(2025) Vol.7 (2) CLI 77-94

THE DEPLOYMENT OF TRACKING TECHNOLOGY AND HEALTH DATA PRIVACY DURING COVID-19 IN MALAYSIA: LEARNING FROM THE EUROPEAN UNION

[i*]Siti Nur Farah Atiqah Salleh, [ii]Nazura Abdul Manap, & [iii]Mohamad Rizal Ab. Rahman

[i*] Jabatan Undang-undang, UiTM Cawangan Melaka, Kampus Alor Gajah, 78000 Alor Gajah, Melaka, Malaysia.

[ii,iii] Fakulti Undang-undang, Universiti Kebangsaan Malaysia (UKM), 43600 UKM Bangi, Selangor, Malaysia

*Corresponding author: sitinurfarahatiqah@uitm.edu.my

ABSTRACT

Article history:
Submission date: 12 Nov 2025
Received in revised form: 30 Dec 2025
Acceptance date: 31 Dec 2025

Keywords:
COVID-19; Data Privacy Law; GDPR; Health Data; PDPA 2010

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., Manap, N., A., & Rahman, M. R. A. (2025). The Deployment of Tracking Technology and Health Data Privacy during COVID-19 in Malaysia: Learning from the European Union. *Current Legal Issues*, *7*(2), 77-94.

Tracking technology is being deployed in Malaysia to trace and track close contacts of those infected by COVID-19. In 2020, Malaysia introduced a tracking technology known as MySejahtera. It needs to be downloaded by mobile users for the purpose of tracking information regarding COVID-19 status. Contact tracking technology efforts to access personal health information have raised privacy concerns in Malaysia. This article aims to legally analyse the protection of health data privacy with the application of tracking technology in Malaysia by looking into the Personal Data Protection Act 2010 and the European Union law on data protection. This study employed qualitative fundamental legal research and conducted library-based research to analyse data from acts, journals and legal documents. This research found that health data privacy and data protection law in Malaysia remains limited during COVID-19, particularly in addressing government-led data processing, emergency-based exceptions to consent, and the governance of digital tracking technologies., but there is room for improvement to develop better health data privacy protection by learning from the European Union data protection law.

INTRODUCTION

Tracking technology is being deployed across the world to trace and track close contacts of those infected by COVID-19. Malaysia also joined this mission in 2020 by introducing a mobile application known as MySejahtera. The application of this tracking technology has raised issues regarding the privacy of health data. Since this technology was used during the COVID-19 pandemic, the deployment of tracking technology was regarded as an important public health measure to mitigate the spread of COVID-19, particularly through contact tracing and early intervention, as acknowledged in international public health guidance.[12]

The legality of tracking technology and how data protection law is applicable in this situation is still vague. Health data privacy concerns have re-emerged during the COVID-19 pandemic, particularly in relation to the collection and use of personal data through digital tracking technologies, with several studies and commentaries highlighting public unease and trust deficits regarding such data practices in Malaysia.[1]

The Personal Data Protection Act 2010 (hereinafter "PDPA 2010") is the only law in Malaysia that governs matters relating to personal data and data privacy, including health data. This Act is very much influenced by the European model of data protection law. Section 2 of the Personal Data Protection Act 2010 historically limits the Act's applicability to personal data processing in connection with commercial transactions by private sector entities, and expressly excludes federal and state government bodies and non-commercial data processing from its scope. Although the Personal Data Protection (Amendment) Act 2024 introduces substantial reforms to strengthen data protection governance, accountability obligations, breach notifications, and data subject rights, it does not materially alter this core scope limitation regarding government applicability.[2] Since PDPA 2010 is the only law that governs personal data in Malaysia, it will be the main reference for analysis.

It was found that the main concern about deploying tracking technology is the public's main concern about the data security and privacy that are collected through this tracking and monitoring technology.[3] Furthermore, there are shortcomings highlighted in deploying tracking technology pertaining to data privacy.[4] Firstly, there is insufficient information as to how the information provided by people will be used and stored. Secondly, the information pertaining to the technology application is not provided consistently to the data user. Both literature also emphasised the fact that PDPA 2010 is not subjected to the government as they claimed it to be in the privacy policy of MySejahtera. This literature does not highlight whether data collected using this technology should be considered as health data. This issue reveals a doctrinal gap that necessitates further explanation within the legal framework. The data that is collected during a public health emergency should be considered health data and be treated as sensitive data.

Since this issue not covered in much literature in Malaysia, it is significant to refer to and analyse the European Union law regarding application tracking technology. This reference is made due to the fact that the European Union (hereinafter "EU") is among the earliest in taking steps to develop data protection rules pertaining to tracking technology and health data privacy in the world. There are other countries that have already developed tracking technology but do not focus much on protecting the privacy of the data. Moreover, the European Union has long been regarded as a global benchmark in the development of data protection law. Malaysia's Personal Data Protection Act 2010 was influenced by European data protection principles, particularly those embodied in the former EU Data Protection Directive 95/46/EC. It is important to note, however, that the Directive has since been repealed and replaced by the General Data Protection

Regulation (GDPR), which represents a significant regulatory shift rather than a mere continuation of the earlier framework. The GDPR introduces enhanced data protection principles, stronger enforcement mechanisms, expanded data subject rights, and heightened obligations on data controllers and processors, particularly in relation to sensitive personal data such as health data. While Malaysia's PDPA 2010 reflects the foundational ethos of the Directive, the GDPR constitutes a more advanced and robust legal regime. Accordingly, this article refers to the GDPR not as the direct model for Malaysia's data protection law, but as a contemporary point of comparative reference in assessing how modern data protection standards address the challenges of health data privacy during public health emergencies.[5]

In order to set a standard, the European Commission of the European Union suggested that these contact tracing apps use a balanced approach and a smart solution.[6] It said that the apps should follow all of the rules set out in laws about data protection and privacy. Also, it said that users should not have to use these apps and that there should be a "sunset" clause, (ii) that the collected data should not be stored in central databases, and (iii) that the collected data should be made anonymous.[7] It is also worth noting that the transition from pandemic to endemic states completely altered perceptions of how health data should be prioritised and protected from any type of privacy threat.[8] The World Health Organization stated that COVID-19 is likely to be an endemic, meaning it will be part of our daily lives, similar to the flu. If this situation happens, is it still relevant to proceed with data collection due to emergency states and without adequate protection of the law?

