Journal of Information and Knowledge Management (JIKM) Vol 1 Special Issue (2022)

Personal Data Abuse: Preliminary Survey Among Malaysian Youth Netizens

Huda Hamidon[1], Salliza Md Radzi[2], Noor Rahmawati Alias[3], Noorfadzilah Arifin[4], and Zuriani Ahmad Zukarnain[5]

[1,2,3]Faculty of Information Management,
UiTM Kelantan Branch, Machang Campus, 18500 Machang, Kelantan, Malaysia
[4,5]Faculty of Computer and Mathematical Sciences,
UiTM Kelantan Branch, Machang Campus, 18500 Machang, Kelantan, Malaysia

Email: huda685@uitm.edu.my

Received Date: : 30 August 2022
Accepted Date: 21 September 2022
Published Date: 1 November 2022

Abstract. Data privacy is concerned with the proper handling of sensitive data that must be protected from unauthorized parties. Given the prevalence of internet activity among Malaysians, instilling a sense of personal data protection awareness at a young age is critical. This paper aims to assess Malaysian youth netizens' knowledge of personal data and data protection awareness of personal data abuse. The methodology used was a descriptive study using online survey questionnaires as their primary tool. The random sampling method was used in the data collection process, which included 213 respondents. The findings indicate that while many respondents were uninformed of data protection, they were knowledgeable about personal data in general. Lack of data protection awareness prevents internet users from taking the necessary steps to stop further misuse of personal data, such as reporting it to the relevant authorities including the Malaysian Department of Personal Data Protection (JPDP).
Keywords: Personal data, data abuse, data protection law, information management.

1 Introduction

Information and communication technology (ICT) advancements have produced a variety of new tools that make it easier for people to carry out their daily activities. The interest and demand for the Internet and online apps have expanded as a result of a variety of online services offered by numerous parties. As reported by the Malaysian Communications and Multimedia Commission (MCMC) in 2020, there were 14% more heavy internet users in Malaysia who spent more than 12 hours a day online. There are

various factors that lead to the increase in Internet use. One of the primary reasons for increased Internet use was the Movement Control Order (MCO), which was implemented in response to the COVID-19 outbreak. Users rely on the Internet to work from home, interact with others, obtain information, and engage in online learning (MCMC, 2020).

Through a media statement issued by the Department of Statistics Malaysia on 12 April 2021 related to the use and access of ICT by individuals and households for the year 2020, internet usage among Malaysians aged 15 and above climbed significantly from 84.2 percent in 2019 to 89.6 percent in 2020. E-learning, e-health, e-government, e-commerce, and e-entertainment are among the popular services in Malaysia (The Office of Chief Statistician Malaysia, 2021). As more individuals access and use online services, it is crucial to start spreading knowledge and awareness about how to stay safe online as soon as possible.

In Malaysia, a total of 10,016 incidents of cyber events were reported to Cyber999 from January to December 2021 (Malaysia Computer Emergency Response Team, 2022). According to a 2018 study conducted by Javelin Strategy & Research, teens or minors are more vulnerable after a data breach than adults. According to the findings, 39 percent of teens were victims of a data breach, compared to only 19 percent of adults (Javelin Strategy & Research, 2018). The concerns about the risk to the younger generation arise because of their increased susceptibility to cyber security risks as a result of internet addiction, a lack of education on digital citizenship, and inadequate parental supervision and guidance (Nor Ain Mohamed Radhi, 2022).

Privacy paradox is defined as Internet users who claim to care about privacy issues but act in a contradictory manner. This situation demonstrates that online users continue to underestimate the importance of data privacy. Nowadays, data privacy is a contentious issue and there are a growing number of articles in the media that discuss digital rights and privacy concerns (Calzada, 2022). Maintaining the privacy of sensitive data is one of the key concerns that Internet users need to be aware of. However, it has been observed that an increasing number of internet users are openly exposing their personal information due to the emergence of numerous and useful social media platforms (Madden et al., 2013).

Whether users share information voluntarily or it is taken from them unknowingly, both pose a risk of identity theft and information misuse. In addition, when users interact directly or indirectly using various devices, whether computers or smartphones, it is certain that the user will leave behind data traces and digital footprints that can be used by third parties to process the data so that they know about the user's life, interests and activities (Addae, Brown, Sun, Towey & Radenkovic, 2017).

According to earlier surveys, there has been a gradual rise in the number of incidents involving young people misusing their personal information (Nurul ‘Ain Ahmad & Nooraini Othman, 2019). This further reinforces the notion that education and awareness of data protection need to be given at an early age. The aims of this paper are:

i. To identify the knowledge state of personal data among Malaysian netizens.

ii. To identify data protection awareness on personal data abuse among Malaysian netizens.

2 Literature Review

2.1 Personal Data

Malaysian Department of Personal Data Protection defined personal data as any information that was used in a business transaction, directly or indirectly related to a data subject who might be recognised from that information is referred to as personal data. Regardless of the source, data can be recorded manually or electronically and can include both objective and subjective information. This includes everything from basic information (such as name, address, and identity card number) to sensitive information (such as person's physical or mental health, political opinions, religious beliefs), as well as any other information that may from time to time be specified by the Minister under the Malaysian Personal Data Protection Act (Malaysia JPDP, 2021).

The European Commission defined personal data as any information that can be used to identify or locate a living person. This also includes various pieces of information that, when combined, can lead to the identification of a specific person. Information like an Internet Protocol (IP) address, cookie ID and location data are also regard as personal data (European Commission, 2022).

