MyJICT
Malaysian Journal of Information and Communication Technology
EISSN 0127-7812

Vol. 10, Issue 2, pp. 55-68 | DECEMBER 2025
DOI: https://doi.org/10.53840/myjict10-2-234

SAFEGUARDING PERSONAL DATA IN ISLAMIC FINTECH: A COMPARATIVE REVIEW OF SHARIAH-COMPLIANT INVESTMENT PLATFORMS

[i*]Surianom Miskam, [i]Farah Mohd Shahwahid, & [i]Nawal Sholehuddin,

[i]Faculty of Syariah and Law, Universiti Islam Selangor, Malaysia

*(Corresponding author) e-mail: surianom@uis.edu.my

Article history:
Submission date: 28 October 2025
Received in revised form: 17 December 2025
Acceptance date: 18 December 2025
Available online: 21 December 2025

Keywords:
Artificial Intelligence, Shariah-compliant investments, personal data protection, Islamic FinTech, ethics

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:
Miskam, S., Mohd Shahwahid, F., & Sholehuddin, N. (2025). Safeguarding Personal Data in Islamic Fintech: A Comparative Review of Shariah-Compliant Investment Platforms. *Malaysian Journal of Information and Communication Technology (MyJICT)*, *10*(2), 55-68. https://doi.org/10.53840/myjict10-2-234

ABSTRACT

With the fast-paced development of digital financial services, Islamic financial technology (FinTech) platforms are gaining recognition for offering Shariah compliant investment options with personalized investment strategies and risk preferences for diverse backgrounds of investors. The integration of big data and artificial intelligence (AI) into Shariah-compliant investment platforms is reshaping portfolio optimization, risk management, and compliance monitoring thereby presenting both opportunities and challenges to the Islamic asset management industry. However, reliance on massive-scale personal and financial datasets in these AI-driven investment platforms introduces significant challenges related to data privacy, security, and governance. The AI-driven investment platforms collect and process personal data to conduct enhanced due diligence in order to assess eligibility and suitability of funds according to their risk preference. Legal and ethical concerns arise where existing legal provisions do not fully address the interests of stakeholders. This paper examines the legal and ethical perspectives of personal data protection within Shariah-compliant investment platforms by reviewing relevant legislations, privacy notice of Islamic funds and, user interface and app walkthroughs experience. The study explores how these platforms balance technological innovation with adherence to Shariah governance principles and data protection requirements, such as the Personal Data Protection Act 2010 and the Islamic Financial Services Act 2013 in safeguarding investor information. The findings show that AI enhances portfolio screening and investment decision while personal data protection laws and Shariah governance framework play significant roles to ensure compliance and maintain investor confidence. The study contributes to the emerging discourse on Islamic FinTech, offering strategic insights for regulators, asset management companies and digital platform developers to strengthen personal data protection while sustaining innovation in AI-driven Shariah-compliant investment.

Introduction

The application of big data and artificial intelligence (AI) in the investment platforms has enabled Islamic investment fund management companies to attract investors and offer tailored products and services based on their risk preference. The development in Islamic FinTech has been attributed mainly to strong demand for alternative financing for small and medium enterprises and new investment avenues for investors, motivated by widespread adoption of Internet devices and social media and further influenced by change in population demography towards a more tech savvy generations of investors (Securities Commission, 2016).

With the fast-paced development of digital financial services, Islamic FinTech platforms are gaining recognition for offering Shariah-compliant investment options with personalised investment strategies and risk preferences for diverse backgrounds of investors. The integration of big data and AI into Shariah-compliant investment platforms is reshaping portfolio optimisation, risk management, and compliance monitoring thereby presenting both opportunities and challenges to the global Islamic asset management industry. However, reliance on massive-scale personal and financial datasets in these AI-driven investment platforms introduces significant challenges related to data privacy, security, and governance. The AI-driven investment platforms collect and process personal identifier data, contact data, professional data, financial data, communication data, behavioural data, geo-location data and personal relationship data to conduct enhanced due diligence in order to assess eligibility and suitability of funds according to their risk preference. Legal and ethical concerns arise where existing legal provisions do not fully address the interests of stakeholders. Breach of financial data is on the rise due to lack of data encryption for sensitive data. Even minor errors in financial transactions may result in a substantial financial loss to the investors and the fund management companies (Miskam et al., 2019).

Based on this background, the paper aims to examine the legal and ethical perspectives of personal data protection within Shariah-compliant investment platforms. This paper is structured as follows: Section 2 provides a review of the literature focusing on personal data protection, big data and artificial intelligence, Islamic FinTech and Shariah-compliant investments. Section 3 explains the methodology applied in this study. Section 4 explains the results and findings of the study and section 5 provides a detailed discussion based on the findings. The final section concludes the discussion by providing recommendations and insights for future research.

Literature Review

Personal Data Protection

Personal data refers to a description that contains information about a person that can be identified either directly or indirectly concerning name, identification number, location data, social identity, genetic, physiological, economic, cultural, and mental (Galic & Gellert, 2021). Personal data protection belongs to the category of informational privacy and it concerns the right of an individual to have control over his or her information (Munir & Yasin, 2010).