Therefore, this article aims to legally analyse the issue of tracking technology and the privacy of health data in Malaysia by examining the Personal Data Protection Act 2010 alongside the European Union's data protection framework during the COVID-19 pandemic. While the PDPA 2010 provides a basic structure for the protection of personal data, it remains insufficient in addressing contemporary challenges associated with large-scale health data processing, particularly in emergency contexts involving digital tracking technologies. In this respect, Malaysia may draw specific lessons from the GDPR in these key areas. First is the explicit recognition of health data as a special category of personal data subject to heightened protection and stricter processing conditions. Secondly is the requirement for clear legal bases and proportionality safeguards when health data is processed for public health purposes.

The European Union, through the General Data Protection Regulation 2018 (hereinafter "GDPR"), has developed a guideline known as "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak." For this reason, the European Data Protection Board made the guideline a legal standard for protecting the personal health data of European Union citizens. This is because data-driven solutions are needed to help healthcare fight this pandemic.

By examining existing legal standards in the European Union regarding the implementation of contact tracing applications, Malaysia could learn and strengthen data protection laws in order to preserve the privacy rights of health data. In this article, we will address the legality of the use of health data and what we can learn to improve Malaysia's health data privacy during this pandemic.

METHODOLOGY

This research employed doctrinal legal research. In this article, it is aimed to fully understand the necessity of using tracking technology in Malaysia and to legally analyse the ambiguity of Malaysia's data protection law in facing the challenges of health data privacy. From this point, the study examines the European Union's data protection framework as a comparative reference to assess how health data privacy

can be protected alongside the deployment of digital tracking technologies.

There are two stages in order to complete the whole process of legal analysis. The first stage is collecting relevant literature with fewer than five important keywords. There are five important keywords that we used in searching for the relevant literature: health data, privacy of health data, tracking technology during COVID-19, and data protection law. These four keywords were found to be in journal articles and legal documents. The primary legal document analysed in this article is the Personal Data Protection Act 2010 (PDPA). Secondary sources include books, legal and technology journals, and materials accessed through legal databases such as LexisNexis, HeinOnline, and Current Law Journal. The data collection process includes journal articles, legal documents (i.e., Acts), official international reports, policy papers, books, and established news from online sources. The journal articles we have collected range from the years 2011–2021. As for the legal documents, we focused on Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak " under the General Data Protection Regulation 2018 because it is found to be suitable for the current discussion in this article.

The second stage is the data analysis process. We adopt descriptive analysis with analytical and critical analysis to analyse the data. The second stage involves data analysis. Descriptive analysis is employed to identify relevant legal concepts and issues in a systematic manner, while analytical and critical analysis is applied to evaluate the adequacy of existing legal frameworks and to develop normative arguments relating to health data privacy. [9]

LITERATURE REVIW

What Is Health Data Dan Tracking Technology?

Health data and tracking technology are not clearly defined under the law in Malaysia.[10] However, the definition of "sensitive personal data" under Section 4 of the PDPA 2010 could give an idea of what this term means.

any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence, or any other personal data as the Minister may determine by order published in the Gazette.

Even though health data is not clearly defined under this provision, we found that what constitutes health data is included under the meaning of sensitive data within the context of the provision.[11] It is safe to say that health data falls within the scope of sensitive personal data. The relevant point is that health data is somewhat associated with information relating to a person or an individual relating to their health. The above provision provides for a direct and general definition of health data within the context of Malaysia's data protection law.

On the other hand, Article 4 (15) of the GDPR defines personal data in a broader sense. The article defines personal to include health data. In summary, it defines personal data concerning health includes all data which reveals information relating to the past, current or future physical or mental health status of a data subject.

The GDPR provides for a broad yet explicit definition of health data. The main point that defines health data under GDPR is that personal data relating to health includes all information pertaining to the data subject's health condition. For the purpose of this article, it is the view of the authors that a combination of both definitions will be applied throughout this piece of writing. The definitions above are good for this article because they help explain the general definition of health data under the PDPA 2010.

The tracking technology is not clearly defined under any laws available in Malaysia. The main function of this

technology supposedly able to collect data for the purpose of track the location and the spread of COVID-19 in the community. The WHO classified digital tools for contact tracking into three.[12] First, the outbreak response tools designed for those who engage in public health response and are involved in tracing contacts and investigating outbreaks.[14] Secondly, proximity tracking tools, use location-based (GPS) or Bluetooth technology.[15] This tool basically attracted the privacy concern about the disclosure or personal data. Lastly is symptom tracking tools which is designed to routinely collect self-reported signs and symptoms to assess diseasese severity.[16]

The application of data in tracking technology should be considered to be given the same protection as sensitive data under the law. We argued that the data collected from tracking technology in the situation of a COVID-19 pandemic to ease tracking and tracing activities deserved privacy protection, and thus it is relevant to include tracking-technology data under the health data definition.

Health Data Privacy Under Malaysian Law

There is a general guideline for using patients' data according to the law that can be found in the Confidentiality Codes 2011 of the Medical Act 1971. The code encouraged the usage of health data for the purpose of medical treatment and as a guideline for medical practitioners. This code is not adequate within the context of tracking technology due to its limitations in terms of medical purposes, especially in providing protection for health data privacy, because of its nature, which is too general and has no legal effect.

In terms of health data protection, the PDPA 2010 lays out a few important provisions that offer protection when handling data related to health. Section 6 (1) (b) of the PDPA 2010 requires that sensitive data be processed only in accordance with Section 40. Under Section 40, the conditions under which data could be processed were listed, and among the important elements for processing sensitive data is explicit consent. However, there are exemptions to the rules that allow health data to be processed without consent under Section 45. When personal data is used to share information about a person's physical or mental health, the Access Principle may not apply. This means that this Act may not apply to personal data that is used in this way.

Health data is inherently sensitive, and its processing ordinarily requires the explicit consent of the data subject under the PDPA 2010. However, the statutory exceptions under Section 45 permit the processing of such data without consent in specific circumstances, including where public interest considerations prevail. During the COVID-19 pandemic, this exception was effectively relied upon to expedite the large-scale collection and processing of health data through digital tracking technologies. While this approach may be justified on grounds of urgency and public health necessity, it raises significant privacy risks by weakening the central role of consent as a safeguard for individual autonomy and informational self-determination.