As stated in the Privacy Protection Act of Australia, personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether it is true or false and whether it is materially recorded or not (Neilsen & Chowns, 2012). According to Skendžić et al., (2018), personal data belong to natural persons and cannot be transferred. However, with the development of technology and the Internet, personal information is becoming more disclosed and made public thus accessible to those who may use it for their own illegal purposes.

2.2 Data Protection Awareness

Data protection can be defined as the process of safeguarding and protecting important information from corruption, compromise, or loss (Crocetti et al., 2021). Data protection terminology is also closely related and is often equated with data privacy and information privacy. Tiganoaia et al., 2017 mentioned, to avoid incidents and unpleasant situations, personal data such information, photos, videos, etc. need to be protected when using social media accounts. Personal and sensitive data must always be taken care of so that it is not misused or abused by irresponsible parties. The question is, to what extent can users share information given that among the purposes of their online activities is for building a career or doing business, socializing and meeting new acquaintances. Nowdays, protecting personal data has become one of the top concerns of society after various incidents and events that have led to the unauthorized disclosure of data by thousands of people around the world (Wright et al., 2019). Furthermore, the use of, or unauthorized access to, personal data is one of the primary concerns of owners

who share data with organizations (Alejo et al., 2019). In meeting certain needs, there must also be a balance in the sharing of information so that the privacy of information is maintained.

In privacy education, an emphasis on privacy risks associated with information disclosure would be effective to trigger the motivation to protect privacy for netizens (Youn, 2009). Netizens should be made informed of the reverse effects of privacy erosion. Personal data and privacy may be abused due to various reasons such as social and economic discrimination, be it on the capacity of consumers or the public (Acquisti et al., 2015). Netizens in Malaysia may be given more information and training on how to make decisions while using their personal data on the Internet, especially in the process of online application of commercial transactions and how they manage their passwords and usernames (Rahim et al., 2019). Netizens, especially youngsters, should be equipped with adequate awareness of the issues of data privacy and be guided on Internet usage to ensure their maturity level can justify better decision-making in any internet transactions involving personal data. This can be accomplished through cybersecurity awareness programs that instruct participants on how to avoid harmful online conduct (Yuliana, 2022).

Researchers who have studied youth characteristics on the Internet suggest that they should be given enhanced levels of awareness on personal data privacy issues. Youths are associated with their eagerness in sharing information on the Internet and their keenness in exploring it but are less careful about the safety measures, security practices, and reliability of Internet applications that they use. They also tend to be misled and distracted by misleading information as well as being victims of cyber threats (Rahim et al., 2019).

Privacy is often regarded as a form of freedom from social, economic, and institutional influences (Masur, 2020). Online privacy literacy is one of the ways to improve awareness of data protection. Netizens will become more equipped with the technical aspects, as well as the rules and regulations pertaining to data protection. They will also be able to apply suitable strategies to manage their online privacy, thus preventing oversharing and breaching of individual privacy.

2.3 Data Oversharing vs Personal Data Breach

Data protection can be difficult and risky due to internal and external factors. Internal factors include oversharing when netizens share excessive amounts of data. Oversharing, as defined by Cambridge Dictionary, is when somebody reveals too much information about his or herself (Cambridge Dictionary, 2021). More or less the same, data disclosure means sharing any information voluntarily (Tatum, 2021). Satista.com reported that in 2020, Malaysians perform the most online content sharing on social media (86.5%), followed by group messaging (58.5%) and private messaging (36.1%). Other platforms used are email, blogs or personal websites, and forums (Müller, 2021).

Based on the MCMC's Internet User Survey 2020, it was discovered that most Internet users (80.3%) revealed their real names, a 55 percent increase over 2016. In Malaysia, internet users also voluntarily disclosed their dates of birth (65.2%) and self-

portrait images (76.7%) (MCMC, 2020). However, it is a bit worrisome when the majority of respondents claimed that they take online privacy seriously.

Among the privacy impacts associated with online social networks include stalking, identification of profile owners such as through facial re-identification as well as shared demographic data (Gross & Acquisti, 2005). According to Joseph Turow in Penn Today, hackers can use any piece of information people share, and from the basic information or pictures posted, they can deduce information which in turn reveals many other details (Patel, 2020). Therefore, if users themselves willingly or unwittingly share their personal data, this will make it easier for cyber criminals to steal their data or information. There are also previous studies mentioning that, in the online environment, it is sometimes mandatory or a requirement for an individual to voluntarily disclose personal data that organisations can easily analyse using various modern technology applications (Agyemang et al., 2015). This is common now as many applications and online platforms require registration for anyone who wants to use a service from the organization or business.

Regarding external factors, one of them is data breach which occurs when the confidentiality of data is violated. Data breaches occur when an individual's personal information including name, social security number (SSN), and passwords are compromised and put at unauthorized risk of use, either on paper or in electronic format, for fraudulent purposes including identity theft (Holtfreter & Harrington, 2015). Beside that, Thomas et al., 2017 found during March 2016 to March 2017, almost 800 thousand potential victims of commercial keyloggers have been indentified, 12.4 million potential phishing kit victims, 1.9 billion usernames and passwords exposed in data breaches and traded on black market forums.

Since practically all actions and transactions that people engage in online are tracked by data brokers, maintaining the privacy of that data is incredibly difficult (Campbell et al., 2020). A data broker, also known as an information broker or information reseller (TechTarget, 2013), is a company that collects information by purchasing data from certain parties such as credit bureaus and telecommunication and technology companies. In addition, a person who seeks information either by using the telephone, Internet, or other printed materials for clients can also be considered as a data broker (Davis, 2021).

