The current issue and full text archive of this journal is available at
https://muwafaqat.uis.edu.my/index.php/journal
DOI: https://doi.org/10.53840/muwafaqat.v9i2.260

Reconstructing Data Privacy Governance in Islamic Fintech Social Finance in Malaysia and Indonesia through Maqasid al-Shariah

Penstrukturan Semula Tadbir Urus Privasi Data dalam Kewangan Sosial Islam Berasaskan Fintech di Malaysia dan Indonesia Menurut Perspektif Maqasid Syariah

SRI WAHYU SAKINA AHMAD SANUSI
(Corresponding Author)
Faculty of Economics, Accounting and Management
Universiti Islam Selangor (UIS)
43000 Kajang, Selangor, Malaysia.
sriwahyu@uis.edu.my

NAWAL SHOLEHUDDIN
Faculty of Syariah and Law
Universiti Islam Selangor (UIS)
43000 Kajang, Selangor, Malaysia
nawal@uis.edu.my

NOOR AIMI MOHD PUAD
Kuliyyah of Economics and Management Sciences
International Islamic University Malaysia
50728 Kuala Lumpur, Malaysia
nooraimi@iium.edu.my

SURIANOM MISKAM
Faculty of Syariah and Law
Universiti Islam Selangor (UIS)
43000 Kajang, Selangor, Malaysia
surianom@uis.edu.my

Muamalat & Islamic Social Finance

121

Submitted date: 11 August 2026
Revised date: 28 October 2026
Acceptance date: 31 October 2026
Available online: 31 October 2026

The current issue and full text archive of this journal is available at
https://muwafaqat.uis.edu.my/index.php/journal

HAMZAH ROBBANI
RAHMAT DWI PUTRANTO
RADIAN SYAM
IBLAM School of Law, Indonesia
hamzahrabbani8@gmail.com, putranto@iblam.ac.id
radiansyam@iblam.ac.id

ABSTRACT

The rapid expansion of Islamic financial technology (Islamic Fintech) has transformed the administration of Islamic social finance, particularly in the management of zakat, waqf, and sadaqah. Digital platforms have significantly enhanced operational efficiency, transparency, and financial inclusion by facilitating wider participation from donors and improving the distribution of charitable funds. Nevertheless, the increasing reliance on digital technologies has simultaneously intensified concerns regarding the protection of personal data, especially information relating to donors and vulnerable beneficiaries. Existing legal frameworks in Malaysia and Indonesia provide statutory safeguards through the Personal Data Protection Act (PDPA) 2010 (Amendment 2024) and Indonesia's Personal Data Protection Law (Law No. 27 of 2022). However, these regulations primarily emphasise legal compliance while providing limited consideration of Islamic ethical obligations and the higher objectives of Shariah (Maqasid al-Shariah). This conceptual study critically analyses data privacy governance in Islamic Fintech social finance from the perspective of Maqasid al-Shariah. Using qualitative doctrinal and comparative legal analysis, the study examines regulatory provisions alongside Islamic legal principles derived from the Qur'an, Sunnah, classical juristic writings, and contemporary Islamic governance literature. The analysis demonstrates that personal data within Islamic social finance should not merely be regarded as digital assets requiring legal protection but should instead be recognised as Data Stewardship, a sacred trust entrusted to Islamic institutions. Accordingly, protecting personal information represents the fulfilment of several objectives of Maqasid al-Shariah, particularly the preservation of religion (*Hifz al-Din*), life and dignity (*Hifz al-Nafs* and *Hifz al-'Ird*), intellect (*Hifz al-'Aql*), and wealth (*Hifz al-Mal*). The study proposes a Maqasid-Based Data Privacy Governance Framework that integrates legal compliance, Islamic ethics, institutional accountability, cybersecurity governance, and public trust into a holistic governance model for Islamic social finance institutions. Unlike conventional privacy frameworks that emphasise regulatory obligations, the proposed framework positions data governance as an act of religious stewardship (*amanah*) that promotes justice (*'adl)*, public interest (maslahah), transparency, and sustainable digital governance. The proposed framework contributes to the growing discourse on Islamic digital governance and offers practical guidance for policymakers, regulators, zakat institutions, waqf authorities, and Islamic Fintech providers in strengthening public confidence while ensuring that technological innovation remains consistent with the objectives of Maqasid al-Shariah.

Keywords: Islamic Fintech, Data Privacy, *Maqasid al-Shariah*, Islamic Social Finance, Data Stewardship, Governance

The current issue and full text archive of this journal is available at
https://muwafaqat.uis.edu.my/index.php/journal

ABSTRAK

Perkembangan pesat teknologi kewangan Islam (*Islamic Fintech*) telah mengubah landskap pentadbiran kewangan sosial Islam, khususnya dalam pengurusan zakat, wakaf dan sedekah. Platform digital telah meningkatkan kecekapan operasi, ketelusan serta keterangkuman kewangan dengan memperluaskan penyertaan penyumbang dan mempertingkatkan keberkesanan agihan dana kebajikan. Walau bagaimanapun, peningkatan penggunaan teknologi digital turut menimbulkan kebimbangan terhadap perlindungan data peribadi, khususnya maklumat berkaitan penyumbang dan golongan penerima manfaat yang terdedah. Kerangka perundangan sedia ada di Malaysia dan Indonesia menyediakan perlindungan statutori melalui Akta Perlindungan Data Peribadi 2010 (Pindaan 2024) dan Undang-Undang Perlindungan Data Peribadi Indonesia (Undang-Undang No. 27 Tahun 2022). Namun demikian, peraturan tersebut lebih menumpukan kepada pematuhan undang-undang berbanding penerapan tanggungjawab etika Islam serta objektif utama Syariah (*Maqasid al-Shariah*). Kajian konseptual ini menganalisis tadbir urus privasi data dalam *Islamic Fintech* bagi kewangan sosial Islam berdasarkan perspektif *Maqasid al-Shariah*. Berdasarkan pendekatan kualitatif melalui analisis doktrinal dan perbandingan perundangan, kajian ini meneliti peruntukan undang-undang bersama prinsip-prinsip Syariah yang bersumberkan al-Quran, al-Sunnah, karya-karya klasik fiqh serta literatur kontemporari berkaitan tadbir urus Islam. Dapatan kajian menunjukkan bahawa data peribadi dalam kewangan sosial Islam tidak seharusnya dilihat semata-mata sebagai aset digital yang memerlukan perlindungan undang-undang, sebaliknya perlu diurus berdasarkan prinsip pengawasan data (*data stewardship*) sebagai satu amanah yang dipertanggungjawabkan kepada institusi Islam. Justeru, perlindungan data peribadi merupakan manifestasi kepada pemeliharaan beberapa objektif utama *Maqasid al-Shariah*, khususnya pemeliharaan agama (*Hifz al-Din*), nyawa dan maruah (*Hifz al-Nafs* dan *Hifz al-'Ird*), akal (*Hifz al-'Aql*) serta harta (*Hifz al-Mal*). Kajian ini seterusnya mencadangkan Kerangka Tadbir Urus Privasi Data Berasaskan Maqasid (*Maqasid-Based Data Privacy Governance Framework*) yang mengintegrasikan pematuhan undang-undang, etika Islam, akauntabiliti institusi, tadbir urus keselamatan siber dan kepercayaan awam dalam satu model tadbir urus yang holistik bagi institusi kewangan sosial Islam. Berbeza dengan kerangka privasi data konvensional yang lebih menekankan aspek pematuhan peraturan, kerangka yang dicadangkan meletakkan tadbir urus data sebagai satu bentuk tanggungjawab berasaskan prinsip *amanah* yang memupuk keadilan (*'adl*), kemaslahatan (*maslahah*), ketelusan dan kelestarian tadbir urus digital. Kerangka ini menyumbang kepada perkembangan wacana tadbir urus digital Islam serta menyediakan panduan praktikal kepada penggubal dasar, pihak pengawal selia, institusi zakat, pihak berkuasa wakaf dan penyedia *Islamic Fintech* dalam memperkukuh keyakinan masyarakat serta memastikan inovasi teknologi sentiasa selari dengan objektif *Maqasid al-Shariah*.