Personal data need to be protected for several reasons. Firstly, personal data is part of the privacy right that is recognized as one of the instruments in the Universal Declaration of Human Rights (UDHR). Article 12 of the Universal Declaration of Human Rights (UDHR) states that: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks. Secondly, protecting personal data is part of a commitment to protect consumers. Data is one of the consumer rights that must be protected by law. Therefore, consumer personal data may not be used, modified, and distributed without the consent from the consumer. Thirdly, business reputation whereby data is one of the valuable assets for the company. for any purposes, thus data leaks may cause the companies to suffer financial loss, distrust and bad reputation from the public (Nurhasanah & Rahmatullah, 2020).

As far as data governance in the financial industry is concerned, regulations have not been responsive to technological developments such as big data and artificial intelligence that bring new dimensions to the risk of privacy violations (Solikha, 2025). Financial institutions are heavily regulated, and implementing AI-driven systems must comply with stringent legal requirements to ensure transparency and fairness in decision-making (Pillai, 2023).

Big Data and Artificial Intelligence

Big data refers to the huge amount of automatically collected data, large data-driven knowledge bases, and data pools involving more than a million instances/entries, rows/records, relations, and parameters/edges (Challa, 2022). The European Commission (2018) argues that the term big data refers to "large amounts of different types of data produced with high velocity from a high number of various types of sources." Big data is often described using the three Vs model: Volume which refers to the sheer amount of data generated by financial transactions, stock exchanges, social media, news, and other sources. Velocity which means the speed at which data is generated and needs to be processed in real-time or near real time. Variety which denotes the diverse types of data (structured, semi-structured, and unstructured) including numerical data, text, images, and video (Pillai, 2023). Big data analytics is typically the technical process of analysing massive amounts of data to discover patterns, linkages, market trends, and customer preferences information that can assist businesses in making better-informed decisions (Ahmadi, 2024) and refers to the variety of technologies, models and procedures that involve the analysis of big data aimed revealing insights, patterns of causality and of correlation, and to predict future events similarly to data science and data mining (Giudici, 2018).

AI refers to the capabilities/task solution state and processes that replicate/improve the individual intelligence, collective intelligence, and decision-making intelligence of the natural and human systems or their characteristics and principles (Challa, 2022). AI is the capability of computer systems to perform tasks that generally require human intelligence, such as speech recognition, decision-making, and pattern understanding. In the age of the digital revolution, the financial industry is undergoing significant changes. There has been a drastic shift in the way financial institutions operated in the past, and this has become possible by the integration of big data and AI in the finance industry (Ahmadi, 2024).

Financial technology (FinTech) refers to the financial-sector smart systems that facilitate financial market/service innovations and smart financial systems and practices (Challa, 2022). Big data and artificial intelligence continue to lead in a digital revolution in FinTech and fundamentally reshape the finance industry (Goldstein, 2021). Big data and AI have been integrated into Islamic FinTech to improve efficiency and transparency of Islamic financial services (Killic, 2023). AI significantly improves operational efficiency by automating processing and reducing manual intervention on financial services. AI-enabled predictive analytics enable financial service providers to forecast investor trends and behaviour, optimize decision and streamline transactions thus reducing the time and costs associated with various financial operations including those requiring Shariah-compliance. AI offers advanced data analysis capabilities that enable Islamic FinTech services providers to improve risk management and fraud detection (Hendarti et al, 2024).

AI-powered tools such as Shariah-compliant robo-advisors and automatic credit risk assessment system can be applied to enhance efficiency without undermining Islamic ethical standards (Mohd Najib et. al (2025). In recent years, robo robo-advisory services have emerged as a critical development, offering algorithm-driven investment management with minimal human intervention. These platforms cater to a growing segment of digitally literate investors who seek low-cost, transparent, and automated investment solutions (Hidayat-ur-Rehman et al., 2025).

The convergence of these technologies in finance is driven by exponential growth of financial data from transactions, market feeds, social media, and other sources that present significant opportunities for extracting actionable insights. Advancements in computational power and the decreasing costs of data storage have made it feasible to process and analyse large datasets efficiently. Despite the significant benefits, this rise of AI in finance has also brought new challenges regarding ethical considerations, explaining algorithmic decisions, man aging bias, ensuring data privacy and security, protecting sensitive data, and mitigating potential risks associated with algorithmic trading. In order to address this, it is vital to have ethical practices and regulations put in place that ensure the responsible and beneficial use of AI in finance to make sure it is being used in a way that benefits everyone (Najem et al, 2025).

Islamic Fintech & Shariah-compliant investment

The Financial Stability Board (2017) defines FINancial TECHnology as "technologically enabled financial innovations that could result in new business models, applications, processes, or products with an associated material effect on financial markets and institutions and on the provision of financial services." Islamic FinTech can be defined as financial services and solutions that provide services using information technology based on Islamic law (Imani et al., 2023). Islamic FinTech is a fusion of technological innovation with Shariah financial principles, grounded on fundamental Shariah financial principles, such as the prohibition of *riba* (interest), *gharar* (uncertainty), and *maysir* (speculation/gambling). All related transactions finance must be based on fair risk-sharing, transparency, and investment in halal activities (Yudha, 2021).