Singapore Personal Data Protection Commission reported that individuals whose personal data have been compromised (the "affected individuals") can be exposed to significant harm if they do not take steps to protect themselves (Personal Data Protection Commission Singapore, 2021). However, there are many limited studies that have examined the impact of data breaches from an individual's perspective (Valecha et al., 2016). Gatzlaff and McCullough (2010) claim that both people and businesses face serious dangers as a result of data breaches involving consumer or employee data. For instance, theft of customer or staff personal information may expose people to credit card fraud. In addition, the affected people could be blackmailed by impersonating them to obtain goods and services, sell copies of their data, or spam their email accounts (Phua, 2009). However, businesses that are impacted by this issue might have to pay for security upgrades as well as fines or other penalties related to the breach.

Additionally, companies may incur costs resulting from litigation that stems from potential liability exposure (Gatzlaff & McCullough, 2010).

A personal data breach can also occur when employees share confidential data of their clients or stakeholders that they need to process with any unauthorised parties in any business transactions or services, whether intentionally or unintentionally. Tolsdorf et al. (2022) commented that employees who handle personal data on the job are essential to privacy protection. They must abide by strict data protection regulations and take appropriate measures to safeguard personal information. For these personnel to be able to comply with privacy rules, it is advisable for the employers to provide them with any proper tools.

2.4 Data Protection Law

In Malaysia, the Department of Personal Data Protection or known as Jabatan Perlinungan Data Peribadi (JPDP) has channeled information related to data protection through their official portal page which can be reached at the address https://www.pdp.gov.my/jpdpv2/?lang=en. It can be accessed by anyone to make references, inquiries and access PDPA 2010 documents directly.

The Malaysian government enacted the Personal Data Protection Act (PDPA) 2010 to hinder the practice of personal data misuse by certain parties involved in non-governmental transactions. Several legal provisions under the Act were specifically made to control the illegal use of personal data regarding commercial transactions. Personal data of the public can be collected, managed, and shared by parties that are licensed by the government to process and use that data (Chen & Ismail, 2013; Pitchan & Omar, 2019). PDPA 2010 defines "personal data" as any information with respect to commercial transactions, which:

i. is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
ii. is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
iii. is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system

The internet users' awareness of the existence of certain cyber laws to safeguard and prevent users from committing cyber threats as well as becoming the victims of any cyber attack is very important. Some users think that they are not obliged to take note of the laws and that they feel unthreatened when using the Internet. The level of awareness among the youths in Malaysia regarding the existence of personal data protection law and knowledge of how this law can provide protection still needs to be improved (Markom et al., 2019). The awareness of both data users and data subjects is important to ensure the efficacy of the Act since data users need to give respect to data subjects' rights and data subjects need to understand their personal data rights and ownership (Chen & Ismail, 2013).

The first division of the Act consisting of sections 5 until section 12 provides the personal data protection principles, outlining the general principle, the notice and choice principle, the disclosure principle, the security principle, the retention principle, the data integrity principle, and the access principle (PDPA, 2010). The following table shows the extraction of legal provisions on seven personal data protection principles that data users must comply with when they process personal data.

Table 1: Legal Provisions on Personal Data Protection Principles

No	Sections and Principles	Legal Provisions
1	Sec. 6: General Principle	A data user may process personal data about a data subject if the processing is necessary— *(a)* for the performance of a contract to which the data subject is a party; *(b)* for the taking of steps at the request of the data subject with a view to entering into a contract; *(c)* for compliance with any legal obligation to which the data user is the subject, other than an obligation imposed by a contract; *(d)* in order to protect the vital interests of the data subject; *(e)* for the administration of justice; or *(f)* for the exercise of any functions conferred on any person by or under any law.
2	Sec.7: Notice and Choice Principle	A data user shall by written notice inform a data subject— *(a)* that personal data of the data subject is being processed by or on behalf of the data user, and shall provide a description of the personal data to that data subject; *(b)* the purposes for which the personal data is being or is to be collected and further processed; *(c)* of any information available to the data user as to the source of that personal data; *(d)* of the data subject's right to request access to and to request correction of the personal data and how to contact the data user with any inquiries or complaints in respect of the personal data; *(e)* of the class of third parties to whom the data user discloses or may disclose the personal data; *(f)* of the choices and means the data user offers the data subject for limiting the

No	Sections and Principles	Legal Provisions
		processing of personal data, including personal data relating to other persons who may be identified from that personal data; *(g)* whether it is obligatory or voluntary for the data subject to supply the personal data; and *(h)* where it is obligatory for the data subject to supply the personal data, the consequences for the data subject if he fails to supply the personal data.
3	Sec.8: Disclosure Principle	No personal data shall, without the consent of the data subject, be disclosed— *(a)* for any purpose other than— i. the purpose for which the personal data was to be disclosed at the time collection of the personal data; or ii. a purpose directly related to the purpose referred to in subparagraph (i); or *(b)* to any party other than a third party of the class of third parties as specified in paragraph 7(1)(e).
4	Sec. 9: Security Principle	A data user shall, when processing personal data, take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction by having regard— *(a)* to the nature of the personal data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction; *(b)* to the place or location where the personal data is stored; *(c)* to any security measures incorporated into any equipment in which the personal data is stored; *(d)* to the measures taken for ensuring the reliability, integrity and competence of personnel having access to the personal data; and *(e)* to the measures taken for ensuring the secure transfer of the personal data.

No	Sections and Principles	Legal Provisions
5	Sec. 10: Retention Principle	(1)The personal data processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose. (2)It shall be the duty of a data user to take all reasonable steps to ensure that all personal data is destroyed or permanently deleted if it is no longer required for the purpose for which it was to be processed.
6	Sec. 11: Data Integrity Principle	A data user shall 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.
7	Sec. 12: Access Principle	A data subject shall be given access to his personal data held by a data user and be able to correct that personal data where the personal data is inaccurate, incomplete, misleading or not up-to-date, except where compliance with a request to such access or correction is refused under this Act.