Keywords: Teknologi Kewangan Islam (Islamic Fintech), Privasi Data, Maqasid al-Shariah, Kewangan Sosial Islam, Pengawasan Data (*Data Stewardship*), Tadbir Urus

INTRODUCTION

The digital transformation of financial services has fundamentally reshaped Islamic finance by expanding the use of mobile platforms, crowdfunding, blockchain, artificial intelligence, and other data-intensive technologies. Islamic Fintech has consequently become an important channel for widening financial access and improving service efficiency, while also generating new governance, Shariah, cybersecurity, and data-protection concerns (Alshater et al., 2022; Kasmon et al., 2024; Kasmon et al., 2024). Within Islamic social finance, these technologies increasingly support the collection, management, and distribution of zakat, waqf, and sadaqah, making the governance of personal and financial information an integral part of institutional accountability (Kamaruddin et al., 2023).

The emergence of Islamic Fintech has transformed traditional philanthropic practices into digital ecosystems that support online donations, beneficiary registration and verification, digital payment channels, crowdfunding, and increasingly data-driven allocation and monitoring. A systematic review of FinTech applications in Islamic social finance identifies crowdfunding, blockchain, banking services, and peer-to-peer mechanisms as prominent applications, with transparency, inclusion, innovation, and efficiency among the principal reported benefits (Kasmon et al., 2024). Malaysian evidence likewise shows that zakat and waqf institutions are progressively adopting FinTech across collection, management, and distribution activities (Kamaruddin et al., 2023).

Despite these benefits, digitalisation also creates governance risks that are not unique to Islamic institutions but acquire particular significance in Islamic social finance because zakat and charitable bodies process information about religious giving, financial hardship, household circumstances, eligibility for assistance, and other data relating to potentially vulnerable beneficiaries. In digital zakat, documented concerns include unauthorised access, hacking, misuse of muzakki data, uncertainty over the lawful collection and reporting of personal information, and the security of financial transactions (Insani et al., 2024; Rahmatullah et al., 2024). In Malaysia, security and privacy have also been identified as relevant considerations in users' acceptance of online zakat services (Ahmad et al., 2021). Accordingly, the issue addressed here is not that Islamic institutions face wholly different cyber threats, but that a breach can simultaneously affect privacy, dignity, trust in religious institutions, and the perceived integrity of zakat and waqf administration.

Data privacy governance has therefore become a substantive governance issue for Islamic social finance rather than a purely technical compliance matter. At the regulatory level, Malaysia and Indonesia have both moved toward more comprehensive personal-data regimes, but their institutional and legal settings differ. Malaysia regulates personal data principally through the Personal Data Protection Act 2010 (Act 709), strengthened by the Personal Data Protection (Amendment) Act 2024 and subsequent guidance on data-breach notification, data-protection officers and data protection by design. Indonesia enacted Law No. 27 of 2022 on Personal Data

Protection as a comprehensive national framework applicable across public and private processing contexts. These regimes establish important legal safeguards, yet they do not by themselves articulate how Islamic social-finance institutions should translate statutory duties into a specifically Islamic ethic of stewardship, dignity, justice and prevention of harm.

The Qur'an repeatedly emphasises the obligation to safeguard trust and uphold justice. Personal information entrusted to Islamic institutions therefore constitutes more than digital property; it represents a sacred responsibility that directly influences the dignity, welfare, and rights of individuals. Any negligence in managing personal information may not only violate statutory regulations but may also contradict the higher objectives of Islamic law (Maqasid al-Shariah), which seek to preserve religion, life, intellect, dignity, lineage, and wealth.

Current scholarship on Islamic Fintech has largely examined innovation, adoption, Shariah governance, financial inclusion, regulatory challenges and technological risk (Alshater et al., 2022; Kasmon et al., 2024; Kamaruddin et al., 2023; Kasmon et al., 2024). More recent studies have begun to address personal-data protection directly. Miskam et al. (2025), for example, examine personal-data safeguards in Shariah-compliant investment platforms, while Rahmatullah et al. (2024) identify legal uncertainty concerning the collection, use and reporting of muzakki data by Indonesian zakat organisations and online platforms. Insani et al. (2024) similarly identify hacking, misuse of personal data and financial-transaction security as material risks in digital zakat. These studies demonstrate a concrete governance problem, although the published evidence located for this study more commonly documents vulnerabilities, regulatory gaps and potential misuse than publicly verified breach incidents involving named zakat or waqf institutions. This distinction is important: the motivation for the present study is grounded in documented exposure and governance gaps rather than an unsupported claim of widespread reported breaches. The remaining theoretical gap is the absence of an integrated model that systematically connects contemporary data-protection duties with Maqasid al-Shariah across the Islamic social-finance data lifecycle.

Accordingly, this article uses data stewardship as the bridge between data privacy and Maqasid al-Shariah. Data stewardship refers here to the responsible custody of personal information throughout its lifecycle : collection, use, sharing, storage, security, retention and disposal so that data are handled not merely because legislation requires it, but because the institution holds the information in trust. In an Islamic social-finance setting, this stewardship is framed by amanah (trust), 'adl (justice), maslahah (public interest), prevention of harm and accountability. Maqasid al-Shariah then provides the evaluative lens for determining what responsible stewardship should protect: dignity and wellbeing (Hifz al-Nafs and Hifz al-'Ird), informed agency and freedom from manipulation (Hifz al-'Aql), property and financial security (Hifz al-Mal), and faithful fulfilment of entrusted religious responsibilities (Hifz al-Din). This relationship converts abstract Maqasid objectives into governance requirements and, conversely, gives legal privacy principles an Islamic ethical rationale (Chapra, 2008; Kamali, 2008a; Auda,

2008). On this basis, the study proposes a Maqasid-Based Data Privacy Governance Framework integrating legal compliance, digital amanah, privacy by design, cybersecurity, institutional accountability, and transparency and public trust.