By integrating modern technologies such as IoT, cloud computing, big data, AI, machine learning, blockchain, and robotic process automation, Islamic FinTech is able to create more inclusive, efficient, innovative and equitable financial services. It is a combination of innovation in finance and technology that facilitates transaction and investment processes based on Shariah principles, which include moral and ethical requirements. Islamic FinTech transactions must adhere to Shariah principles, including the necessary pillars and conditions in contracts (Ruslan et al., 2024). The growth in Islamic FinTech is mainly influenced by increased digital technology users especially in Muslim-majorities countries such as Indonesia, Malaysia and United Arab Emirates. These countries have seen a significant surge in adopting Shariah-compliant financial services, bridging the gap in the traditional financial system that often does not provide options for Shariah-compliant products (Setiawan et al, 2021).

In the meantime, his rise of AI in finance has also brought new challenges regarding ethical considerations, explaining algorithmic decisions, managing bias, ensuring data privacy and security, protecting sensitive data, and mitigating potential risks associated with algorithmic trading. Hence, it is crucial to have ethical practices and regulations put in place that ensure the responsible and beneficial use of AI in finance to make sure it is being used in a way that benefits everyone (Najem et al., 2025).

Methodology

This study examines the legal and ethical perspectives of personal data protection within Shariah-compliant investment platforms by reviewing relevant legislations, privacy notice of Islamic investment platforms and user interface and app walkthroughs experience. The study explores how these platforms balance technological innovation with adherence to Shariah governance principles and data protection requirements, such as the Personal Data Protection Act 2010 and the Islamic Financial Services Act 2013 in safeguarding investor information.

For the purpose of this study, three smart apps were selected i.e. BEST by BIMB Investment Management Berhad, Wahed by Wahed Technology Sdn. Bhd. and StashAway Malaysia Sdn. Bhd. All three platforms offer Shariah-compliant portfolios, ensuring investments align with Islamic finance principles. Each platform operates as a mobile or web-based smart app, representing the digital transformation of investment services. BEST uses Big Data analytics, Wahed applies Modern Portfolio Theory (MPT), and StashAway employs ERAA® (Economic Regime-based Asset Allocation). Despite using different methods, all platforms rely on data-driven decision-making, raising important questions about data protection and ethical use of personal information. The three platforms operate under the Malaysian regulatory framework i.e. PDPA 2010 and IFSA 2013. Their user-friendly interfaces make them relevant for examining privacy notices and transparency in communication. All three platforms emphasize clear disclosures (fees, methodologies, portfolio composition). In conclusion, these platforms were selected because they collectively embody the convergence of Shariah governance, fintech innovation, and data protection law. Their shared features make them representative case studies for analyzing how Islamic investment platforms in Malaysia safeguard personal data while promoting ethical and inclusive financial innovation.

Results and Findings

BEST

BEST is a non-automated discretionary Robo-Intelligence unit trust online investing platform aims to provide an easy-to-use online investing platform for new and existing investors to perform investments transactions (purchase, sell and switch) on BIMB Investment's selected unit trust funds. BEST Robo-Intelligence platform allows investors to decide on which unit trust funds they wish to invest in, by how long and how much. BEST will then manage the investment portfolio according to the preference set. BEST and BIMB Investment uses Big Data technology in daily day-to-day data processing from managing online investment transactions and analytical data to make investment decisions.

Wahed

Wahed provides a fully automated investment process: Risk Assessment where investors answer questions to determine risk tolerance. Portfolio Allocation where investments are optimized using Modern Portfolio Theory (MPT). Continuous Monitoring where portfolios are rebalanced when market conditions shift. Full Transparency where all investment methodologies and fees are publicly disclosed. Wahed provides a range of portfolios with varying target returns, investing across multiple asset classes such as global equity, emerging markets equity, Malaysian equity, REITs, commodities and fixed income to enhance diversification benefits.

StashAway

StashAway is the first robo-advisor in Malaysia to be awarded the Capital Markets License by the Securities Commission under the Digital Investment License framework. The Shariah Global Portfolio is a globally diversified investment portfolio that complies with Islamic principles. The portfolio is managed using ERAA® (Economic Regime-based Asset Allocation) and only invests in Shariah-compliant ETFs across equities, Islamic bonds (sukuk), and gold.

The first stage is on the features of the three Shariah-compliant investment platforms. Table 1 summarises the features of the three Shariah-compliant investment platforms.