The bypassing of explicit consent increases the risk of excessive data collection, function creep, prolonged data retention, and secondary uses of health data beyond the original public health purpose. In the absence of consent, data subjects are placed in a structurally vulnerable position, with limited awareness or control over how their health data is processed, shared, or retained. This is particularly problematic in the Malaysian context, where the PDPA 2010 does not apply to government bodies and where binding safeguards governing emergency data processing remain limited.

To mitigate these risks, the relaxation of consent requirements during public health emergencies must be accompanied by robust alternative safeguards. These should include strict purpose limitation to ensure that health data collected for pandemic control is not repurposed for unrelated objectives; clear temporal limits on data retention, supported

by mandatory deletion or anonymisation once the public health objective is achieved; enhanced transparency obligations requiring authorities to publicly disclose how data is processed, stored, and shared; and independent oversight mechanisms to monitor compliance and prevent abuse. Without such safeguards, the temporary suspension of consent risks normalising intrusive data practices and undermining long-term trust in public health technologies.

Accordingly, while Section 45 of the PDPA 2010 enables expedient data processing in emergency contexts, its application must be narrowly construed and supplemented by enforceable accountability measures. This ensures that the protection of public health does not come at the expense of disproportionate interference with individual health data privacy.

Emergency (Essential Powers) Ordinance and Its Impact on The Use Of Health Data In Malaysia During Covid-19

A tracking technology known as MySejahtera was introduced in 2020 in Malaysia. It is a mobile application that people will be able to download from the Google Playstore or Apple Store. At first, people could download the app to their phones or write down names and other information in a book provided by the people who ran the place.

The MySejahtera tracking application has a limited privacy policy that comes with it. It is a voluntary software, where individuals have the option of downloading the application or not. According to MySejahtera's official website, the app was built by the Malaysian government to assist in managing the country's COVID-19 outbreaks. It enables users to self-assess their health and that of their families. Additionally, users can monitor their health status throughout the pandemic. In addition, MySejahtera lets the Ministry of Health (MOH) keep an eye on the health of its users and act quickly to get them the treatment they need.

If we look thoroughly into the sites where questions relevant to the apps were asked and answered, the privacy aspects were not regulated to the extent that the app user should not be concerned.[17] In terms of personal information security, the government of Malaysia owns and operates the app. The Ministry of Health is responsible for its administration, with assistance from the MAMPU and the National Security Council. This personal information will be used solely for the purpose of managing and mitigating the COVID-19 outbreak. It will not be distributed to a third party. The confidentiality of medical records should keep the identities of patients safe. This is not a law, but just a set of rules.

If we look only through the lens of health and public safety, especially during the COVID-19 pandemic, the use of such applications is quite fair. The priority is the government's intention to mitigate the harm and risk of infections among citizens. Is it fair, then, if we don't think about the risks of using too much personal health data on an individual's privacy?

MySejahtera is not the only tracking app used to track COVID-19 in Malaysia, as some premises management also deploys other types of tracking apps or QR code scanners, for example, Gerak Malaysia and My Trace. The state governments, such as in Selangor, have also introduced tracking applications known as SeLangkah (Ying, 2020).[18]

As a result, customers would have to scan QR codes or download different apps, and some would have to fill out Google Forms for each location they wanted to visit. Can this be considered an oversharing of personal health data? What is the law in Malaysia when it comes to protecting the privacy of Malaysian citizens' health data? Malaysia's Commissioner for Personal Data Protection has yet to issue any specific guidelines on the lawful processing of personal data in connection with the COVID-19 pandemic. However, the Ministry of Health has issued several guidelines requiring event organisers to

retain contact information for all participants for at least one month after the event concludes. The Prevention and Control of Infectious Diseases Act 1988 contains two significant regulations (PCIDA).[19] The PCIDA existed prior to the declaration of an emergency. Two regulations were introduced during the recent emergency state: the Prevention and Control of Infectious Diseases (Measures Within Infected Local Areas) Regulations 2020 and Regulation 9 of the Prevention and Control of Infectious Diseases (Measures Within Infected Local Areas) Regulations (No. 2) 2020, both of which require you to provide information about infectious disease prevention and control upon request from an authorised officer.

Another important and vital ordinance in this state is known as Emergency (Essential Power) Ordinance 2021. It was promulgated on January 11, 2021, and it gave powers to an independent body to advise the King on emergency matters relating to security, economic life, and public order.[21] In other words, every action taken by the government to curb and manage COVID-19 in Malaysia, including the usage of health data, is allowed.

In Malaysia, the PDPA 2010 is the only Act that governs data protection. It was formed to govern the processing of personal data for commercial transactions in various sectors, including health. However, there are two main shortcomings that limit the functions of the Act. The first one is regarding applicability, which only covers commercial transactions. Secondly, the government and state bodies are exempted from being exceptional bodies applying to the Act. The government is effectively occupied with preparing own information.[20]

A large volume of personal data is gathered, kept, and processed by various government departments for many reasons and purposes.[4] The processing of individual information has, in this way, become a critical action inside private and public areas. Along these lines, it is particularly pertinent for such impediments to be mentioned by the public authorities, particularly in talking about the lawfulness and impact of contact-tracking applications for COVID-19. The shortcomings should not be in silos, so there is a necessity to refer to the EU to observe health data protection offered under the law during COVID-19.

As a matter of fact, the EU has started the move to offer health data protection while using tracking technology. For the purpose of observation and learning, the next part will be a legal analysis of how the EU and its member states have used the GDPR to protect health data privacy while using tracking technology.

Privacy Rights, Gdpr and Health Data Protection In The Eu

The right to privacy is an established fundamental right in the European Union. The manifestation of this is properly delivered in the EU data protection law.[21] Data protection was first regulated under EU law, known as the Data Protection Directive in 1995. ECHR Article 8 protects the right to privacy and family life, as well as the home and correspondence, and sets out how this right can be limited. The right to protect personal data is one of them.