The primary objective of this study is to examine data privacy governance in Islamic Fintech social finance through the perspective of Maqasid al-Shariah and to propose a governance framework that integrates Islamic ethical principles with contemporary legal requirements in Malaysia and Indonesia.

Specifically, this study aims:

1. To examine the concept of data privacy in Islamic Fintech social finance from the perspective of Maqasid al-Shariah, particularly the objectives of preserving religion (*Hifz al-Din*), life and human dignity (*Hifz al-Nafs* and *Hifz al-'Ird*), intellect (*Hifz al-'Aql*), and wealth (*Hifz al-Mal*).
2. To critically analyse the existing legal and regulatory frameworks governing personal data protection in Islamic Fintech social finance in Malaysia and Indonesia in light of Islamic ethical values and the principles of Maqasid al-Shariah.
3. To develop a Maqasid-Based Data Privacy Governance Framework that integrates Islamic ethical principles, legal compliance, institutional governance, and cybersecurity practices to strengthen public trust and sustainable governance in Islamic social finance

LITERATURE REVIEW

The rapid digitalisation of Islamic social finance has created new opportunities for efficiency, inclusion and transparency while expanding the volume and sensitivity of data processed by zakat and waqf institutions. Empirical and review studies show increasing use of digital payment channels, crowdfunding, blockchain and other FinTech applications in the sector (Kamaruddin et al., 2023; Kasmon et al., 2024). These developments improve reach and operational capability, but they also heighten the importance of security, privacy, governance and institutional trust (Ahmad et al., 2021; Insani et al., 2024).

Within conventional information governance, privacy is protected through legal rights, organisational accountability, fair processing principles and technical safeguards; information ethics also emphasises the moral significance of how information is created, processed and used (Floridi, 2013; Solove, 2008). Islamic governance adds a further normative dimension: information entrusted to an institution is an amanah, requiring honesty, confidentiality, justice and accountability beyond minimum legal compliance (Beekun, 1997; Haniffa & Hudaib, 2007; Hassan & Muneeza, 2014). Consequently, data governance in Islamic social finance can be assessed simultaneously as a legal, organisational and Shariah-ethical responsibility.

Among the earliest systematic discussions of Maqasid, al-Ghazali articulated the protection of the essential necessities of religion, life, intellect, lineage and wealth, while

al-Shatibi further developed the role of maslahah and the prevention of harm in understanding the purposes of Shariah (Al-Ghazali, 1993; Al-Shatibi, n.d.). Contemporary scholars have extended Maqasid reasoning to questions of governance, development and complex modern systems (Ibn Ashur, 2006; Kamali, 2008a; Auda, 2008; Chapra, 2008). These developments support the use of Maqasid as a normative framework for evaluating digital governance where technological practices affect dignity, autonomy, property, trust and social welfare.

Although classical jurists did not explicitly discuss digital privacy, the principles underlying Maqasid provide a robust normative framework for addressing contemporary technological challenges. Personal information represents an extension of individual identity and dignity; therefore, its protection aligns directly with the preservation of human welfare envisioned by Islamic law. Unlike secular legal frameworks that primarily regulate data through contractual rights and statutory obligations, Maqasid approaches data governance as an ethical responsibility rooted in accountability to Allah SWT.

This distinction is particularly relevant within Islamic social finance, where institutions manage sensitive information relating to vulnerable beneficiaries. Mishandling personal information not only violates legal obligations but also undermines public trust (*amanah*), social justice (*'adl*), and institutional integrity. Consequently, data privacy should be understood as an essential component of Islamic governance rather than merely a technical cybersecurity issue.

Contemporary privacy law treats personal information as information linked to identifiable individuals and regulates its processing through principles such as lawfulness, notice, consent, purpose limitation, security and accountability (Solove, 2008). In Islamic social finance, however, personal data also carry an ethical dimension because the institution receives the information in the course of fulfilling a religious and social mandate. This is consistent with Islamic governance literature in which accountability is not confined to contractual or shareholder relationships but extends to moral responsibility, trust and social justice (Iqbal & Mirakhor, 2011; Haniffa & Hudaib, 2007; Hassan & Muneeza, 2014). The Qur'anic commands to render trusts and uphold justice (Qur'an 4:58) and to avoid betrayal of trusts (Qur'an 8:27) therefore provide a normative basis for treating responsible data custody as part of institutional amanah.

From an Islamic perspective, however, personal information possesses an additional moral dimension. Information entrusted to Islamic institutions represents an *amanah*, requiring custodians to exercise honesty, confidentiality, and justice throughout the data lifecycle. The Qur'an explicitly commands believers to fulfil trusts and judge with justice (Qur'an 4:58), while another verse prohibits believers from betraying entrusted responsibilities (Qur'an 8:27). These verses establish trustworthiness as a foundational ethical obligation applicable to both physical and digital assets.

Accordingly, this study operationalises Data Stewardship as the responsible custody of personal information across the entire data lifecycle. The concept links conventional

privacy duties - lawful collection, purpose limitation, data minimisation, security, transparency, accountability and breach response - with Islamic ethical duties of amanah, 'adl, mas'uliyyah and prevention of harm. Its analytical value is that it provides an intermediate governance concept between positive law and Maqasid al-Shariah: legal rules identify minimum duties, stewardship describes how institutions discharge those duties in practice, and Maqasid evaluates whether those practices protect dignity, intellect, wealth, religious responsibility and public welfare. This approach is consistent with broader information-ethics scholarship on responsible information practices (Floridi, 2013) and Islamic governance scholarship on trust and accountability (Beekun, 1997; Hassan & Muneeza, 2014).

The Data Stewardship concept therefore serves as an established governance practice adapted to this setting for understanding data governance in Islamic social finance and forms the conceptual foundation of the governance framework proposed in this study.

Table 1: Selected Foundational and Contemporary Literature
(Narrative Synthesis; Not A Systematic Review)

Author(s)	Year	Context	Key Findings	Research Gap
Al-Ghazali	1993 (translated edition)	Maqasid al-Shariah	Introduced five essential objectives (*al-daruriyyat al-khams*)	No discussion of digital governance
Al-Shatibi	2003 (translated edition)	Maqasid theory	Public welfare (*maslahah*) as objective of Shariah	Technology not addressed
Ibn Ashur	2006	Contemporary Maqasid	Expanded Maqasid to social reform and governance	No application to data governance
Kamali	2008	Islamic jurisprudence	Human dignity, privacy and justice are integral to Islamic law	Limited discussion of digital privacy
Auda	2008	Systems approach to Maqasid	Proposed dynamic, multidimensional interpretation of Maqasid	Fintech not examined
Haniffa & Hudaib	2007	Islamic governance	Accountability extends beyond shareholders to Allah SWT	No data privacy perspective
Lewis	2001	Islamic corporate governance	Amanah is central to governance	Predates digital economy
Kamaruddin et al.	2023	Islamic social finance FinTech	FinTech adoption in Malaysian zakat and waqf institutions creates opportunities and governance challenges	Does not develop a Maqasid-based data-privacy framework