Table 1: Features of Shariah-compliant Investment Platforms

Features	BEST	Wahed	StashAway
Place of Origin	BIMB Investment is a subsidiary of Bank Islam Malaysia Berhad (BIMB), which was established in Malaysia.	Wahed Inc. is a global company with its headquarters in New York, USA and its Malaysian operations are managed locally.	StashAway is a Singapore-based fintech company with a license to operate in Malaysia from the Securities Commission of Malaysia.
Onboarding	eKYC with NRIC & face recognition	Risk questionnaire and ID verification	Goal-based and risk profiling
Portfolio Options	Goal-based (Do It For Me / Yourself)	Regular & Thematic portfolios	Global Shariah-compliant portfolios
User Interface	Functional, goal-centric	Sleek, modern, educational	Clean, data-driven dashboard
Fee Structure	No sales charges; annual management fees	RM2.50 or 0.39%-0.79% (whichever higher)	Tiered fees based on assets
Minimum Investment	RM10	RM100	RM100
Shariah Compliance Oversight	Shariah advisers registered with SC.	Internal Shariah Board	Masryef Advisory
Investment Methodology	Arabesque's Al investment research process uses alpha signals	Modern Portfolio Theory (MPT) to determine optimal portfolios for clients. The	Economic Regime-based Asset Allocation, or ERAA®, is the intelligent

	generated using its proprietary AI Engine and model portfolio construction via its in-house portfolio optimisation and risk modelling system. Its AI Engine uses a wide range of machine learning algorithms, such as Deep Learning models, to analyse and identify investment opportunities in the equity markets.	investment strategy is based on allocating assets across multiple classes, ensuring diversification, capital growth, income generation, and risk mitigation. Each asset class is evaluated based on: capital growth potential, volatility, diversification benefits, inflation protection and cost-efficiency.	investment framework that minimises risk and maximises returns which include the General Investing Portfolio, Thematic Portfolios, and Responsible Investing Portfolio.
Apps Support	Android & iOS	Android & iOS (no web for MY)	Android, iOS, and web platform

The second stage is the review of the personal data protection in AI-driven Shariah-compliant investment platforms. The summary is provided in Table 2.

Table 2: Review of personal data protection in AI-driven Shariah-compliant investment platforms

Themes	**BEST**	**Wahed**	**StashAway**
Legal Framework	BIMB Investment Berhad is an Islamic fund management company, licensed and registered with the Securities Commission of Malaysia and governed by the Capital Market Services Act 2007. It is a wholly-owned subsidiary of Bank Islam Malaysia Berhad under the supervision of Central Bank of Malaysia (CBM).	Wahed is a digital investment manager (DIM) licensed by the Securities Commission of Malaysia and governed by the Capital Market Services Act 2007.	StashAway Malaysia Sdn Bhd is licensed by the Securities Commission Malaysia and governed by the Capital Market Services Act 2007.
Personal Data Protection Law	Personal Data Protection Act 2010.	Personal Data Protection Act 2010 and General Data Protection Regulation (GDPR).	Personal Data Protection Act 2010
Jurisdiction in Dispute	Disputes fall under the jurisdiction of Malaysian courts.		
Scope of Notice	The privacy notice relates to the personal information that Bank Islam Malaysia Berhad, its subsidiaries, affiliate companies, representatives and branch offices collects in relation to the products and services offered.	The privacy policy applies to Wahed Technologies Sdn. Bhd and Wahed X Sdn Bhd's website at www.wahed.com. This privacy policy covers the collection, processing and other use and disclosure of personal data.	The privacy notice explains how StashAway Malaysia manages personal data in possession and under control of the company.
Types of Data Collected	Personal Identifier Data/Information: name, identity card number or passport number and other relevant information for application, images and biometrics, specimen signatures	Personal data including contact data such as name, address, postal address, e-mail address, telephone number and employer; financial information such	Contact data including name, telephone number, email address, residential address and correspondence address; specimen signature;

	(digital or electronic or physical signatures), date of birth, gender, race, religion, citizenship/residency, marital status, spouse name, number of dependents Contact Data: residential or business address, e-mail address, mobile or landline number, emergency contact Professional Data: level of education, occupation and employer details or any data that is referring to an individual's work or profession Financial Data: financial position such as assets and income, source of funds, investment objectives, annual income, tax details, account balances, payment history, account activity and credit rating data to assess credit worthiness Communication Data: live chats, phone calls to contact centre, messaging and email Behavioural Data: views or opinions made known to us via feedback or surveys, competitions, activities, habits, preferences and interests, browsing behaviour on websites and transactional activities Geo-location Data: IP addresses, cookies, activity logs, online identifiers, and location data Personal Relationship Data: Immediate family members, directors, emergency contacts, individual shareholders, authorised signatories and guarantors that can determine identity of the customer. Sensitive personal information: racial or ethnic origin data, religious data: information relating to your religious beliefs and other beliefs of a similar nature and biometric data which physically identifies the customer such as facial recognition, fingerprint or voice recognition.	as credit card number; demographic data such as gender, date of birth and zip code; and certain usage data such as IP address. Location Data: the location of a mobile device or computer, including: the location of the mobile device or computer used to access the Website derived from GPS or WiFi use; the IP address of the mobile device or computer or internet service used to access the Website; and; and other information made available by a user or others that indicates the current or prior location of the user.	occupation, education and income levels; identification card or passport number, date of birth, place of birth and other information for the verification of identity; financial and banking information such as net assets, income, expenses, credit history, bank account and banking transactions, securities trading account); images and voice recordings of conversations with customer; tax and insurance information; risk profile, investments, investment objectives, knowledge and experience and/or business interests and assets.
Methods of Collection	Digitally or manually such as application forms, when customers open and operate accounts and use facilities, participating in customer surveys, competitions, and marketing promotions.	Information is collected automatically through use of cookies and similar data collection tools, when customers create an account to use the service, connect	Personal data will be obtained from the information provided or submitted by customer through among others, dealings and agreements with the company, which