In the countries of the European Union, protecting the privacy of personal information is one of the most important human rights. This means that the need to protect personal data is no longer an option but an obligation.[22] It is not an absolute right, though. These fundamental rights to data privacy apply to all types of data, including health data.[23]

The General Data Protection Regulation is the most important piece of privacy law in the EU. It is an upgraded version of the Data Protection Directives, introduced in 2018. It is common knowledge that using technology to collect, use, and share health data is more efficient. On the other hand, they pose new challenges to privacy and data security. As a result, the GDPR establishes specific principles that apply to all uses of patient data and to all data controllers. In the design and implementation of these systems, all of the

GDPR Article 5 principles, (i) lawfulness, fairness, and transparency, (ii) purpose limitation, (iii) data minimisation, (iv) accuracy, (v) storage limitation, (v) integrity and confidentiality, and (vi) accountability, must be followed.[24] These principles are translated into a specific architecture of data subject protection and enforcement. Because health data is considered a distinct category of data, the general rule is that it should not be processed because it includes all personal data that, by definition, is particularly sensitive in relation to fundamental rights and freedoms and deserves special protection, as the context of its processing may pose significant risks.

Under the GDPR, health data are given higher levels of protection. First, as a general rule, the GDPR forbids the processing of health-related data. Here, it cover a number of exceptions to this restriction. Second, the GDPR views the processing of sensitive data including health data as one that may endanger the rights and liberties of natural persons. Fundamentally, there are circumstances where the GDPR considers the processing of personal health data to be at "high-risk." For instance, the GDPR requires controllers to conduct a DPIA in this situation because it recognises that a serious danger to the rights and freedoms of natural persons may occur when health data are handled on a wide scale. Although the GDPR is cautious to stress out that the processing of a patient's personal data by a single doctor or other health care professional would not be classed as "large-scale," this would include the scenario where a sizable hospital collects the patients' genetic and health data. Third, the GDPR forbids automated decision-making, including profiling, based on health data unless the data subject has given her explicit consent or processing is required for reasons of substantial public interest and appropriate safeguards are in place to protect the data subject's rights, freedoms, and legitimate interests.

Fourth, the GDPR expressly refers to the data subject's rights to access and information on their health data. These rights include the ability for data subjects to "access data concerning their health, for example, the data in their medical records containing information such as diagnoses, examination findings, assessments by treating physicians and any treatment or interventions provided." Finally, extra obligations are placed on controllers processing health data. These controllers must designate a Data Protection Office and retain records of processing operations, even if their organisation employs fewer than 250 people. Data Protection Officer and controllers and processors not based in the EU are required to name a representative in the Union if they process health data on a large scale.[25]

There are exceptions for these rules to be loosened. There are grounds or circumstances that permit the processing of health data in accordance with GDPR Article 9 paragraph 2. In terms of health care, the law allows the processing of patient data (without seeking consent) for preventive or occupational medicine, assessing working capacity, medical diagnosis, providing health or social care treatment, or managing health or social care systems and services. In such cases, it is critical to ensure that personal data can only be collected, used, or shared by a professional non-disclosure subject. For example, if the specialist needs to inform the general practitioner about the data subjects' health information, they do not need to obtain permission first.

While the GDPR provides a comprehensive and structured framework for the protection of health data, Malaysia's Personal Data Protection Act 2010 adopts a more limited approach. Although both regimes recognise core data protection principles, the divergence between them becomes particularly pronounced when examining the governance of health data processed through large-scale digital technologies such as contact tracing applications.

One of the most significant doctrinal differences lies in the scope of application. The GDPR applies broadly to both public

and private actors, including public authorities involved in healthcare administration and disease surveillance, subject only to narrowly defined exemptions. This ensures that the processing of health data by government bodies remains subject to legal scrutiny, even during public health emergencies. In contrast, the PDPA 2010 is confined to personal data processed in the context of commercial transactions and expressly excludes the Federal and State Governments from its application. As a result, much of the health data collected through state-led tracking technologies during the COVID-19 pandemic falls outside the direct reach of Malaysia's primary data protection statute. This structural limitation weakens legal accountability precisely in circumstances where large volumes of sensitive health data are centrally collected and processed.

A second key distinction concerns the legal basis and proportionality framework governing health data processing. Under the GDPR, the processing of personal data must satisfy a general lawful basis under Article 6 and, where health data is involved, an additional condition under Article 9. This dual-layer structure ensures that the processing of sensitive health data is justified not only by necessity but also by proportionality and appropriate safeguards. By contrast, while the PDPA 2010 requires explicit consent for the processing of sensitive personal data, its exceptions. Particularly those relied upon during emergencies. They are not accompanied by an equally rigorous proportionality analysis. Consequently, non-consensual health data processing in Malaysia risks becoming overly permissive, with limited statutory guidance on how necessity, scope, and duration should be constrained.

The accountability framework of the two regimes further highlights their divergence. The GDPR operationalises accountability through concrete governance mechanisms, most notably the requirement to conduct a Data Protection Impact Assessment (DPIA) where processing is likely to result in a high risk to the rights and freedoms of individuals, such as large-scale processing of health data.[22] DPIAs function as an ex ante safeguard, compelling data controllers to identify risks, assess proportionality, and implement mitigating measures before deployment. Although recent amendments to the PDPA 2010 have strengthened compliance obligations and expanded the responsibilities of data processors, the Malaysian framework still lacks an explicit and systematic equivalent to the GDPR's DPIA regime, particularly in the context of emergency health technologies.

Differences are also evident in relation to data security and breach governance. The GDPR establishes stringent security obligations and mandatory breach notification requirements, reinforcing data protection through enforceable transparency and oversight. Malaysia's 2024 amendments move in a similar direction by enhancing enforcement powers and strengthening security-related duties. However, the continued exclusion of government processing from the PDPA's scope means that these strengthened safeguards may not fully apply to public-sector health data infrastructures, where the risks associated with centralised databases and mass data collection are most acute.

Finally, the GDPR addresses automated decision-making and profiling with a level of specificity absent from the PDPA 2010. Article 22 of the GDPR restricts decisions based solely on automated processing that produce legal or similarly significant effects, particularly where special category data such as health data is involved. This is highly relevant in the context of digital contact tracing systems that may generate risk scores, access permissions, or behavioural restrictions based on health status. The PDPA 2010 does not provide a comparable doctrinal framework governing such practices, leaving potential gaps in protection against opaque or discriminatory automated outcomes.