Rahmatullah et al.	2024	Indonesia: zakat and personal data	Identifies legal uncertainty and potential personal-data breaches in digital zakat management	Focuses on legal reform rather than integrated Maqasid governance
Miskam et al.	2025	Malaysia: Islamic FinTech and personal data	Examines legal and ethical personal-data protection in Shariah-compliant investment platforms	Not specific to Islamic social finance and does not integrate the full Maqasid-data lifecycle
Fidhayanti et al.	2025	Indonesia PDP Law	Indonesia adopts comprehensive personal data governance	Shariah integration remains limited
Al-Ghazali	1993 (translated edition)	Maqasid al-Shariah	Introduced five essential objectives (*al-daruriyyat al-khams*)	No discussion of digital governance
Al-Shatibi	2003 (translated edition)	Maqasid theory	Public welfare (*maslahah*) as objective of Shariah	Technology not addressed
Ibn Ashur	2006	Contemporary Maqasid	Expanded Maqasid to social reform and governance	No application to data governance
Kamali	2008	Islamic jurisprudence	Human dignity, privacy and justice are integral to Islamic law	Limited discussion of digital privacy
Auda	2008	Systems approach to Maqasid	Proposed dynamic, multidimensional interpretation of Maqasid	Fintech not examined
Haniffa & Hudaib	2007	Islamic governance	Accountability extends beyond shareholders to Allah SWT	No data privacy perspective
Lewis	2001	Islamic corporate governance	Amanah is central to governance	Predates digital economy
Kamaruddin et al.	2023	Islamic social finance FinTech	FinTech adoption in Malaysian zakat and waqf institutions creates opportunities and governance challenges	Does not develop a Maqasid-based data-privacy framework
Rahmatullah et al.	2024	Indonesia: zakat and personal data	Identifies legal uncertainty and potential personal-data breaches in digital zakat management	Focuses on legal reform rather than integrated Maqasid governance

Miskam et al.	2025	Malaysia: Islamic FinTech and personal data	Examines legal and ethical personal-data protection in Shariah-compliant investment platforms	Not specific to Islamic social finance and does not integrate the full Maqasid-data lifecycle
Fidhayanti et al.	2025	Indonesia PDP Law	Indonesia adopts comprehensive personal data governance	Shariah integration remains limited
Al-Ghazali	1993 (translated edition)	Maqasid al-Shariah	Introduced five essential objectives (*al-daruriyyat al-khams*)	No discussion of digital governance

RESEARCH METHODOLOGY

This study adopts a qualitative doctrinal legal research design complemented by comparative and thematic analysis. Doctrinal research is appropriate where the research question requires systematic interpretation of legislation, regulatory guidance and normative legal principles, while comparative analysis enables those rules to be examined across jurisdictions and against a common analytical lens (Hutchinson & Duncan, 2012). The design is also suitable for Islamic Fintech research because the field sits at the intersection of rapidly evolving technology regulation, Shariah governance and institutional practice; a document-based approach allows legal rules, Islamic jurisprudential principles and sector-specific FinTech literature to be analysed together before empirical validation of the proposed framework.

The doctrinal component identifies and interprets the applicable legal rules, while the Maqasid analysis evaluates their ethical purpose and implications for Islamic social finance. This combination avoids treating Shariah values as a separate discussion appended to statutory analysis. Instead, the study uses legal requirements as the minimum governance baseline and Maqasid al-Shariah as the normative lens through which the adequacy and purpose of those requirements are assessed. The approach is consistent with methodological guidance that doctrinal legal research systematically analyses legal texts and principles and can be combined with broader theoretical analysis where the research question requires normative evaluation (Hutchinson & Duncan, 2012).

A comparative dimension is incorporated to examine Malaysia and Indonesia because both are major Muslim-majority jurisdictions with active Islamic-finance and Islamic-social-finance ecosystems, yet they employ different institutional arrangements for data protection and the administration of zakat and waqf. Malaysia combines a federal personal-data regime with state-based Islamic religious administration, while Indonesia combines a national PDP law with national legislation on zakat and waqf. Both jurisdictions have also experienced substantial digitalisation of Islamic social finance, making them analytically useful for examining how common privacy principles operate

within different legal and institutional structures (Kamaruddin et al., 2023; Kasmon et al., 2024; Rahmatullah et al., 2024). The comparison therefore seeks analytical variation rather than claiming that the two systems are identical.

Primary Legal Sources

Primary legal sources include legislation, regulations, and official policy documents governing personal data protection and Islamic financial services.
For Malaysia, these include:

i. Personal Data Protection Act 2010 (Act 709)
ii. Personal Data Protection (Amendment) Act 2024
iii. Islamic Financial Services Act 2013
iv. Guidelines issued by the Personal Data Protection Department (JPDP)
v. Relevant policy documents issued by Bank Negara Malaysia (BNM)

Selected state Islamic-administration, zakat and waqf enactments relevant to the governance of beneficiary and contributor information, together with federal waqf policy instruments, were also considered where they illuminate the institutional context. These include Pekeliling Am Bilangan 1 Tahun 2020 on voluntary cash-waqf salary deductions for public officers and the state waqf-law materials compiled by JAWHAR. These instruments are treated as contextual governance sources rather than as substitutes for the PDPA.

For Indonesia, the study analyses:

i. Law No. 27 of 2022 on Personal Data Protection
ii. Law No. 21 of 2008 on Sharia Banking
iii. Law No. 23 of 2011 on Zakat Management
iv. Law No. 41 of 2004 on Waqf
v. Regulations issued by the Financial Services Authority (OJK)

Classical Islamic Sources

The Islamic normative framework is derived from:

i. The Holy Qur'an
ii. Authentic Hadith literature
iii. Classical works on Maqasid al-Shariah, particularly those of Imam al-Ghazali and Imam al-Shatibi
iv. Contemporary Maqasid literature by Ibn Ashur, Mohammad Hashim Kamali, and Jasser Auda

These sources provide the theological and ethical foundations for evaluating data privacy from an Islamic perspective.