		with social media through the website.	includes information provided when registering as a user, providing information regarding any account, providing answers to security questions, completing any confirmations, declarations or forms, or through utilization of any of services, accessing or viewing the platform.
Purpose of Use	Data is used to provide facilities to customer including opening of account, conducting Enhanced Due Diligence/Know Your Customer and/or Enhanced Customer Due Diligence as required by law, assessing eligibility, merits and/or suitability of Facility applications, assessment and analysis including credit / lending/financing / insurance risks / behaviour scoring / product analysis/ Anti-Money Laundering Risk Profile and market research, assessing the suitability of being an individual guarantor, conducting and maintaining credit checks and financial assessments as required by applicable law and regulations and assessing and setting of credit limits.	Data is used to open, manage, improve and personalise the product and services, to detect fraud and illegal activities, to communicate with users.	Date will be used to serve the provision of the services as requested by customer, carrying out any transactions on behalf of the customer contemplated on the platform, assessing and processing applications, instructions or requests, communicating with customer, to verify identity for the purposes of providing services; conducting due diligence checks, screenings or credit checks; to detect and protect the company or any third parties against negligence, fraud, theft and other illegal activities; to understand the customer's needs and preferences; improving the content, appearance and utility of the platform; to manage and develop infrastructure and business operations; to administer any account; to process payments; to comply with internal policies and procedures; and any other purposes that are appropriate or authorized by any applicable laws.
Data Sharing	Data is shared with authorized parties, which includes officer, employee, agent or director of the company, authorised third parties such as legal guardians, joint account holders, actual or intended guarantors/sureties, trustees, beneficiaries, executors and legal representatives, third parties that verifies personal information such as credit	Data may be shared when consent is obtained in the event of selling or buying any business or assets. Data may also be shared in connection with a merger, sale, acquisition or other change of ownership or control by or of us or any affiliated company but when one of these events	Data may be shared with any directors, officers, employees, representatives, agents or delegates; shareholders or related corporations, and any of their successors or assigns, and their directors, officers, employees, representatives, agents or delegates; professional

	bureaus, financial crime references agencies and rating agency, third party service providers such as auditors, legal counsel or technology service providers, strategic business partners, government authorities and law enforcement and other financial services organisations.	occurs, the company will use reasonable efforts to notify users before it is transferred or becomes subject to a different privacy policy. Sharing is permitted, as needed, to enforce rights, protect property or protect the rights, property or safety of others, or as needed to support external auditing, compliance and corporate governance functions.	advisers, consultants and auditors; service providers, agents, contractors, delegates, suppliers or third parties which we may appoint from time to time to provide services in connection with the platform and their directors, officers, employees, representatives, agents or delegates; pursuant to a request by any relevant governmental or regulatory authority; and any person to whom the company believes in good faith, under an obligation to make disclosure as required by any applicable laws.
International Transfer	Personal data may be transferred outside Malaysia for the purpose of processing, storing, sharing, transferring, or disclosing to operate effectively and securely, improve and support the process and business operations and for legal proceedings or legal advice.	Personal data may be transferred to other countries for processing and storage particularly if service providers or parent companies are located abroad.	The company may transfer, store and/or process your Personal Data outside Malaysia according to PDPA and other applicable data protection and privacy laws and ensure that the recipient outside of Malaysia is obliged to protect the personal data at the standard comparable to the protection under the applicable laws.
Retention Policy	Personal information is retained as long as the purpose for which it was collected exists. Personal information may be retained for a period of time upon the termination of the relationship between the company and the customer. Data will be destroyed or deleted once the purpose ceases, unless it must be retained to meet legal or regulatory requirements.	The company retains personal data for a period of seven years. Personal data from closed accounts may be retained to comply with applicable law, prevent fraud, resolve disputes, troubleshoot problems, assist with any investigation and other actions permitted by law. After this period, we dispose of it according to our data retention and deletion policies.	Personal data is retained as long as the purpose for which it was collected remains and until it is no longer necessary for any other business purposes or to comply with any applicable laws.
Rights to Personal Data	The customer has the right to access data, correct and update the data, restrict or object the processing of data, right not to provide or change or withdraw consent and right to withdraw from direct marketing.	Users can contact the data protection officer to inquire about their rights, which include the right to access, review and request copy of the personal data, to correct	Customers may request access to personal data or request the correction of any inaccurate, incomplete, misleading or not up-to-date data.

		and request the deletion of their personal data.	
Security Measures	The company shall take all the necessary precautions to keep personal information safe and place an appropriate level of protection and safeguards to comply with the applicable law for jurisdiction outside of Malaysia and where their local laws may not have similar data protection laws as Malaysia.	The company shall take all appropriate security and organisational measures to prevent unauthorized access to, alteration of, disclosure of, accidental loss, and destruction of personal information. The secure server software (SSL) encrypts all information input and all sensitive data collected is protected by several layers of encryption and several layers of security to prevent unauthorized access.	The company have introduced appropriate administrative, physical and technical measures such as minimised collection of personal data; authentication and access controls such as good password practices, need-to-basis for data disclosure, etc.; encryption of data; data anonymization; up-to-date antivirus protection; regular patching of operating system and other software; securely erase storage media in devices before disposal; web security measures against risks; security review and testing performed regularly.