Taken together, these differences demonstrate that the GDPR does not merely

offer stronger protection in abstract terms, but rather embodies a more institutionalised, risk-based, and rights-oriented regulatory model. For Malaysia, the lessons to be drawn from the GDPR are therefore specific and practical. These include the need to extend core data protection obligations to public-sector health data processing, to condition emergency-based exceptions on clear proportionality safeguards, to institutionalise impact assessment mechanisms for high-risk health data processing, and to strengthen transparency and oversight in the deployment of digital health technologies. Without such measures, the reliance on emergency justifications risks normalising intrusive data practices and undermining long-term trust in public health governance.

FINDINGS AND DISCUSSION

The legal situation of the COVID-19 tracking technology application in the European Union

For the benefit of public health, the GDPR establishes a number of exclusions and limitations to data privacy laws. For reasons of public interest in the field of "public health," the processing of sensitive data, including health data, is permitted. Access to preventative healthcare and the right to get medical treatment are protected under the terms of national laws and customs under Article 35 of the EU Charter of Fundamental Rights (EUCFR). The GDPR allows for the processing of health information when it is required to defend against "severe cross-border dangers to health" or maintain the highest levels of quality and safety for medical services, medications, and devices.[26]

Recital 46 GDPR states that processing may be carried out to serve both critical interests of the data subject and significant grounds of public interest, such as when processing is required for humanitarian efforts like tracking the spread of epidemics. The GDPR permits limitations on the data protection principles and the rights of data subjects where those actions are conducted for "public health" causes. It contains exceptions to both the right to be forgotten and the general rule that prohibits the transmission of personal data to nations outside the EU. It also covers the processing of personal data for "scientific research purposes," which includes basic, applied, and privately sponsored research as well as technological development and demonstration.[27] The general GDPR regulations also apply to those actions if the outcome of scientific study in the context of health justifies taking additional steps in the subject's best interests.

The European Union has assessed the two grounds outlined in the previous section to approve the deployment of tracking technology in the context of the COVID-19 epidemic. The European Data Protection Board (EDPB) issued a guideline in April 2020, titled "Guidelines 04/2020 on the Use of Location Data and Contact Tracing Tools in the Context of the COVID-19 Outbreak."

According to the recommendations, governments and corporate actors are turning to data-driven solutions to combat the COVID-19 epidemic, creating a variety of privacy concerns.[28] The EPDB emphasises that the legislative framework for data protection has been created to be flexible, allowing for both an informed response to the epidemic and the safeguarding of basic human rights and freedoms.

This guideline also emphasises the importance of deploying contact tracing applications during the COVID-19 pandemic, recommending that they be accompanied by support measures to ensure that the information provided to users is contextualised and that alerts may be useful to the public health system, or that such applications may not have their full impact.

Personal data in the domains of health data, geolocation data, and contact tracing data will be used in the implementation of contact tracing. This data will be used for two distinct objectives. The geolocation data is meant to aid in the

pandemic response by simulating viral propagation in order to assess the overall success of containment efforts. Contact tracing, on the other hand, is intended to notify individuals that they have been in close proximity to someone who is later verified to be a carrier of the virus in order to break the chains of contamination as soon as feasible. To what extent will the privacy of personal health data be protected in this case?

Such data may be transferred to authorities or other third parties only if it is anonymized by the provider or, with the prior approval of the users, for data revealing the geographical location of the user's terminal equipment that is not traffic data. The application's data collection for contact tracing is limited to and only during the pandemic. However, extra restrictions must be followed when it comes to the re-use of data (such as location data). It has been expressed in this respect, in accordance with paragraph 13 of the guidelines:

...when data have been collected in compliance with Art. 5(3) of the ePrivacy Directive, they can only be further processed with the additional consent of the data subject or on the basis of a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Art. 23 (1) GDPR.

The EPDB places a high value on the protection of personal health data. They believe that when utilising tracking applications, consumers should retain control over their data. National health authorities should be involved in the system's design. Close proximity between contact tracking applications should be permitted only anonymously and aggregately, with no citizen tracking, and the identities of possibly affected people should not be shared with other users. Contact tracing and warning applications should be made available to the public but should be disabled as soon as the COVID-19 situation is over, and any residual data should be erased.

The EPDB has already said that the use of contact tracing programmes should be optional and should not rely on individual movement tracing, but rather on proximity information for users.[29] Monitoring the whereabouts and/or interaction of natural people on a large scale is a significant invasion of their privacy. It can only be legitimised by depending on users' voluntary assent for each of the reasons at hand. This would imply that people who do not use or are unable to utilise these applications should not be penalised for doing so.

The EPDB also highlights in the rules for the processing of health data that applications for contact tracing entail the storage and/or access of information already saved on a terminal, which is subject to Art. 5(3) of the Directive on ePrivacy. If the processing is strictly necessary for the application's provider to perform the service explicitly requested by the user, the user's permission is not required. In the case of transactions that are not technically essential, the provider must get the user's approval.

They further point out that the voluntary use of contact tracking software does not always imply that personal data is used with consent. A government agency provides a service when it is granted a mandate by law and follows the rules of the law. The necessity to do anything in the public interest is the most significant legal premise for processing.

Furthermore, the EU has developed a toolkit for mobile applications to track the spread of COVID-19. With the assistance of the European Commission, Member States investigated the data protection and privacy aspects of different digital tools to combat the epidemic. Such applications should only be developed and implemented in close collaboration with and under the supervision of the relevant public health authorities. The contact tracing procedure in the region will be overseen by public health experts. They will adhere to international obligations that specify which contacts should be used and how they should be managed.

The standard approach mentioned in this publication is based on knowledge and best practises given by eHealth Network Member States. Nationally, public health authorities should publicly recognise the app's availability. Individual acceptance is contingent on the public's impression that they are effective, correct, discreet, and confident, that they avoid mass monitoring, and that they are firmly confined to the period of the current crisis. To prevent disproportionate data retention regulations, the data should only be stored for the period of the COVID-19 situation. Storage restrictions should take into consideration genuine demands as well as medical significance. Following that, all personal data should be erased or anonymized as a general practise.