Academic Literature

Peer-reviewed journal articles, academic books, conference proceedings, and book chapters indexed in Scopus, Web of Science, and MyCITE were examined through a targeted narrative review. Particular attention was given to publications discussing:

i. Islamic Fintech
ii. Islamic Social Finance
iii. Data Privacy
iv. Cybersecurity
v. Islamic Corporate Governance
vi. Maqasid al-Shariah
vii. Digital Ethics

Institutional Documents

Additional documentary evidence includes official publications from:

i. Bank Negara Malaysia
ii. Jabatan Perlindungan Data Peribadi (JPDP)
iii. Financial Services Authority Indonesia (OJK)
iv. BAZNAS
v. State Islamic Religious Councils (MAIN)
vi. International organisations such as AAOIFI and IFSB where relevant

The documentary materials were identified through a targeted documentary and narrative literature search using major academic databases, including Scopus, Web of Science, Google Scholar, HeinOnline, and LexisNexis. The search strategy employed combinations of keywords such as:

i. Islamic Fintech
ii. Data Privacy
iii. Personal Data Protection
iv. Islamic Social Finance
v. Zakat
vi. Waqf
vii. Maqasid al-Shariah
viii. Amanah
ix. Islamic Governance
x. Malaysia
xi. Indonesia

The literature search covered publications from 2000 to September 2026, while foundational classical and modern Maqasid works were included irrespective of date. Publications in English, Bahasa Melayu/Malay and Bahasa Indonesia were eligible where they were directly related to Islamic finance, Islamic social finance, data governance, privacy, cybersecurity, Islamic jurisprudence or governance. The principal emphasis was on peer-reviewed and authoritative sources; duplicate records, non-scholarly opinion pieces and sources without sufficient bibliographic or institutional

credibility were excluded. Earlier seminal works were retained where necessary to establish the theoretical foundations of Maqasid, Islamic governance and information ethics.

The collected documents were analysed using thematic content analysis supported by comparative legal analysis.The thematic analysis was conducted in four sequential stages.

First, relevant documentary evidence was organised according to recurring themes associated with Islamic Fintech, data governance, legal compliance, cybersecurity, Islamic ethics, and Maqasid al-Shariah.

Second, statutory provisions governing personal data protection in Malaysia and Indonesia were comparatively examined to identify similarities, differences, strengths, and regulatory limitations.

Third, the identified legal principles were interpreted through the framework of Maqasid al-Shariah by examining their contribution towards the preservation of:

i. *Hifz al-Din* (protection of religion)
ii. *Hifz al-Nafs* (protection of life and human dignity)
iii. *Hifz al-'Aql* (protection of intellect)
iv. *Hifz al-'Ird* (protection of honour and dignity)
v. *Hifz al-Mal* (protection of wealth)

Finally, findings from both legal and Islamic analyses were synthesised to construct a Maqasid-Based Data Privacy Governance Framework. The framework integrates statutory compliance, Islamic ethical principles, institutional governance, and cybersecurity practices into a unified governance model specifically designed for Islamic Fintech social finance institutions.

To enhance the credibility of the study, documentary cross-checking was applied by integrating multiple documentary sources, including legislation, classical Islamic jurisprudence, contemporary scholarly publications, and official institutional documents. Data were continuously compared across different jurisdictions and academic perspectives to minimise interpretative bias and improve analytical consistency.

Interpretive comparison was achieved by interpreting the documentary material through three complementary lenses: positive data-protection law, Maqasid al-Shariah and Islamic governance/data-stewardship principles. Triangulation in qualitative research strengthens analysis by examining a phenomenon through multiple sources or theoretical perspectives rather than relying on a single interpretive frame (Patton, 1999). Here, convergence between statutory duties, sector literature and Islamic ethical principles was used to identify governance elements that could be justified from more than one analytical perspective.

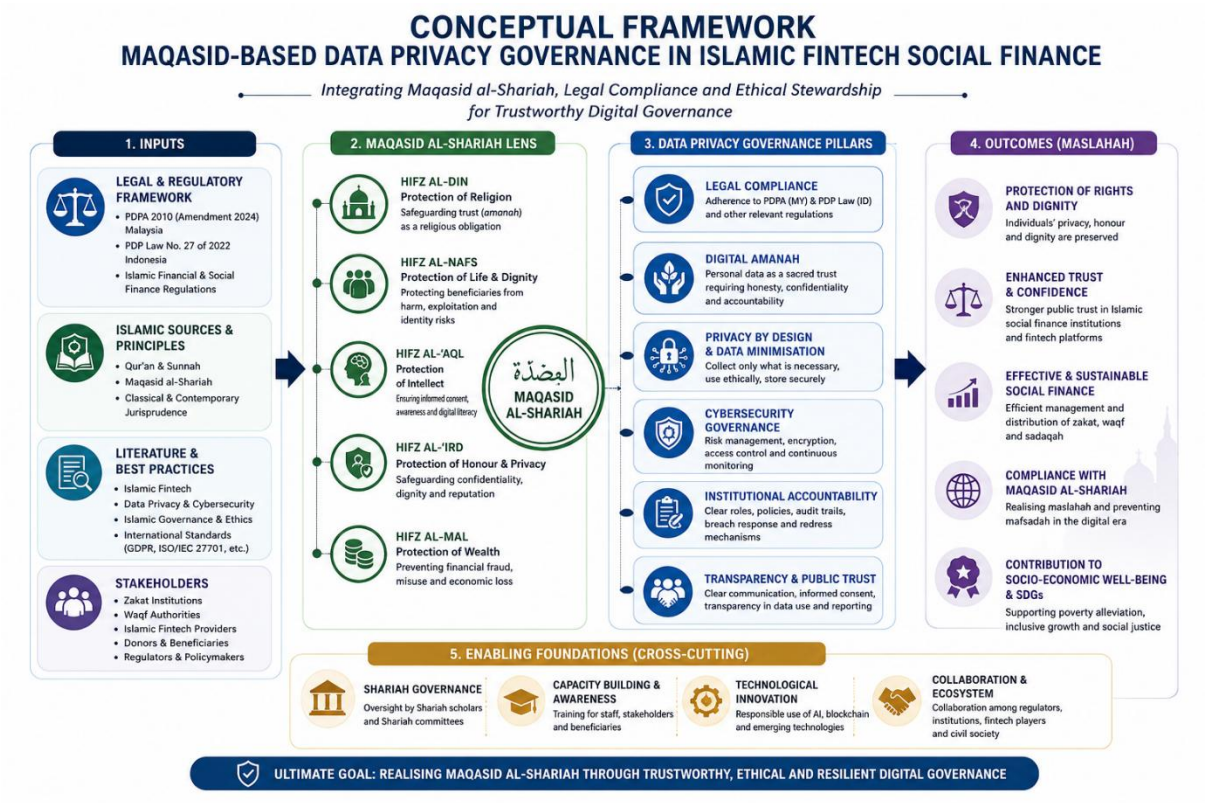
Each proposed linkage was assessed by (1) identifying a concrete processing practice and foreseeable harm; (2) locating the applicable legal duty where established; (3) identifying the Islamic ethical duty and the Maqasid interest protected; and (4) selecting a feasible governance control. These links are interpretive and many-to-many, not exclusive classifications: accuracy can serve hifz al-mal and hifz al-nafs as well as hifz al-'aql, while purpose limitation can protect dignity and financial security simultaneously. Documentary comparison reduces interpretive arbitrariness but does not constitute empirical validation or expert consensus. Future Delphi or practitioner validation is required.