(Source: Privacy Notice of Investment Platforms)

Discussion

As far as personal data protection is concerned, the three platforms examined come under the purview of the Personal Data Protection Act 2010 (PDPA 2010). The PDPA is Malaysia's primary law regulating the collection, processing, storage, and disclosure of personal data in commercial transactions.

Section 4 defines "personal data" as any information in respect of commercial transactions, which is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose; is recorded with the intention that it should wholly or partly be processed by means of such equipment; or is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system, that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed for the purpose of a credit reporting business carried on by a credit reporting agency under the Credit Reporting Agencies Act 2010. Section 4 further clarifies that "sensitive personal data" 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 (PDPA, 2010).

The seven principles of data protection form the backbone of this law, are the General, Notice and Choice, Disclosure, Security, Retention, Data Integrity and Access. General principle states that data users must not process personal data about an individual unless the data owner grants the permission. Notice and choice principle stipulates that a data user is obliged to give a written notice informing the data owner that his/her personal data is being processed. Disclosure principle provides that without the permission of the data owner, personal data must not be disclosed for any purpose other than the purpose which was initially disclosed at the time of collection or to any party other than third parties for whom the data owner has given permission. The security principle requires that data users must take technical steps to ensure the integrity, reliability and security of the personal data. Data users must take all the necessary efforts to protect any loss, accidental access or disclosure, modification, misuse, unauthorized, alteration and destruction of personal data. Retention principle states that the personal data processed cannot be kept longer than is necessary and the data user must take all reasonable steps to delete personal data whenever is no longer required except the life span of personal data. Integrity principle stipulates that a data user must take all necessary measures to ensure that personal data is complete, not misleading, accurate, up to date, and related to the purpose for which it was collected. Lastly, access principle provides that a data owner must be given access to, and be able to amend, correct, or destroy personal data whenever it is invalid (PDPA, 2010).

Generally, Malaysia's position in having personal data protection laws is in line with the practice of other ASEAN countries, which makes it mandatory for businesses to take measures for safeguarding personal data collected from their customers (Sudarwanto, 2022). Organisations that were referred to as data users (now referred to as data controllers) must obtain consent, give notice of purpose and extent of data processing, communicate privacy policies, secure data against misuse, limit retention, maintain accuracy, and grant individuals or customers, known as data subjects, access to, and the right to correct and update their data (Shahwahid & Miskam, 2015). Non-compliance to these principles are punishable offences which carry severe penalties, including fines and imprisonment (Sholehuddin, et. Al., 2024).

Malaysia introduced changes to the PDPA 2010 with the passing of the Personal Data Protection (Amendment) Act 2024. Recent amendments to this law which came into effect in June 2025, align the PDPA more closely with international frameworks such as the European Union's General Data Protection Regulation (EU's GDPR) and the Personal Data Protection Act of Singapore. The amendments include the introduction of mandatory breach notification, the right to data portability, and having compulsory Data Protection Officers (DPOs). There is an expressed need for more due diligence for cross-border data transfers. The amendment removed the white-list regime which could simplify international operations, but also required data controllers to enhance their due diligence and ensure compliance with these standards. Specifically, that the receiving destination should have laws substantially similar to the PDPA or provide an adequate level of protection in relation to the processing of personal data that is at least equivalent to the protection afforded by the PDPA (Shepherdson, 2025). The amendment has the effect of substituting the term data user to data controller, when referring to organisations that process personal data of customers These data controllers face heightened responsibilities and stiffer penalties, demonstrating Malaysia's regulatory evolution. These amendments are designed to elevate Malaysia's data protection standards to meet global expectations (Medina, 2025).

The amendment creates several responsibilities to data controllers in regard to mandatory breach notification. Organisations must ensure that notification of the breach to the Commissioner is done within 72 hours of awareness of the breach, and notification to affected individuals is within seven days of the breach, if there is a risk of significant harm. The law defines 'significant harm' broadly and includes risks such as financial loss, identity theft, reputational damage, or loss of access to essential services. Data controllers must also maintain a data breach register for a minimum of two years. This register must specify the nature of the breach, the affected data, actions taken, and any remedial steps implemented (Medina, 2025).

The addition of breach notification requirements into the law brings Malaysia in line with global data privacy standards and places a greater burden on companies to adopt a proactive, transparent approach to security incidents. The amendment requires mandatory appointment of a DPO whose role is integral to ensuring compliance. This applies to organisations in the finance sector that typically process large volumes of personal data, handle sensitive information, or conduct regular and systematic monitoring of individuals. The DPO's role is integral to ensuring compliance. Responsibilities of DPOs include advising the organisation on its obligations under the PDPA, monitoring internal data protection activities, conducting impact assessments where necessary, and serving as the point of contact with the Personal Data Protection Commissioner. Businesses are required to notify the Commissioner of their appointed DPO and must display a designated DPO email address on their website or public channels. This measure is critical for promoting accountability and transparency in handling personal data. Prompt notification helps data controllers in maintaining transparency and building trust with their customers in order to mitigate the negative impact on the organisation's reputation and customer relationships. Data controllers need to have incident response plans in place to quickly identify, assess, and respond to data breaches which includes having clear procedures for detecting breaches, assessing their impact, and notifying the relevant parties (Sheperdson, 2025).