The Government will continue to improve the PDPA 2010 (Act 709) from time to time as needed by obtaining the views of various parties (BERNAMA, 2020). It should be noted that PDPA 2010 does not cover the practice of government offices in handling and using citizens' personal information. Instead, it regulates the use of publics' personal data for commercial transaction purposes only. The sophistification of information technology in processing the personal data may raise concerns regarding security, confidentiality, and privacy protection of personal information. Therefore, the sufficiency and sustainability of current data protection principles and the associated rights of individuals under the Malaysian Personal Data Protection Act (PDPA) must contend with issues when using advanced technological applications of data processing (Dali et al., 2022).

Alibeigi and Munir (2020) commented that comparative and descriptive methods of examination and study of the PDPA's application and scope reveal that the Act has a limited reach and several exemptions. This might make it more difficult to secure people's privacy using a common legal framework for personal data protection. However, a study on the compatibility gaps between blockchain and PDPA has identified few elements that make a blockchain application PDPA compliant (Baskaran et al., 2020).

The Malaysian government established the Personal Data Protection Department or Jabatan Perlindungan Data Peribadi (JPDP), an agency under the Ministry of Communications and Multimedia (KKMM) in 2011 to enforce and regulate PDPA in

the country. Its vision is to advance national prosperity in line with the Malaysian National Transformation Agenda by becoming be a leader in protecting personal data. Among its significant functions are to coordinate and oversee issues connected to the Personal Data Protection Act's provisions for the registration of user forums and consumer data. It enforces and promotes data privacy culture to foster an environment of trust among firms and consumers, which increases consumer trust in business dealings.

In enforcing the PDPA, JPDP has been given the authority to register all classes of data users under the order of the responsible Minister. JPDP consists of five main divisions, namely the Registration and Operation Division, Monitoring Division, Information Technology Unit, Management Services Unit and Corporate Communications Unit (JPDP, 2021).

3 Methodology

3.1 Research Instruments

This study has adapted the questions based on a study by Human Dynamics in association with IPS Institute, AlmavivA S.p.A, Czech Office for Personal Data Protection OPDP and Privacy International. The study is entitled "Public Awareness for the Right for Personal Data Protection" and was conducted to support the Directorate for Personal Data Protection.

However, to ensure the suitability of the questions with the situation in Malaysia, the researchers have modified the questions and set the breakdown into three main sections. The first section is on demographic details to classify respondents. Then, the question set in the second section is to identify respondents' knowledge of personal data. The final section is on data protection awareness. Table 2 shows a more detailed mapping of the questionnaire components based on the three sections for this study.

Table 2: Questionnaire Components

Section	Component	Topic
Section A	Demographic details	• Gender • Nationality • Race • Age group • Educational level • Employment • Residence
Section B	Knowledge on personal data	• Knowledge on personal data • Information that is considered as personal data • Knowledge on privacy rights and personal data protection

Section	Component	Topic
		• Concerns over data misuse
Section C	Data protection awareness	• Data abuse experience • Organization that is perceived to have misused the data • Impacts on data misused • Knowledge to protect personal data • Data misused on some social media network • Knowledge on Malaysia Personal Data Protection Department (JPDP) • Knowledge about the Personal Data Protection Act 2010

3.2 Research Methodology

This research applied descriptive analysis using SPSS software, implementing a quantitative research approach by using online survey questionnaires as the main instrument. The random sampling method was utilized in the data gathering process involving 213 respondents among Malaysian youth netizens. The sample size matches the rule of thumb written by Uma Sekaran in Research Method for Business 4th Edition (2003) in which a sample size that is larger than 30 and less than 500 is appropriate for most research.

4 Result and Discussions

This survey was answered by 213 respondents involving netizens in Malaysia where the response time took approximately 5-10 minutes. The questionnaire contains 23 questions and are included in three sections, namely Demographic Details (Section A), Knowledge of Personal Data (Section B), and Data Protection Awareness (Section C). There are 7 items in Section A, followed by 4 items in Section B and 12 items in Section C. To facilitate all the respondents involved, the researchers provided the questions in Malay and English. The findings of this survey will be further discussed by focusing on respondents' views on data protection.

4.1 Section A. Demographic Details

This survey involved 140 female (65.7%) and 73 male respondents (34.3%) with the majority of 166 respondents (77.6%) aged 15-24 years old. 149 respondents (70%) have

a level of education at the tertiary level while the remaining are at the secondary and primary school level. 154 respondents (72.3%) are unemployed, and 93 of the total respondents (43.7%) live in urban areas followed by 78 (36.6%) in suburbs and 42 (19.7%) in rural areas.

4.2 Section B. Knowledge of Personal Data

For this section, 206 respondents (96.7%) claimed to know what personal data is. Identity card information (99.5%) is the most prominent type of data that respondents regarded as their personal data, as seen in Figure 1. It is encouraging to know that the respondents gave this response, indicating that they will do their best to safeguard the data. Identity card and passport information is a piece of personally identifiable information (PII) that allow identifying a person uniquely. This can happen when quasi-identifiers are combined (Frankenfield, 2022).

Besides identity card, respondents are also aware and informed that sensitive data includes financial information (91.5%) and residence address (93.9%). Respondents also considered that their parents' information (88.7%), full name (76.5%), and health data (70.9%) are among the top sensitive data.

From the 213 respondents, more than half, or 141 respondents (66.2%) admitted that they knew and were very knowledgeable about their rights to privacy and protection of personal data. Figure 2 illustrates which personal information people are worried will be misused, with identity card data (98.1%), financial information (89.7%), and personal information (75.6%) being among the most feared categories. Other categories include information related to work, health, nationality, religion, politics, and others. The result shows that most of the respondents are having factual or declarative knowledge as explained by Trepte et al., (2015).