This article undergo a documentary analysis protocol. Each instrument was considered using the following fields: jurisdiction; issuing authority; instrument and version; operative scope; institutional category; relevant section/article; data subject rights; controller/processor duties; exceptions; enforcement; and Maqasid-related risk. The analysis compares the legal baseline before making a normative recommendation. The literature component is a purposive narrative synthesis, not a systematic review or PRISMA study; no reproducible database screening counts are claimed. Potentially relevant 2026 Indonesian amendments and implementing regulations mentioned by the reviewer require independent gazette confirmation before being stated as operative law. No unverified commencement date is adopted here.

CONCEPTUAL FRAMEWORK OF THE STUDY

Figure 1 illustrates the conceptual framework underpinning this study. The framework demonstrates how statutory legal requirements and Islamic ethical principles converge through Maqasid al-Shariah to produce an integrated governance model for protecting personal data in Islamic Fintech Social Finance.

Figure 1: Conceptual Framework Maqasid-Based Data Privacy Governance in Islamic Fintech Social Finance



The conceptual framework is organised as a sequential logic. First, the study identifies two sets of inputs: contemporary legal/privacy requirements and Islamic normative principles. Second, those inputs are interpreted through the Maqasid objectives most directly implicated by personal-data processing. Third, the analysis translates the resulting normative expectations into governance mechanisms such as lawful processing, privacy by design, cybersecurity, accountability and transparency. Finally, the expected governance outcomes are assessed in terms of protection of rights and dignity, ethical public trust, sustainable social-finance delivery and maslahah. The framework therefore does not treat Maqasid as an additional compliance checklist; it functions as the evaluative layer that explains why particular privacy controls matter in an Islamic social-finance context and what human and social interests those controls are intended to protect.

FINDINGS AND DISCUSSION

The literature reviewed demonstrates that the rapid digitalisation of Islamic social finance has created unprecedented opportunities for improving transparency, financial inclusion, and operational efficiency. At the same time, it has introduced complex governance challenges concerning the protection of personal data. Although Malaysia and Indonesia have enacted comprehensive legal frameworks to regulate data protection, the analysis indicates that current governance mechanisms remain predominantly compliance-oriented. Existing regulations prescribe statutory obligations relating to consent, data processing, breach notification, and organisational accountability, yet they provide limited guidance on the ethical responsibilities expected of Islamic institutions entrusted with managing sensitive information belonging to donors and beneficiaries.

From the perspective of Maqasid al-Shariah, protecting personal information extends beyond legal compliance. Data governance should be regarded as an institutional manifestation of *amanah* (trust), where every stage of the information lifecycle is guided by justice (*'adl*), public interest (*maslahah*), accountability (*mas'uliyyah*), and the prevention of harm (*darar*). Accordingly, this discussion reconstructs existing data privacy governance by integrating contemporary legal requirements with the higher objectives of Islamic law.

The comparative analysis demonstrates that both Malaysia and Indonesia have made substantial progress in strengthening personal data protection. Malaysia's Personal Data Protection Act 2010, particularly following the 2024 amendments, introduces mandatory breach notification, greater organisational accountability, and stronger enforcement mechanisms. Likewise, Indonesia's Personal Data Protection Law No. 27 of 2022 adopts a comprehensive approach inspired by international standards, extending legal obligations to both public and private organisations.

Despite these improvements, both regulatory systems remain principally designed around legal compliance. Organisations are required to fulfil statutory responsibilities through documentation, consent management, security controls, and regulatory reporting. Such mechanisms undoubtedly enhance legal certainty but provide relatively limited consideration of Islamic ethical responsibilities associated with managing information belonging to vulnerable members of society.

The limitations of a purely legal-centred approach are relevant to charitable organisations generally because many charities process sensitive donor and beneficiary information. They are especially salient in Islamic social finance, however, because zakat and waqf institutions combine charitable functions with explicit religious mandates and may process data revealing financial hardship, eligibility as asnaf, religious giving, household circumstances and other indicators of vulnerability. Consequently, a privacy failure may create conventional harms such as fraud or unauthorised disclosure while also undermining dignity, religious trust and confidence in the administration of Islamic funds. Studies of digital zakat in Malaysia and Indonesia

have accordingly highlighted security, privacy, personal-data misuse and regulatory uncertainty as governance concerns (Ahmad et al., 2021; Insani et al., 2024; Rahmatullah et al., 2024). The framework proposed in this study is therefore tailored to Islamic social finance, although several of its governance controls may also be transferable to other charitable institutions.

Conventional data governance generally regards personal information as an organisational asset requiring legal protection. Islamic jurisprudence offers a broader ethical understanding by recognising entrusted information as an *amanah* carrying both legal and spiritual obligations.

The Qur'an stated:

> *Indeed, Allah commands you to render trusts to whom they are due and when you judge between people to judge with justice.*
>
> (Surah al-Nisa', 4:58)

Similarly:

> *O you who believe! Do not betray Allah and the Messenger, nor betray your trusts knowingly.*
>
> (Surah al-Anfal, 8:27)

These verses establish that every entrusted responsibility carries moral accountability before Allah SWT. Within Islamic Fintech, personal information should therefore be understood not merely as digital data but as a sacred trust requiring responsible stewardship.

The Data Stewardship concept developed in this study extends data governance by combining responsible information custody with Islamic institutional accountability. Rather than describing privacy protection as ibadah in a manner that substitutes theology for law, the study treats stewardship as an organisational duty: institutions must know what data they hold, why they hold it, who may access it, how long it is retained, how it is secured, and how harm is prevented or remedied. In Islamic social finance, amanah supplies the ethical foundation for this duty, while Maqasid provides criteria for evaluating its consequences. This formulation draws on information ethics, which treats information practices as morally consequential (Floridi, 2013), and Islamic governance scholarship emphasising trust, accountability and social responsibility (Beekun, 1997; Haniffa & Hudaib, 2007; Hassan & Muneeza, 2014).

Reconstructing Data Privacy through Maqasid al-Shariah

The findings from the literature indicate that each objective of Maqasid al-Shariah provides distinct guidance for contemporary data governance.

Hifz al-Din (Protection of Religion)

Protecting entrusted information fulfils religious obligations concerning honesty, trust, and accountability. Institutions handling Islamic charitable funds must therefore regard data governance as part of their religious responsibility rather than simply administrative compliance.

Hifz al-Nafs (Protection of Life and Human Dignity)

Beneficiary information often contains highly sensitive socio-economic information. Data breaches may expose individuals to discrimination, social exclusion, and psychological distress. Protecting confidentiality therefore directly preserves human dignity.

Hifz al-'Aql (Protection of Intellect)

Digital literacy, informed consent, transparency, and responsible use of artificial intelligence enable individuals to make informed decisions regarding their personal information while reducing algorithmic manipulation and misinformation.

Hifz al-'Ird (Protection of Honour)

Unlike conventional financial data, beneficiary information frequently reveals personal hardship and social vulnerability. Protecting confidentiality safeguards personal honour and prevents unnecessary public exposure.

Hifz al-Mal (Protection of Wealth)

Strong cybersecurity controls, fraud prevention mechanisms, encryption, and secure identity verification protect both financial assets and personal information against misuse and identity theft. Collectively, these objectives demonstrate that effective data governance contributes directly to achieving *maslahah* while simultaneously preventing *mafsadah*.