Failure to comply with the notification requirements can result in significant penalties, including fines and potential legal action. Under the PDPA 2010, penalties for non-compliance to personal data protection principles were punishable with fines up to RM300,000 and imprisonment for a maximum of two years, but after the amendment, non-compliance are punishable with fines up to RM1 million and/or imprisonment up to three years. The increased penalties for non-compliance under the amendment law enhances the importance of adhering to data protection principles by Data Controllers.

The earlier findings highlight that all three platforms operate under a consistent regulatory umbrella, with the Personal Data Protection Act 2010 (PDPA). This regulatory uniformity ensures a baseline for data protection and market conduct, which is critical for building consumer trust in a rapidly evolving sector. However, the analysis also reveals a significant distinction in the legal frameworks, with BIMB Best's adherence to the Islamic Financial Services Act 2013 (IFSA). As far as the Islamic Financial Services 2013 (IFSA 2023) is concerned, the law provides for strict confidentiality of customer financial data. Section 145 (1) of the FSA states that anyone with access to customer details must not disclose it except with written consent from the customer or under specific legal exceptions. This provision prohibits unauthorized disclosure, with exceptions permitted only under tightly defined circumstances. Section 146 of the FSA lays out operational details and exceptions related to disclosures permitted. Schedule 11 of the IFSA provides a list of permissible exceptions under which financial institutions may disclose customer information without breaching the secrecy provisions. For example, disclosures with the customer’s written permission, disclosures required by law, or disclosures necessary to protect vital interests. Non-compliance may lead to imprisonment for a term not exceeding five years or to a fine not exceeding ten million ringgit or to both.

A central theme of this analysis is the use of AI-driven FinTech and its complex relationship with Islamic finance. All three platforms leverage AI, but the purpose extends beyond mere efficiency and risk management. For BIMB Best and Wahed Invest, AI is an essential tool for ensuring Shariah compliance. This aligns with scholarly work that emphasizes the role of technology in automating compliance checks and strengthening ethical oversight in Islamic finance. Wahed Invest and StashAway's dedicated Shariah portfolios, with their rigorous, AI-powered screening methodologies that exclude sectors like gambling and products with *riba* (interest), demonstrate a sophisticated integration of technology and religious principles.

The analysis of data practices, from data collection methods to international transfers, reveals the globalised nature of modern fintech. While all platforms adhere to Malaysian law, their differing places of origin (Malaysia for BIMB Best, the USA for Wahed, and Singapore for StashAway) introduce complexities, particularly concerning cross-border data flows. This highlights a critical issue in the data protection discourse: the challenge of ensuring data privacy and security when information is transferred across jurisdictions with varying legal standards. The platforms' commitment to security measures like encryption and multi-factor authentication is a necessary response to these risks, but the reliance on contractual obligations for international data transfers shows the evolving nature of digital trust in a globalized financial ecosystem. The consistency in granting user rights to access and correct data across all platforms, a direct mandate of the PDPA, underscores the legal rights afforded to Malaysian consumers regardless of the service provider's origin.

Conclusion

The findings show that AI enhances portfolio screening and investment decision while personal data protection laws and Shariah governance framework play significant roles to ensure compliance and maintain investor confidence. Malaysian fintech platforms are not merely adopting technology but are actively shaping it to fit local market needs and ethical principles. The integration of AI for Shariah compliance is a key innovation, positioning Malaysia as a leader in this niche but growing market. As

Shariah-compliant investment continues to grow, driven by increasing awareness of global challenges and evolving regulatory landscapes, the role of big data and AI will become even more critical.

The study contributes to the emerging discourse on Islamic FinTech, offering strategic insights for regulators, asset management companies and digital platform developers to strengthen personal data protection while sustaining innovation in AI-driven Shariah-compliant investment. The findings suggest several avenues for future research, including a deeper analysis of the effectiveness of AI-driven Shariah screening, an exploration of how consumer trust is built through ethical transparency in different cultural contexts, and an examination of the legal and ethical challenges of cross-jurisdictional data transfers as fintech becomes increasingly global.

Acknowledgement

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

References

Ahmadi, S. (2022). A Comprehensive Study on Integration of Big Data and AI in Financial Industry and and Review, 2024, 07 (01), pp.66-74. 10.47191/ijcsrr/V7-i1-07. hal-04456267

Challa, S. R. (2022). Artificial Intelligence and Big Data in Finance: Enhancing Investment Strategies and Client Insights in Wealth Management International Journal of Science and Research (IJSR)ISSN: 2319-7064 SJIF (2022): 7.942

European Commission (2018). Fintech Action Plan: For a More Competitive and Innovative European Financial Sector. European Commission.

