd Shukri, M. I., Mahmud, A., & Abdul Manaf, R. (2022). The role of big data analytics in digital health for COVID-19 prevention and control in Asia. *Malaysian Journal of Medicine and Health Sciences, 18*(4), 173–181.

Batumalai, K. (2020, June 16). "Central contact tracing app may threaten data protection, SELangkah creator says". *CodeBlue.* https://codeblue.galencentre.org/2020/07/16/central-contact-tracing-app-may-threaten-data-protection-selangkah-creator-says/

Brazier, M., Cave, E., & Heywood, R. (2023). Capacity, consent and compulsion. In *Medicine, patients and the law.* Manchester University Press.

Cate, F. H., & Mayer-Schoberger, V. (2013). Notice and consent in a world of big data. *International Data Privacy Law, 3*(2), 67–73.

Cate, F. H., Kune, C., Svantesson, D. J. B., Lynskey, O., & Millard, C. (2017). Machine learning with personal data: Is data protection law smart enough to meet the challenge? *International Data Privacy Law, 7*(1), 1–2.

Chen, M., Mao, S., & Liu, Y. (2014). Big data: A survey. *Mobile Networks and Applications, 19,* 171–209.

Cieh, E. L. Y., & Ismail, N. (Eds.). (2013). *Beyond data protection: Strategic case studies and practical guidance.* Springer.

Cohen, I. G., Lynch, H. F., Vayena, E., & Gasser, U. (Eds.). (2018). *Big data, health law, and bioethics.* Cambridge University Press.

Cormack, A. N. (2016). Downstream consent: A better legal framework for big data. Winchester University Press.

Custers, B., Dechesne, F., Pieters, W., Schermer, B., & Van Der Hof, S. (2018). *The Routledge handbook of the ethics of consent.* Routledge.

Dash, S., Kumar Shakyawar, S., Sharma, M., & Kaushik, S. (2019). Big data in healthcare: Management, analysis and future prospects. *Journal of Big Data, 6*(54), 1–25. https://doi.org/10.1186/s40537-019-0217-0

Dhali, M., Hassan, S., Zulhuda, S., & Ismail, S. F. (2022). Artificial intelligence in health care: Data protection concerns in Malaysia. *International Data Privacy Law, 12*(2), 143–161.

Directive 95/46/EC of the European Parliament and of the Council, Data Protection Directive 31, Pub. L. No. 1.281 (1995). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=NL

Dove, E. S., & Chen, J. (2020a). Should consent for data processing be privileged in health research? A comparative legal analysis. *International Data Privacy Law, 10*(2), 117–131.

Dove, E. S., & Chen, J. (2020b). To what extent does the EU General Data Protection Regulation (GDPR) apply to citizen scientist-led health research with mobile devices? *The Journal of Law, Medicine & Ethics, 48*(1), 187–195.

Faden, R. R., & Beauchamp, T. L. (1986). *A history and theory of informed consent.* Oxford University Press.

Froomkin, A. M. (2019). Big data: Destroyer of informed consent. *Yale Journal of Law and Technology, 21*(3), 27–54.

Hallinan, D. (2020). Broad consent under the GDPR: An optimistic perspective on a bright future. *Life Sciences, Society and Policy, 1,* 1–12.

Institute for Democracy and Economic Affairs. (2022, April 22). "Ideas: MySejahtera episode poses questions about data privacy". *The Edge.* https://theedgemalaysia.com/article/ideas-mysejahtera-episode-poses-questions-about-data-privacy

Ioannidis, J. P. A. (2013). Informed consent, big data, and the oxymoron of research that is not research. *The American Journal of Bioethics, 13*(4), 40–42.

Jahn Kassim, P. N. (2019). *Persetujuan kepada rawatan*. Bengkel Undang-Undang Perubatan 2019.

Kaye, J., & Prictor, M. (2021). *The Cambridge handbook of health research regulation*. Cambridge University Press.

Kaye, J., Whitley, E. A., Kanellopoulou, N., Creese, S., & Hughes, K. J. (2011). Dynamic consent: A solution to a perennial problem? *BMJ*, *343*. https://doi.org/10.1136/bmj.d6900

*Lee Ewe Poh v. Dr Lim Teik Man & Anor* (2011) 1 MLJ 835.