To that end, it is critical to emphasise the subject of COVID-19 tracking apps since health data and their content are extremely sensitive and it is also critical to preserve the data owner's privacy. There is a risk that this data may be exploited, particularly in the example where mobile developers create false tracing apps for COVID-19. The EU built the data protection regulation to be flexible enough to enable an expedient reaction to the epidemic while also protecting core human rights and freedoms. By enacting a variety of laws and norms, EU institutions have demonstrated their ability to keep people's personal data private during times of crisis.

The Guidelines establish a legal framework for the deployment of monitoring technology in the EU, but the guidelines must first be applied to evaluate how they operate and what the challenges are that we can learn from and improve on. The most difficult task for the EU is persuading individuals who are conscious of their privacy to use the instruments.[30] For example, the Red Cross of Austria publishes the "Stop Corona" app in Austria, which was also one of the first nations in Europe to use coronavirus surveillance technology. Nonetheless, it has heightened public anxiety. The Austrian software uses a Bluetooth transmitter on users' phones to monitor other phones that come close to them. This preserves the information on the phone. If consumers do not wish to be monitored, they may simply remove the app and the data.

As a result of the COVID-19 epidemic, Italy is one of the worst-affected nations in the European Union.[31] Immuni, a mobile tracking application, is used to trace the contacts of those who have been infected. Italy's attempt to protect its citizens' privacy is based on adherence to European Commission standards. The information will only be used for a limited time, until the end of the year.

In contrast, the Netherlands unintentionally exposed data for tracking apps.[32] The Dutch personal data from the COVID-19 tracking apps was stolen early this year, and they are suspending use of the tracking technology applications to focus on resolving the problem.[33]

According to the Council of Europe's official report only Norway, Italy, Belgium, France, and Finland established specific laws and went through the appropriate preliminary steps to limit the tool's impact on fundamental rights.[34] The application is regulated by a set of rules. Parliament has also authorised two goals: 1) contact tracking; and 2) analysis of infection patterns and their influence on infection control (collectively). The app's (legal) purpose does not include symptom self-reporting.[35]

A few nations have made the source code of their applications open source in order to boost openness and create a greater degree of confidence among the general public in order to promote transparency and trust when implementing tracking technologies. As an important part of transparency, the disclosure of the source code may serve to generate confidence in the system and give a way of controlling the respect for privacy and data protection rights. There must also be assurances that data subjects' rights will be protected; confusing aims, contradictory signals about the legislation, and severe data minimisation

will only make them distrustful of the process.

Based on the above-mentioned circumstances in EU nations and the use of this technology, it is possible to conclude that the danger of data leakage is considerable, and it has already occurred.

To date, however, nations within the European Union have managed to retain the privacy element of monitoring technology use in compliance with the legal norms set by the GDPR via official recommendations.

Learning from the European Union for the betterment of Malaysia's health data privacy during COVID-19

The European Union model of data protection law is the legal standard for Malaysia's data protection. Based on this fact, the Personal Data Protection Act 2010 was legislated based on the spirit of the EU and aims to provide sufficient protection for personal data, including health data.[36] As compared to the EU, health data privacy in Malaysia is still underdeveloped and the government has not given adequate focus to the protection of the privacy of health data. During this pandemic, the usage of health data is vital with the application of tracking technology.[37] The COVID-19 pandemic necessitated the large-scale collection, storage, and processing of personal and health-related data to support public health interventions. The greater the amount of data collected, the greater the risk that the data will be compromised.

Based on the foregoing discussion, two principal lessons may be drawn from the European Union's experience that directly expose and respond to shortcomings within Malaysia's current health data protection framework under the PDPA 2010.

First, the EU demonstrates the importance of establishing a clear and publicly articulated legal standard governing the use of tracking technologies during public health emergencies. Under the GDPR, the deployment of contact tracing tools during COVID-19 was guided by dedicated regulatory instruments, particularly the European Data Protection Board's Guidelines 04/2020, which clarified permissible data uses, safeguards, and limitations. In contrast, Malaysia lacks a specific statutory or regulatory framework governing the collection and processing of health data through tracking technologies during emergencies. The PDPA 2010 does not provide tailored rules addressing large-scale public health surveillance, nor does it apply to government bodies that are the primary users of such technologies. This regulatory gap resulted in reliance on fragmented policies and general privacy notices, which are insufficient to provide legal certainty or accountability. Accordingly, Malaysia could benefit from adopting sector-specific guidelines that is modelled on the EU approach to articulate clear standards for health data processing during emergencies, even if such guidelines are non-binding in nature.

Secondly, the EU experience highlights the central role of transparency and trust as substantive governance mechanisms rather than mere formal obligations. Under the GDPR, transparency is operationalised through continuous disclosure obligations, accountability mechanisms, and supervisory oversight, particularly where consent is bypassed on public interest grounds. By contrast, transparency under Malaysia's PDPA framework is largely procedural and limited in practical effect, especially where government-led health data processing falls outside the Act's scope. While the PDPA recognises data subject principles and rights, these protections are significantly weakened in emergency contexts due to limited disclosure, uncertainty surrounding data retention and secondary use, and the absence of enforceable oversight mechanisms. The EU approach demonstrates that transparency must extend beyond basic notices to include meaningful disclosure of data governance practices, risk management measures, and retention limits. Without such mechanisms, public trust in health data processing cannot be sustainably maintained.

Finally, the EU framework illustrates how a contextual balancing of public health interests and data privacy rights can be achieved through a flexible yet structured legal regime. The GDPR explicitly recognises that public health imperatives may justify restrictions on individual privacy rights during emergencies, while simultaneously imposing safeguards such as necessity, proportionality, and purpose limitation. In Malaysia, although emergency measures enabled rapid data collection to curb COVID-19 transmission, the PDPA 2010 does not provide an equivalent doctrinal framework for balancing competing interests in a principled manner. The absence of explicit proportionality standards and sunset mechanisms risks normalising intrusive data practices beyond emergency contexts. The EU model demonstrates that flexibility need not come at the expense of rights protection, provided that emergency-based data processing remains legally bounded and temporally limited.

The EU experience does not merely offer abstract best practices but exposes concrete regulatory gaps in Malaysia's PDPA framework, particularly in relation to public-sector accountability, emergency-specific safeguards, and enforceable transparency. Addressing these gaps is essential if Malaysia is to strengthen health data privacy while maintaining effective public health responses in future crises.