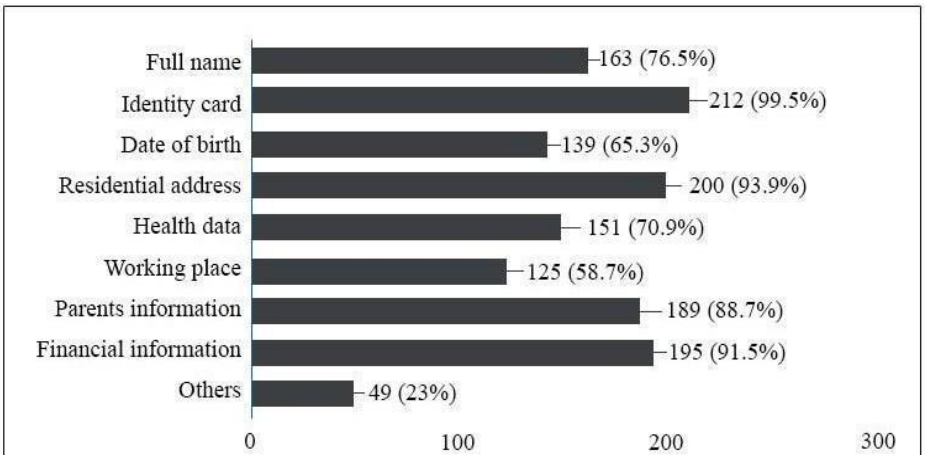

Figure 1: Information Considered as Personal Data

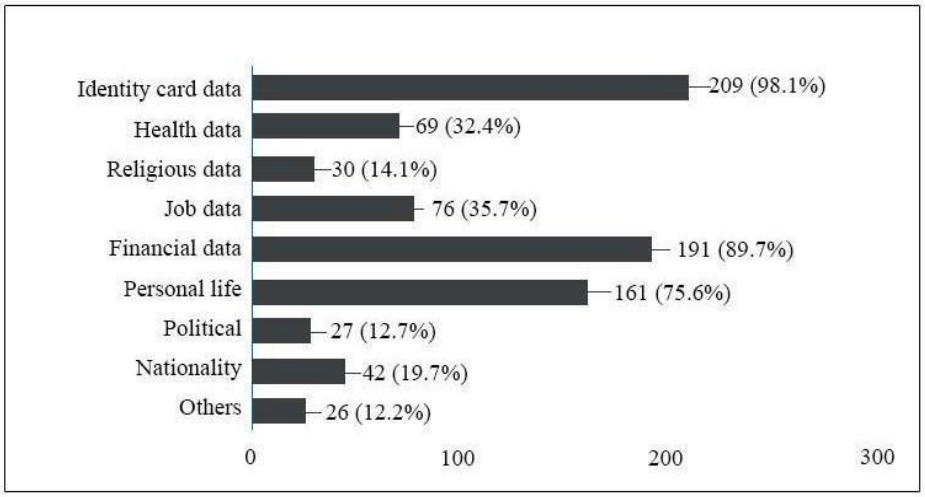

Figure 2: Personal Data Types Most Concerned About Misuse

4.3 Section C. Data Protection Awareness

Figure 3 demonstrates that, of the 213 respondents, 106 (49.8%) acknowledged that their personal information had not been exploited. On the other hand, 82 respondents were unsure (38.5%) and only 25 agreed (11.7%) that their personal data had been misused.

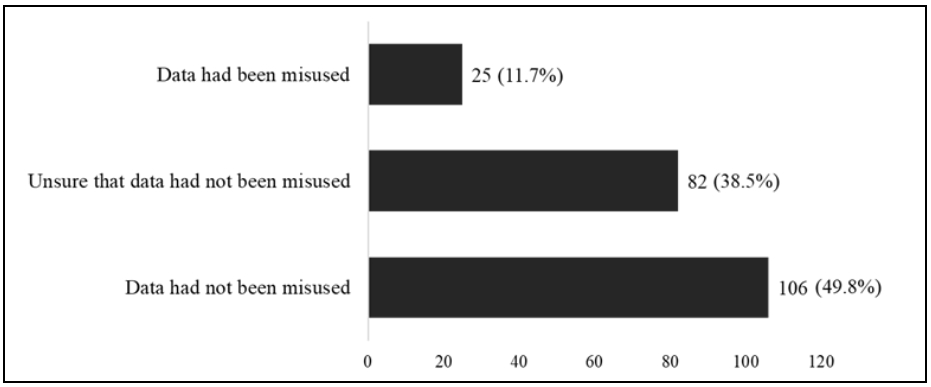

Figure 3: Data Misused

Figure 4 below shows that 63.2% of respondents believed that telecommunication operators had misused their personal data, followed by banks and financial institutions (52.6%), insurance companies (47.4%), marketing firms (47.4%), and other parties. These findings are based on additional responses obtained from 25 respondents who

agreed that their personal data had been misused. These respondents were permitted to select from multiple answers.

When using online services for operators, it is simple to discover the truth of the absence of a guarantee for the protection of personal data information in modern life. Many personal data leaks have been found to be freely shared with the public and this can be dangerous if mishandled (Sabowo et al., 2022). Victims are greatly impacted by the improper use of data by irresponsible parties. Identity theft (50%), loss of faith in people (45.2%), and financial loss (42.9%) were the three primary impacts experienced by respondents. Not only that, but this issue additionally has an impact on their life, leading to the loss of some people's jobs, strained friendships, ties to family, and unsettled emotions.