Mostert, M., Bredenoord, A. L., van der Sloot, B., & van Delden, J. J. M. (2017). From privacy to data protection in the EU: Implications for big data health research. *European Journal of Health Law*, *24*, 1–13.

Munir, A. B., Mohd Yasin, S. H., & Karim, M. E. (2012). Malaysia's Personal Data Protection Act: Is it too little? In *Data protection law in Asia* (pp. 181–202). Sweet & Maxwell.

Munir, A. B., Yasin, S. H., & Karim, M. E. K. (2014). *Data protection law in Asia*. Sweet & Maxwell.

O'Connor, Y., Rowan, W., Lynch, L., & Heavin, C. (2017). Privacy by design: Informed consent and Internet of Things for smart health. *Procedia Computer Science*, *113*, 653–658.

OECD. (2015, October). "Health data governance: Privacy, monitoring and research – Policy brief". *OECD*. https://www.oecd.org/health/health-systems/Health-Data-Governance-Policy-Brief.pdf

Pointon, L. D., & Phuoc, J. C. (2012). *Personal data protection cases and commentary with applied Syari'ah principles*. CLJ Publication.

Price II, W. N., & Cohen, I. G. (2019). Privacy in the age of medical big data. *Nature Medicine*, *25*(1), 37–43.

Prictor, M., Lewis, M. A., Newson, A. J., Haas, M., Baba, S., Kim, H., Kokado, M., Minari, J., Molnár-Gábor, F., Yamamoto, B., Kaye, J., & Teare, H. J. A. (2019). Dynamic consent: An evaluation and reporting framework. *Journal of Empirical Research on Human Research Ethics*, *15*(3), 1–12.

Rothstein, M. A., & Shoben, A. B. (2013). Does consent bias research? *The American Journal of Bioethics*, *13*(4), 27–37.

San, T. P. (2020). Predictions from data analytics: Does Malaysian data protection law apply? *Information & Communications Technology Law*, *29*(3), 291–307.

Terry, N. P. (2015). Big data proxies and health privacy exceptionalism. *Health Matrix: The Journal of Law and Medicine*, *24*(1), 98–100.

Tharini, R., & Low, J. (2021). Patient autonomy, consent, and capacity of minors. In R. Tharini & J. Low (Eds.), *Medical law and ethics in Malaysia* (pp. 229–245). Lexis Nexis.

Torra, V., & Navarro-Arribas, G. (2017). Big data privacy and anonymization. In A. D. W. S. F.-H. L. F. C. R. Lehman (Ed.), *IFIP advances in information and communication technology* (pp. 15–26). Springer.

Tzanou, M. (2021). *Health data privacy under the GDPR: Big data challenges and regulatory responses*. Routledge.

Vayena, E., & Blasimme, A. (2018). Health research with big data: Time for systemic oversight. *The Journal of Law, Medicine & Ethics*, *46*, 119–129.

Vayena, E., & Madoff, L. (2019). Navigating the ethics of big data in public health. *Public Health Ethics*. Oxford University Press.

Vayena, E., Gasser, U., Wood, A., O'Brien, D. R., & Altman, M. (2016). Elements of a new ethical framework for big data research. *Washington and Lee Law Review*, *72*(3), 420–441.

Walker, T. (2018). Consent and autonomy. In *The Routledge handbook of the ethics of consent* (pp. 131–139). Routledge.

Walters, R., Trakman, L., & Zeller, B. (2019). *Data protection law: A comparative analysis of Asia-Pacific and European approaches*. Springer.

Working Party 259. (2016). Guidelines 05/2020 on consent under Regulation 2016/679 (pp. 1–33). European Data Protection Board.

Yuan, B., & Li, 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 Environmental Research and Public Health*. *16*(6), 1070 https://doi.org/10.3390/ijerph16061070

Zenkera, S., Strechb, D., Ihrigc, K., Müllerf, G., Schickhardt, C., Schmidt, G., Speer, R., Winkler, E., von Kielmansegg, S. G., Drepper, J., & Jahnse, R. (2022). Data protection-compliant broad consent for secondary use of healthcare data and human biosamples for (bio)medical research: Towards a new German national standard. *Journal of Biomedical Informatics*, *131*, 1–8.