CONCLUSION

The COVID-19 pandemic has brought up a number of problems with data privacy that have not yet been solved. But being vigilant about people's health isn't something new. The application of tracking technology in Malaysia is an effort made by the government to control COVID-19. Nevertheless, the application of tracking technology does come with a cost, even though it is for the benefit of people. Based on our arguments, data that is collected during pandemics and during public health emergencies is health data and is also categorised as sensitive data. Even though there is an emergency need for data to be processed without consent from data subjects, the data protection aspect should never be neglected. The PDPA, as the only data protection law available to protect personal data, could not be implemented due to its shortcomings, and by limiting its application to the government as the main body that collects personal data, we need to improve the protection of health data. If we are to say that Malaysia has adopted the model of the EU in legislating our own data protection law, the important question to be asked would be why are we so reluctant to prepare our own law as the EU, especially in terms of health data privacy? It is now possible and foreseeable that COVID-19 will live with us. It is no longer a pandemic rather an endemic. The possibility is that this data will be collected to the point where no one knows. Instead of preparing the law for temporary measures, why we cannot prepare for the worst? The state of a pandemic is currently approaching that of an endemic, which means the normalisation of health data processing should no longer be an emergency.

As compared to other nations and states throughout the world, the EU is known to embrace the fundamental right is privacy and its manifestation could be seen through the implementation of GDPR. The GDPR has a broad definition of health data and recognises that it needs more protection because it is sensitive. This shows that the EU legislators think the privacy of health data is an important interest that is often at risk and needs more protection. At the same time, the GDPR has a number of exceptions and limits when it comes to health data privacy. Some of these are based on the individual circumstances of data subjects, such as "explicit consent" or protecting the "vital interests" of the data subject, but most of them are about public health interests. The GDPR has exceptions for public health crises, which means that its' most strict provisions do not apply to technologies designed to combat pandemics, but the emergency situation does not allow for the

compromise of health data. Malaysia may learn a lot from the EU's use of tracking technology applications.

NOTES

[1] Bernama, Minister: Govt to Consult Public on Amendments to Personal Data Protection Law, The Malay Mail, Feb. 12, 2020, https://www.malaymail.com/news/malaysia/2020/02/12/minister-govt-to-consult-public-on-amendments-to-personal-data-protection-l/1836984. (last visited June 15, 2021).

[2] Ali Alibeigi, Malaysian Personal Data Protection Act, a Mysterious Application, *University of Bologna Law Review*, Vol.5: 362-74.

[3] Olivia Tan Swee Leng et al., Digital Tracing and Malaysia's Personal Data Protection Act 2010 amid the COVID-19 Pandemic, 1 *Asian Journal of Law And Policy* 47-62 (2021). SEE ALSO: Chui Yee Mun, Data Privacy: Tracing more than just contacts? *The Edge*.

[4] Matthew Sebastian (2021), Privacy and Ethical Concerns with Mysejahtera Mobile Contract Tracing App, 1 *Current Law Journal* 1-9.

[5] Abu Bakar Munir, Virtual Lecture on Personal Data Protection Law: EU GDPR VS Asian Laws". Lecture, Zoom Online.

[6] Emre Kursat Kaya (2023), Safety and Privacy in the Time of COVID-19: Contact Tracing Applications, *Centre for Economics And Foreign Policy Studies,* 1-9.

[7] Ibid.

[8] Anon, Living with the Endemic Coronavirus, The Sun Daily, July 27, 2021.

[9] Nuraisyah Chua Abdullah (2019), Legal Research Methodology, 17-30.

[10] Edwin Lee Yeong Cieh, Limitations of The Personal Data Protection 4 Act 2010 and Personal Data Protection in Selected Sectors", in *Beyond Data Protection* 65-78, SEE ALSO supra note 5.

[11] Leo Desmund Pointon & Jeong Chun Phuoc (2012), Personal Data Protection Cases and Commentary with Applied Syari'ah Principles 15-16 (CLJ Publications 2012). SEE ALSO Abu Bakar Munir et al. (2014), Data Protection Law in Asia 181-202.

[12] World Health Organization, Digital tools for COVID-19 contact tracing 2020.

[13] Ibid.

[14] Ibid.

[15] Ibid.

[16] Government of Malaysia, MySejahtera, FAQ MySejahtera 2021.

[17] Teoh Pei Ying (2020), Selangor introduces 'SElangkah' for Covid-19 contact tracing, *New Straits Times,* May 4.

[18] Supra note 4 and note 2.

[19] Majlis Keselamatan Negara, Emergency (Essential Powers) (No.2) Ordinance 2021.

[20] *Id* at page 5, note 10.

[21] Graham Greenleaf (2021), Asian Data Privacy Laws: Trade and Human Rights Perspectives.

[22] Magdalena Kędzior (2022), The Right to Data Protection and the COVID-19 Pandemic: The European Approach, 21 *ERA FORUM* 533-43.

[23] Trix Mulder (2019), The Protection of Data Concerning Health In Europe, *European Data Protection Law Review*, Vol.5: 209.

[24] Christopher Kuner et al. (2023), *The Eu General Data Protection Regulation (Gdpr): A Commentary*.

[25] Maria Tzanou, (2020), The GDPR and (Big) Health Data: Assessing the EU Legislator's Choices, in *The Gdpr And (Big) Health Data* 3-22.

[26] Article 9 (2) (i) GDPR.

[27] Recital 159 GDPR.

[28] European Data Protection Board, Review of Guidelines 04/2020 On The Use Of Location Data And Contact Tracing Tools In The Context Of The Covid-19 Outbreak, 1-19.

[29] Ibid.

[30] Michael Birnbaum & Christine Spolar (2020), Coronavirus Tracking Apps Meet Resistance in Privacy-Conscious Europe, *The Washington Post*, Apr. 18.

[31] Pietro Altomani et al. (2021), Contact Tracing Apps in Italy, *Norton Rose Fullbright*, June 19.

[32] Victoria Seveno, Data Leak Allows Anyone to Download Fake Coronacheck Certificate, *Iamexpat,* Mar. 16.

[33] Toby Sterling, (2020), Personal Data Stolen from Dutch Coronavirus Track-And-Trace Programme, Reuters, Jan. 29.

[34] Anne-Christine Lacoste & Sjoera Nas (2020), Digital Solutions to Fight COVID-19 Council *of Europe.*

[35] Ibid.