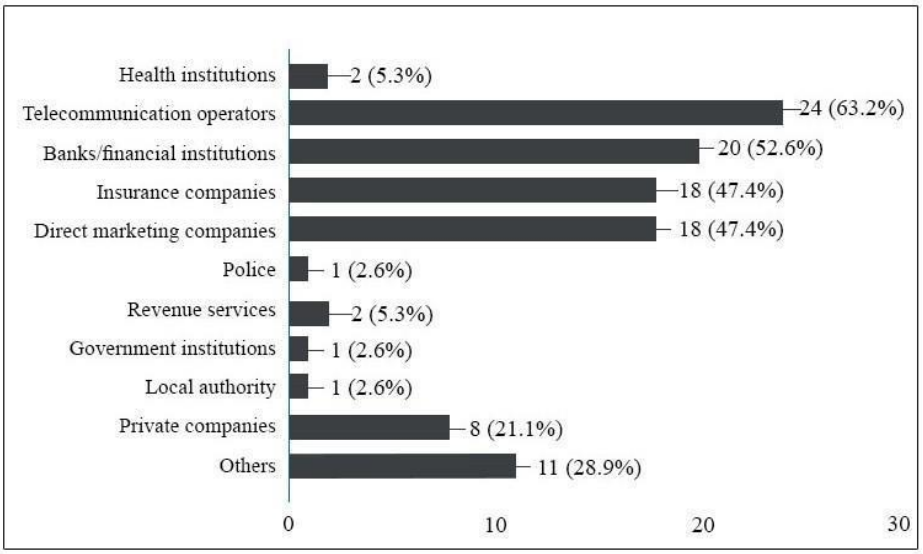

Figure 4: Parties Deemed of Misusing Personal Data by Respondents

This study found that 49.8% or 106 respondents agreed that they know how to protect their personal data, with the remaining 107 (50.2%) answering not sure or no. Additionally, the results revealed that just 100 (46.9%) respondents claimed to be aware of what to do if their personal information has been misused on social media. The actions taken by the respondents include reporting to the Malaysian Department of Personal Data Protection (JPDP) (43.8%) and relevant authorities (32.1%), followed by reporting to social media administrators (20.5%) as shown in Figure 5 below.

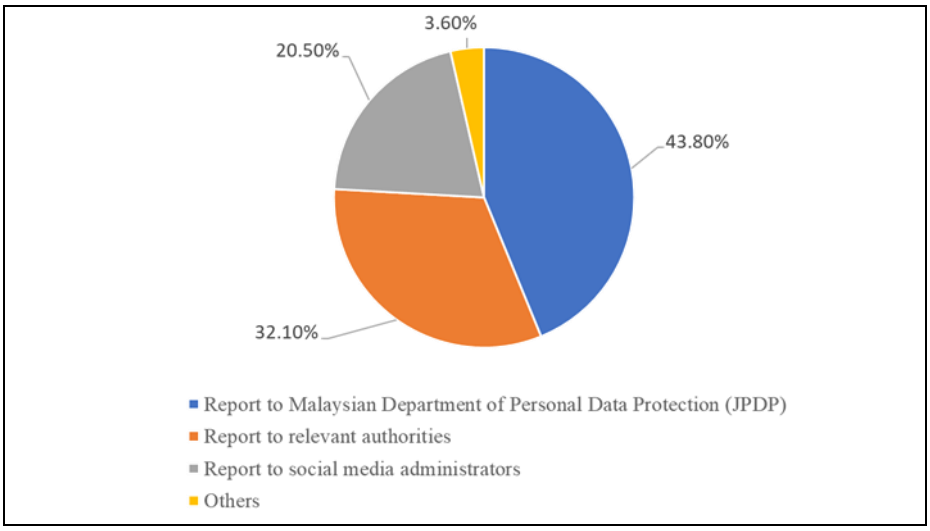

Figure 5: Action Taken by Respondents upon Data Misused on Social Media

The finding also shows that only 94 respondents (44.1%) admitted that they have heard of Malaysian Department of Personal Data Protection (JPDP) from various media like the Internet (72.3%), television (72%), radio (19.8%), others (23.8%) and newspaper (13.9%). 73 out of 94 respondents (70.2%) who have heard about JDPD also agreed that they knew about the role of the department.

In terms of awareness of personal data protection law, generally, only 92 (43.2%) out of 213 respondents knew about PDPA Act 2010 in Malaysia and only 39.8% of respondents were familiar or very familiar with the Act. This finding is consistent with Markom et al., (2019), who stated that the level of awareness among Malaysian youths about the existence of personal data protection laws, as well as knowledge about how this law can provide protection, needs to be improved.

5 Conclusions

According to the findings, most respondents know and understand some of the data that is considered personal and are aware that the data needs to be protected. This means that they understand personal data and have a good understanding of privacy rights and personal data protection. Nonetheless, some of them still experience being victims of personal data exploitation by irresponsible parties.

Through this research, it was discovered that more than half of the respondents were unaware of data protection in the context of the responsible authority, specifically the Malaysian Personal Data Protection Department (JPDP) of MCMC and the regulating act, known as PDPA 2010. Lack of data protection awareness hinders the netizens from making appropriate actions to prevent further personal data misuse such as reporting to the Malaysian Department of Personal Data Protection (JPDP) and

relevant authorities. More initiatives should be planned by relevant authorities to raise Malaysian netizens' awareness of personal data protection, particularly regarding procedural knowledge.

Since this study only focuses on data protection among youth netizens or data subjects, it is recommended that future research will focus more on the data users or the entities who use and process personal data as defined in the PDPA 2010.