Accountability does not require indiscriminate publication of personal information. A proportionate maslahah assessment should identify the legitimate reporting purpose, assess foreseeable harm, consider aggregated or redacted alternatives, restrict access and record the decision. Confidentiality is not absolute: valid court orders, legally mandated reporting and prevention of serious harm may justify carefully limited disclosure. In each case the institution should document the legal basis, necessity, recipient, minimisation measures and audit trail. This reconciles hisbah (oversight/accountability) with satr (protection against unnecessary exposure).

Proposed Maqasid-Based Data Privacy Governance Framework

Drawing upon the comparative legal analysis and Maqasid al-Shariah, this study proposes a Maqasid-Based Data Privacy Governance Framework comprising six mutually reinforcing governance pillars.

Framework Development And Integration Logic

The proposed framework was developed through a four-step synthesis. First, the comparative legal analysis extracted recurring privacy obligations from Malaysia and Indonesia, including lawful processing, consent/notice, purpose limitation, security, accountability and breach response. Second, the literature review identified sector-specific governance concerns in Islamic Fintech and Islamic social finance, particularly cybersecurity, trust, beneficiary vulnerability, digital-platform accountability and data misuse.

Third, these legal and sectoral themes were mapped to Maqasid objectives and Islamic governance principles. For example, confidentiality and minimisation protect dignity (*Hifz al-Nafs*/*Hifz al-'Ird*); clear information and meaningful consent support informed agency (*Hifz al-'Aql*); cybersecurity and fraud prevention protect property (*Hifz al-Mal*); and faithful handling of information entrusted through zakat and waqf administration reflects amanah and *Hifz al-Din*.

Fourth, overlapping themes were consolidated into six governance pillars that are sufficiently distinct for implementation but mutually reinforcing in practice.

The framework is specifically contextualised for Islamic Fintech social finance in Malaysia and Indonesia. Legal compliance represents the mandatory baseline; Digital Amanah supplies the stewardship ethic; Privacy by Design embeds privacy requirements into digital systems and workflows; Cybersecurity Governance protects confidentiality, integrity and availability; Institutional Accountability assigns responsibility, oversight and remedy; and Transparency and Public Trust ensures intelligible communication and accountable relationships with donors and beneficiaries. Maqasid al-Shariah operates across all six pillars rather than as a seventh pillar. It is the evaluative lens connecting each control to the human interest it protects and to the prevention of mafsadah. Therefore, this article proposed:

Pillar 1: Legal Compliance
Compliance with national data protection legislation forms the minimum governance requirement.

Pillar 2: Digital Amanah
Personal information is recognised as a sacred trust requiring ethical stewardship.

Pillar 3: Privacy by Design
Privacy considerations should be embedded throughout the system development lifecycle rather than introduced after implementation.

Pillar 4: Cybersecurity Governance
Robust cybersecurity controls ensure confidentiality, integrity, availability, and resilience against evolving cyber threats.

Pillar 5: Institutional Accountability
Clear governance structures, defined responsibilities, internal audits, breach management procedures, and continuous oversight strengthen institutional integrity.

Pillar 6: Transparency and Public Trust
Transparent communication, informed consent, and ethical reporting practices strengthen public confidence in Islamic social finance institutions. Rather than functioning independently, these governance pillars reinforce one another and collectively contribute towards the realisation of Maqasid al-Shariah within the digital ecosystem.

Figure 2 : Maqasid-based Data Privacy Governance Framework

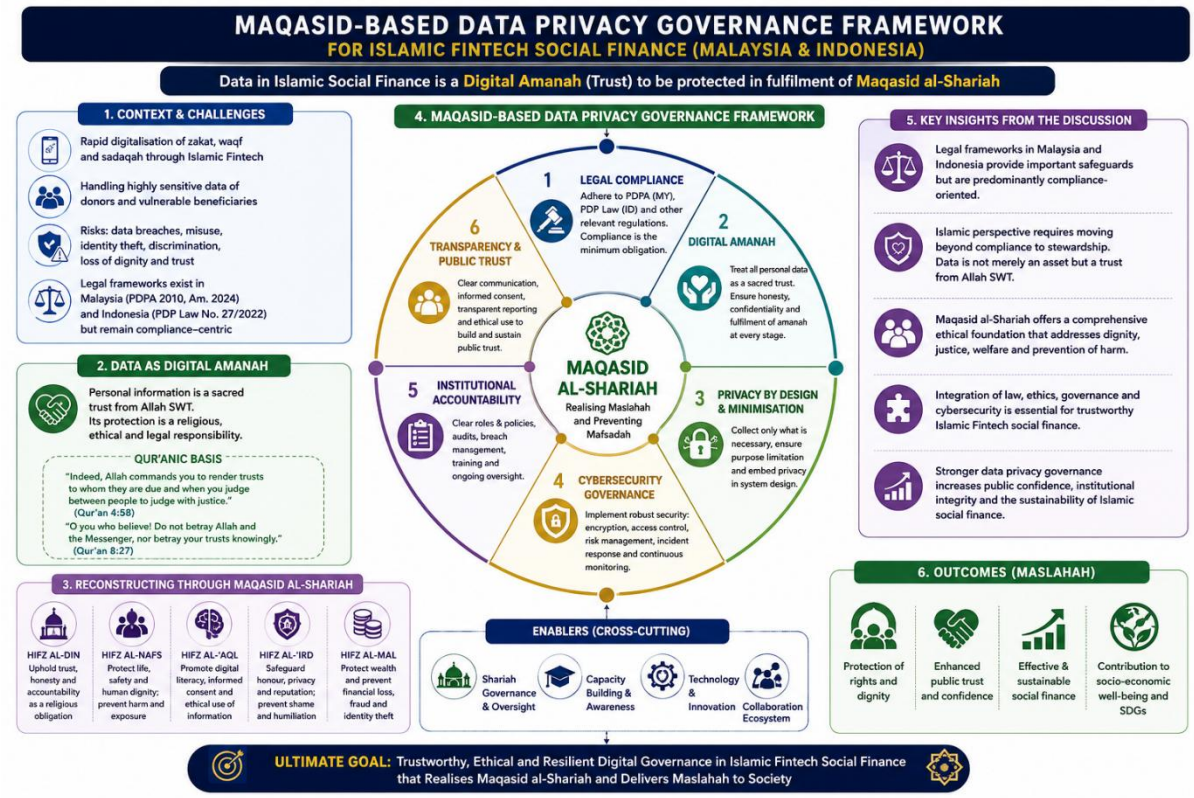


Table 2 : Mapping Contemporary Data Privacy Principles to Maqasid al-Shariah and Islamic Governance