[36] *See supra* note 10. *See also supra* note 10 and 18.

[37] Victor V. Ramraj (2021), Covid-19 In Asia: Law and Policy Contexts, 10-31.

REFERENCES

Abdullah, N. C. (2019). *Legal research methodology* (pp. 17–30). Sweet & Maxwell.

Alibeigi, A. (2020). Malaysian Personal Data Protection Act: A mysterious application. *University of Bologna Law Review, 5*, 362–374. https://doi.org/10.6092/issn.2531-6133/12441
(Accessed August 17, 2021)

Altomani, P., et al. (2020, June 19). *Contact tracing apps in Italy*. Norton Rose Fulbright. https://www.nortonrosefulbright.com/-/media/files/nrf/nrfweb/contact-tracing/italy-contact-tracing.pdf
(Accessed September 21, 2022)

Anon. (2021, July 27). Living with the endemic coronavirus. *The Sun Daily*. https://www.thesundaily.my/home/living-with-the-endemic-coronavirus-AE8125222
(Accessed April 19, 2022)

Bernama. (2020, February 12). Minister: Govt to consult public on amendments to personal data protection law. *The Malay Mail*. https://www.malaymail.com/news/malaysia/2020/02/12/minister-govt-to-consult-public-on-amendments-to-personal-data-protection-l/1836984
(Accessed June 15, 2021)

Birnbaum, M., & Spolar, C. (2020, April 18). Coronavirus tracking apps meet resistance in privacy-conscious Europe. *The Washington Post*. https://www.washingtonpost.com/world/europe/coronavirus-tracking-app-europe-data-privacy/2020/04/18/89def99e-7e53-11ea-84c2-0792d8591911_story.html
(Accessed June 15, 2022)

Chui, Y. M. (2021, May 24). Data privacy: Tracing more than just contacts? *The Edge*. https://www.theedgemarkets.com/article/data-privacy-tracing-more-just-contacts
(Accessed July 21, 2021)

European Data Protection Board. (2021). *Review of Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak* (pp. 1–19). https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_20200420_contact_tracing_covid_with_annex_en.pdf

Government of Malaysia. (2021). *MySejahtera: FAQ*. https://mysejahtera.malaysia.gov.my/faq_en/ (Accessed September 22, 2021)

Greenleaf, G. (2014). *Asian data privacy laws: Trade & human rights perspectives*. Oxford University Press.

Kaya, E. K. (2020). Safety and privacy in the time of COVID-19: Contact tracing applications. *Centre for Economics and Foreign Policy Studies*, 1–9. https://www.jstor.org/stable/pdf/resrep26089.pdf
(Accessed March 8, 2023)

Kędzior, M. (2020). The right to data protection and the COVID-19 pandemic: The European approach. *ERA Forum, 21*, 533–543. https://doi.org/10.1007/s12027-020-00644-4
(Accessed June 15, 2022)

Kuner, C., et al. (2020). *The EU General Data Protection Regulation (GDPR): A commentary*. Oxford University Press.

Lacoste, A.-C., & Nas, S. (2020). *Digital solutions to fight COVID-19*. Council of Europe. https://rm.coe.int/prems-

120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c
(Accessed May 18, 2022)

Lee Yeong Cieh, E. (2013). Limitations of the Personal Data Protection Act 2010 and personal data protection in selected sectors. In *Beyond data protection* (pp. 65–78). Springer.

Leng, O. T. S., Vergara, R. G., & Khan, S. (2021). Digital tracing and Malaysia's Personal Data Protection Act 2010 amid the Covid-19 pandemic. Asian Journal of Law and Policy, 1(1), 47–62.

Majlis Keselamatan Negara. (2021). *Emergency (Essential Powers) (No. 2) Ordinance 2021*. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2021/03/Ordinan-Anti-Berita-Tidak-Benar-20211.pdf
(Accessed January 4, 2022)

Maamedicare. (2020). *MySejahtera*. https://maamedicare.org/kidney_charity_fund/pdf/covid19/Annex_42_MySejahtera.pdf
(Accessed September 21, 2021)

Mulder, T. (2019). The protection of data concerning health in Europe. *European Data Protection Law Review, 5*, 209.

Munir, A. B. (2021, August 18). *Virtual lecture on Personal Data Protection Law: EU GDPR vs Asian laws* [Lecture]. Zoom Online. https://fh.unpad.ac.id/a-virtual-lecture-on-personal-data-protection-law-eu-gdpr-v-asian-laws-by-professor-abu-bakar-munir-at-international-islamic-university-malaysia/

Pointon, L. D., & Phuoc, J. C. (2012). *Personal data protection cases and commentary with applied Syari'ah principles*(pp. 15–16). CLJ Publications.

Ramraj, V. V. (2021). *COVID-19 in Asia: Law and policy contexts* (pp. 10–31). Oxford University Press.

Sebastian, M. (2021). Privacy and ethical concerns with MySejahtera mobile contact tracing app. *Current Law Journal, 1*, 1–9.

Seveno, V. **(**2021, March 16). Data leak allows anyone to download fake CoronaCheck certificate. *IamExpat*. https://www.iamexpat.nl/expat-info/dutch-expat-news/data-leak-allows-anyone-download-fake-coronacheck-certificate
(Accessed February 16, 2022)

Sterling, T. (2021, January 29). Personal data stolen from Dutch coronavirus track-and-trace programme. *Reuters*. https://www.reuters.com/article/us-health-coronavirus-netherlands-datapr-idUSKBN29Y1H3
(Accessed August 16, 2022)

Tan, S. L. (2020, May 4). Selangor introduces "SElangkah" for COVID-19 contact tracing. *New Straits Times*. https://www.nst.com.my/news/nation/2020/05/589727/selangor-introduces-selangkah-covid-19-contact-tracing
(Accessed August 18, 2021)

Tzanou, M. (2020). The GDPR and (big) health data: Assessing the EU legislator's choices. In *The GDPR and (big) health data* (pp. 3–22). Routledge.

World Health Organization. (2020). *Digital tools for COVID-19 contact*

tracing. https://apps.who.int/iris/bitstream/handle/10665/332265/WHO-2019-nCoV-Contact_Tracing-Tools_Annex-2020.1-eng.pdf (Accessed October 28, 2021)