References

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514. doi:10.1126/science.aaa1465

Addae, J. H., Brown, M., Sun, X., Towey, D., & Radenkovic, M. (2017). Measuring attitude towards personal data for adaptive cybersecurity. *Information & Computer Security*

Agyemang, O. S., Fantini, G., & Frimpong, J. (2015). Does country-level governance enhance ethical behaviour of firms? An African perspective. *International Journal of Law and Management*.

Alejo, C., Navarro-Ruiz, A., & Mauricio, D. (2019, August). Reference model for personal data protection in the Peruvian microfinance sector. In *2019 IEEE XXVI International Conference on Electronics, Electrical Engineering and Computing (INTERCON)* (pp. 1-4). IEEE.

Alibeigi, A., & Munir, A. B. (2020). Malaysian Personal Data Protection Act, a mysterious application. *University of Bologna Law Review*, *5*(2), 362-374. doi:10.6092/ISSN.2531-6133/12441

Baskaran, H., Yussof, S., Rahim, F. A., & Bakar, A. A. (2020). Blockchain and the personal data protection act 2010 (PDPA) in Malaysia. Paper presented at the 2020 8th International Conference on Information Technology and Multimedia, ICIMU 2020, 189-193. doi:10.1109/ICIMU49871.2020.9243493

BERNAMA. (2020). Govt still studying the need to amend Personal Data Protection Act. The Malaysian Reserve. Retrieved from https://themalaysianreserve.com/2020/08/26/govt-still-studying-need-to-amend- personal-data-protection-act/

Calzada, I. (2022). Citizens' data privacy in China: The state of the art of the Personal Information Protection Law (PIPL). *Smart Cities*, *5*(3), 1129-1150.

Cambridge University Press. (n.d.). Overshare. In Cambridge dictionary. Retrieved July 15, 2021, from https://dictionary.cambridge.org/dictionary/english/overshare

Campbell, J. T., Ciampa, M., Clemens, B., Freund, S. M., Frydenberg, M., Hooper, R. E., & Ruffolo, L. (2020). Technology for Success: Computer Concepts. Cengage Learning Asia Pte Ltd.

Chen, L. F., & Ismail, R. (2013). Information technology program students' awareness and perceptions towards personal data protection and privacy. International Conference on Research and Innovation in Information Systems, ICRIIS, 2013, 434–438. https://doi.org/10.1109/ICRIIS.2013.6716749

Crocetti, P., Peterson, S. & Hefner, K. (2021). What is data protection and why is it important?. Retrieved from https://searchdatabackup.techtarget.com/definition/data-protection

Department of Personal Data Protection (JPDP). (2021). Official Portal of Department of Personal Data Protection. Retrieved from https://www.pdp.gov.my/jpdpv2/?lang=en

Dhali, M., Hassan, S., Zulhuda, S., & Bt Ismail, S. F. (2022). Artificial intelligence in health care: Data protection concerns in Malaysia. *International Data Privacy Law*, *12*(2), 143-161. doi:10.1093/idpl/ipac005

European Commission, Official Website. European Commission - European Commission. (n.d.). Retrieved November 26, 2022, from https://ec.europa.eu/info/index_en

Frankenfield, J. (2022, August 3). Personally identifiable information (PII). Investopedia. Retrieved August 20, 2022, from https://www.investopedia.com/terms/p/personally-identifiable-information-pii.asp

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. Risk Management and Insurance Review, 13(1), 61–83. https://doi.org/10.1111/j.1540-6296.2010.01178.x

Gross, R. & Acquisti, A. (2005). Information revelation and privacy in online social networks: The Facebook case). ACM Workshop on Privacy in the Electronic Society, pp.1-22

Holtfreter, R. E., & Harrington, A. (2015). Data breach trends in the United States. Journal of Financial Crime, 22(2), 242–260. https://doi.org/10.1108/JFC-09-2013-0055

Human Dynamics (n.d.). Public Survey on Awareness in Personal Data Protection. IPS Institute. Skopje: Czech Office for Personal Data Protection (OPDP). Retrieved from https://dzlp.mk/sites/default/files/Dokumenti/IPA/Annex%206%20Final%20documents/doc_id_3.1.2.pdf

Javelin Strategy & Research. (2018) 2018 Child Identity Fraud Study. Retrieved from https://javelinstrategy.com/node/59561

Madden, M., Lenhart, A., Cortesi, S., Gasser, U., Duggan, M., Smith, A. & Beaton, M. (2013). Teens, social media, and privacy. Retrieved from https://www.pewresearch.org/internet/2013/05/21/teens-social- media-and-privacy

Malaysia, Jabatan Perlindungan Data Peribadi (2021). *Personal data*. Official Portal of Department of Personal Data Protection. https://www.pdp.gov.my/jpdpv2/public/data-peribadi/?lang=en

Malaysian Communications and Multimedia Commission. (2020). Internet Users Survey 2020. Retrieved from https://www.mcmc.gov.my/skmmgovmy/media/General/pdf/IUS-2020-Report.pdf

Markom, R. & Zainol, Z. & Fuad, N. (2019). Literasi perundangan media baharu dalam kalangan belia. Jurnal Komunikasi. 35. 372-389. 10.17576/JKMJC-2019-3503-22.