Financial Stability Board (2017a). Artificial Intelligence and Machine Learning in Financial Services: Market Developments and Financial Stability Implications. Financial Stability Board.
Front. Artif. Intell. 1:1. doi: 10.3389/frai.2018.00001

Galic, M. & Gellert, R. (2020). Data Protection Law Beyond Identifiability? Atmospheric Profiles, Nudging and the Stratumseind Living Lab (September 26, 2020). Computer Law and Society Review volume 40, 2021

Giudici, P (2018). Fintech Risk Management: A Research Challenge for Artificial Intelligence in Finance.

Goldstein, I, Spatt, C. S. & Ye. M. (2021). Big Data in Finnace, The Review of Financial Studies 34 (2021) 3213-3225

Hendarti, Y., Winarno, B., & Primbang Aprilianto, M. (2024). Use of Blockchain Technology and AI in Sharia Financial Risk Management. Jurnal Ekuisci, 1(3), 155–163. https://doi.org/10.62885/ekuisci.v1i3.165

Hidayat-ur-Rehman, I., Alam, M. N., Alsolamy, M., Alharbi, S. H. H., AlAnazi, T. M. B., & Bhuiyan, A. B. (2025). Examining Investor Interaction with Digital Robo-Advisory Systems: Green Value and Interface Quality in a Socio-Technical Context. *Systems*, *13*(9), 787. https://doi.org/10.3390/systems13090787

Islamic Financial Services Act 2013 (IFSA)

Kılıc G., & Turkan, Y. (2023). The Emergence of Islamic Fintech and Its Applications. Uluslararası İslam Ekonomisi Ve Finansı Araştırmaları Dergisi, 9(2), 212-236. https://doi.org/10.54427/ijisef.1328087

Medina, A. F. (2025). Malaysia Tightens Data Protection from June 2025, https://www.aseanbriefing.com/news/malaysia-tightens-data-protection-from-june-2025/, accessed on 3 August 2025

Miskam, S., Yaacob, A. M. & Rosman, R. (2019. Fintech and Its Impact on Islamic Fund Management in Malaysia: A Legal Viewpoint in Emerging Issues in Islamic Finance Law and Practice in Malaysia, Emerald Publishing Limited, 223-246

Munir, A. B. & Yassin, S. H. M (2010). Personal Data Protection in Malaysia, (Selangor: Sweet & Maxwell, 2010), at 3-4.221 t

Najem, R., Bahnasse, A., Amr, M. F. & Tale, M. (2025) Advanced AI and big data techniques in E-finance: a comprehensive surevy Vol.:(0123456789)Discover Artificial Intelligence (2025) 5:102 | https://doi.org/10.1007/s44163-025-00365-y

Najib, N. W. M., Basarud-din, S. K., & Fazial, F. (2025). Artificial Intelligence (AI) In Islamic Finance: A Maqasid Al-Shariah Perspective. International Journal Law, Government and Communication, 10 (40), 41-50.

Nurhasanah & Rahmatullah, I. (2020) Financial Technology and The Legal Protection of Personal Data: The Case of Malaysia and Indonesia, Al-Risalah Forum Kajian Hukum dan Sosial Kemasyarakatan, Vol. 20 No. 2, December 2020 (pp. 197- 214)

Personal Data Protection Act 2010 (PDPA)

Pillai, V. (2023). Integrating AI-Driven Techniques in Big Data Analytics: Enhancing Decision-Making in Financial Markets, International Journal Of Engineering And Computer Science, Volume 12 Issue 07 July 2023, Page No. 25774-25788, ISSN: 2319-7242 DOI: 10.18535/ijecs/v12i07.4745

Securities Commission Malaysia. (2016). Annual Report 2016. Retrieved from https:// www.sc.com.my/api/documentms/download.ashx?id=ef843977-2536-4258-b2b0-

Shahwahid, F. M. & Miskam, S. (2015). Personal Data Protection Act 2010: Taking the First Steps towards Compliance: Akta Perlindungan Data Peribadi 2010: Mengambil Langkah Awal ke arah Pematuhan. Journal of Management and Muamalah, 5(2), 64-75.

Sheperdson, B (2024), Malaysia's PDPA Amendment 2024: What Organisations Need to Know, https://www.dpexnetwork.org/articles/malaysias-pdpa-amendment-2024-what-organisations-need-to-know, accessed on 1 August 2025

Sholehuddin, N., Miskam, S., Mohd Shahwahid , F. ., Raja Abdul Aziz , T. N. ., & Mansor, N. (2024). A Comparative Legal Analysis on Personal Data Protection Laws in Selected ASEAN Countries: Analisis Perundangan Perbandingan Undang-undang Perlindungan Data Peribadi di Negara-negara ASEAN . Journal of Muwafaqat, 7(1), 23–38.

Solikhah, M. (2025). Personal Data Protection in the Era of Digital Transformation: Challenges and Solutions in the Indonesian Cyber Law Framework, Vol. 2 No. 1 (2025): Indonesian Cyber Law Review

Sudarwanto, A. S & Kharisma, D.B. (2022). Comparative study of personal data protection regulations in Indonesia, Hong Kong and Malaysia. Journal of Financial Crime 30 September 2022; 29 (4): 1443–1457