Masur, P. K. (2020). How online privacy literacy supports self-data protection and self-determination in the age of information. Media and Communication, 8(2), 258–269. https://doi.org/10.17645/mac.v8i2.2855

Müller, J. (2021). Online content sharing Malaysia 2020 by platform. Retrieved from https://www.statista.com/statistics/981291/malaysia-online-content-sharing-by-platform/

Neilsen, M. A., & Chowns, J. (2012, November 7). Parliament of Australia. Retrieved November 26, 2022, from https://parlinfo.aph.gov.au/parlInfo/download/legislation/billsdgs/1923143/upload_binary/1923143.pdf;fileType=application/pdf

Nor Ain Mohamed Radhi. (2022, February 22). Younger generation faces increased cybersecurity risks. New Straits Times. Retrieved July 10, 2022, from https://www.nst.com.my/news/nation/2022/02/773686/younger-generation-faces-increased-cybersecurity-risks.

Nurul 'Ain Ahmad & Nooraini Othman. (2019). Information privacy awareness among young generation in Malaysia. Journal of Science, Technology and Innovation Policy, 5 (2), 1-10. https://doi.org/10.11113/jostip.v5n2.41

Patel, D. (2020). The dangers of sharing personal information on social media. Retrieved from https://penntoday.upenn.edu/news/dangers-sharing-personal-information-social-media

Personal Data Protection Commission Singapore. (2021). Guide on managing and notifying data breaches under the personal data protection act. Retrieved from https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF- Files/Other-Guides/Guide-on-Managing-and-Notifying-Data-Breaches-under-the-PDPA-15-Mar- 2021.pdf?la=en

Phua, C. (2009). Protecting organisations from personal data breaches. In Computer Fraud and Security (Vol. 2009, Issue 1, pp. 13–18). https://doi.org/10.1016/S1361-3723(09)70011-9

Pitchan, M. A., & Omar, S. Z. (2019). Dasar keselamatan siber Malaysia: tinjauan terhadap kesedaran netizen dan undang-undang (Cyber security policy: review on netizen awareness and laws). Jurnal Komunikasi: Malaysian Journal of Communication, 35(1), 103–119. https://doi.org/10.17576/jkmjc-2019-3501-08

Rahim, N., Hamid, S. & Mat Kiah, M. L. (2019). Enhancement of cybersecurity awareness program on personal data protection among youngsters in Malaysia: An assessment. Malaysian Journal of Computer Science. 32. 221-245. 10.22452/mjcs.vol32no3.4.

Sabowo, H. K., Hartati, S., & Karyono, H. (2022). The Urgency Of Personal Data Protection For The Community: There Is Need For An Independent Commission. *International Journal of Educational Research & Social Sciences*, *3*(1), 413-424.

Sekaran, U. (2003). Research Methods for Business: A Skill-building Approach (4th ed.). John Wiley & Sons, Inc.

Skendžić, A., Kovačić, B., & Tijan, E. (2018, May). General data protection regulation—Protection of personal data in an organisation. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1370-1375). IEEE.

Tatum, M. (2021). What is data disclosure? Retrieved from https://www.infobloom.com/what-is-data-disclosure.htm#:~:text=Malcolm%20Tatum,Malcolm%20Tatum,specific%20circumstances%20of%20th e%20situation.

TechTarget. (2013). Data broker. In WhatIs.com. Retrieved from https://whatis.techtarget.com/definition/data- broker-information-broker

The Office of Chief Statistician Malaysia. (2021, April 12). ICT use and access by individuals and household 2020. [Media Statement]. Retrieved from https://www.dosm.gov.my/v1/uploads/files/5_Gallery/2_Media/ 4_Stats%40media/4-Press_Statement/2021/20210412-Kenyataan_Media Penggunaan_dan_Capaian_ICT_oleh_Individu_dan_Isi_Rumah_2020.pdf

Thomas, K., Li, F., Zand, A., Barrett, J., Ranieri, J., Invernizzi, L. & Bursztein, E. (2017, October). Data breaches, phishing, or malware? Understanding the risks of stolen credentials. In *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1421-1434).

Tiganoaia, B., Cernian, A., & Niculescu, A. (2017, September). The use of social platforms and personal data protection—An exploratory study. In *2017 16th RoEduNet Conference: Networking in Education and Research (RoEduNet)* (pp. 1-5). IEEE.

Tolsdorf, J., Dehling, F. & Lo Iacono, L. (2022) Data cart – designing a tool for the GDPR-compliant handling of personal data by employees. *Behaviour & Information Technology*, *41*(10), 2070 - 2105, DOI: 10.1080/0144929X.2022.2069596

Trepte, S., Teutsch, D., Masur, P. K., Eicher, C., Fischer, M., Hennhofer, A., et al. (2015). € Do people know about privacy and data protection strategies? Towards the "online privacy literacy scale" (OPLIS). In S. Gutwirth, R. Leenes, & P. de Hert (Eds.), Reforming European data protection law (pp. 333e365). Heidelberg, Germany: Springer. http://dx.doi.org/10.1007/978-94-017-9385-8

Valecha, R., Bachura, E., Chen, R., & Raghav Rao, H. (2017). An exploration of public reaction to the OPM data breach notifications. Lecture Notes in Business Information Processing, 296 (Csid 2015), 185–191. https://doi.org/10.1007/978-3-319-69644-7_19

Wright, S. A., & Xie, G. X. (2019). Perceived privacy violation: Exploring the malleability of privacy expectations. *Journal of Business Ethics*, *156*(1), 123-140.

Youn, S. (2009). Determinants of online privacy concern and its influence on privacy protection behaviors among young adolescents. Journal of Consumer Affairs, 43(3), 389–418. https://doi.org/10.1111/j.1745- 6606.2009.01146.x

Yuliana, Y. (2022). The importance of cybersecurity awareness for children. Lampung Journal of International Law, 4(1), 41–48. https://doi.org/10.25041/lajil.v3i2.2526

Ziff Davis. (2021). Information broker. In PCMag Encyclopedia. Retrieved from https://www.pcmag.com/encyclopedia/term/information-broker