Contemporary Data Privacy Principle	**Relevant Legal Requirement**	**Maqasid al-Shariah Objective**	**Islamic Governance Principle**	**Practical Implication for Islamic Fintech Social Finance**
Lawfulness and lawful processing	PDPA 2010 (MY); PDP Law 2022 (ID)	*Hifz al-Din* (Protection of Religion)	Amanah (Trust)	Personal data must be processed honestly and ethically as a religious obligation, not merely a legal requirement.
Informed consent	Consent before data collection	*Hifz al-'Aql* (Protection of Intellect)	*Ikhtiyar* (Free Choice)	Individuals should understand why their data are collected and how they will be used before giving consent.
Purpose limitation	Data used only for stated purposes	*Hifz al-'Ird* (Protection of Honour and Privacy)	*Satr* (Confidentiality)	Personal information should never be disclosed or reused beyond the original charitable purpose.
Data minimisation	Collect only necessary information	*Hifz al-Nafs* (Protection of Life and Human Dignity)	*Ihsan* (Benevolence)	Islamic institutions should avoid collecting excessive personal information that could expose beneficiaries to unnecessary risks.
Accuracy of data	Data integrity principle	*Hifz al-'Aql*	*'Adl* (Justice)	Accurate information ensures fair eligibility assessment and equitable distribution of zakat, waqf and sadaqah.
Confidentiality	Security safeguards	*Hifz al-'Ird*	*Amanah* and *Satr*	Beneficiaries' identities, financial conditions and personal circumstances must remain confidential.
Cybersecurity protection	Encryption, access control, breach management	*Hifz al-Mal* (Protection of Wealth)	*Mas'uliyyah* (Responsibility)	Robust cybersecurity prevents financial fraud, identity theft and unauthorised access to sensitive information.
Accountability	Data controller	*Hifz al-Din*	*Hisbah*	Islamic institutions

	responsibility		(Institutional Accountability)	should establish internal governance mechanisms, audits and oversight to ensure responsible data stewardship.
Transparency	Privacy notice and reporting	*Hifz al-'Aql*	*Sidq* (Truthfulness)	Islamic institutions should clearly disclose how personal data are collected, used, shared and protected, enabling donors and beneficiaries to make informed decisions while strengthening public trust.
Breach notification	Mandatory reporting of incidents	*Hifz al-Nafs* and *Hifz al-Mal*	*Maslahah* (Public Interest)	Prompt reporting minimises harm, restores public confidence and protects beneficiaries from further risks.
Contemporary Data Privacy Principle	Relevant Legal Requirement	*Maqasid al-Shariah* Objective	Islamic Governance Principle	Practical Implication for Islamic Fintech Social Finance.
Lawfulness and lawful processing	PDPA 2010 (MY); PDP Law 2022 (ID)	*Hifz al-Din* (Protection of Religion)	*Amanah* (Trust)	Personal data must be processed honestly and ethically as a religious obligation, not merely a legal requirement.
Informed consent	Consent before data collection	*Hifz al-'Aql* (Protection of Intellect)	*Ikhtiyar* (Free Choice)	Individuals should understand why their data are collected and how they will be used before giving consent.
Purpose limitation	Data used only for stated purposes	*Hifz al-'Ird* (Protection of Honour and Privacy)	*Satr* (Confidentiality)	Personal information should never be disclosed or reused beyond the original charitable purpose.
Data minimisation	Collect only necessary information	*Hifz al-Nafs* (Protection of Life and Human	*Ihsan* (Benevolence)	Islamic institutions should avoid collecting excessive personal information

		Dignity)		that could expose beneficiaries to unnecessary risks.
Accuracy of data	Data integrity principle	*Hifz al-'Aql*	*'Adl* (Justice)	Accurate information ensures fair eligibility assessment and equitable distribution of zakat, waqf and sadaqah.
Confidentiality	Security safeguards	*Hifz al-'Ird*	*Amanah* and Satr	Beneficiaries' identities, financial conditions and personal circumstances must remain confidential.
Cybersecurity protection	Encryption, access control, breach management	*Hifz al-Mal* (Protection of Wealth)	*Mas'uliyyah* (Responsibility)	Robust cybersecurity prevents financial fraud, identity theft and unauthorised access to sensitive information.
Accountability	Data controller responsibility	*Hifz al-Din*	*Hisbah* (Institutional Accountability)	Islamic institutions should establish internal governance mechanisms, audits and oversight to ensure responsible data stewardship.
Transparency	Privacy notice and reporting	*Hifz al-'Aql*	*Sidq* (Truthfulness)	Islamic institutions should clearly disclose how personal data are collected, used, shared and protected, enabling donors and beneficiaries to make informed decisions while strengthening public trust
Breach notification	Mandatory reporting of incidents	*Hifz al-Nafs* and *Hifz al-Mal*	*Maslahah* (Public Interest)	Prompt reporting minimises harm, restores public confidence and protects beneficiaries from further risks.

Contemporary Data Privacy Principle	Relevant Legal Requirement	*Maqasid al-Shariah* Objective	Islamic Governance Principle	Practical Implication for Islamic Fintech Social Finance
Lawfulness and lawful processing	PDPA 2010 (MY); PDP Law 2022 (ID)	*Hifz al-Din* (Protection of Religion)	*Amanah* (Trust)	Personal data must be processed honestly and ethically as a religious obligation, not merely a legal requirement.
Informed consent	Consent before data collection	*Hifz al-'Aql* (Protection of Intellect)	*Ikhtiyar* (Free Choice)	Individuals should understand why their data are collected and how they will be used before giving consent.
Purpose limitation	Data used only for stated purposes	*Hifz al-'Ird* (Protection of Honour and Privacy)	*Satr* (Confidentiality)	Personal information should never be disclosed or reused beyond the original charitable purpose.
Data minimisation	Collect only necessary information	*Hifz al-Nafs* (Protection of Life and Human Dignity)	*Ihsan* (Benevolence)	Islamic institutions should avoid collecting excessive personal information that could expose beneficiaries to unnecessary risks.
Accuracy of data	Data integrity principle	*Hifz al-'Aql*	*'Adl* (Justice)	Accurate information ensures fair eligibility assessment and equitable distribution of zakat, waqf and sadaqah.
Confidentiality	Security safeguards	*Hifz al-'Ird*	*Amanah* and *Satr*	Beneficiaries' identities, financial conditions and personal circumstances must remain confidential.
Cybersecurity protection	Encryption, access control, breach management	*Hifz al-Mal* (Protection of Wealth)	*Mas'uliyyah* (Responsibility)	Robust cybersecurity prevents financial fraud, identity theft and unauthorised access to sensitive information.

CONCLUSION

The digital transformation of Islamic social finance has expanded the reach and efficiency of zakat, waqf and sadaqah while increasing the amount and sensitivity of personal information processed through digital platforms. Malaysia and Indonesia now possess stronger personal-data frameworks, but this study shows why statutory compliance should be treated as the baseline rather than the complete governance objective for Islamic social-finance institutions. Through the concept of Data Stewardship, the article connects legal privacy duties to amanah and uses Maqasid al-Shariah to evaluate the interests those duties should protect. The resulting Maqasid-Based Data Privacy Governance Framework integrates six mutually reinforcing pillars: legal compliance, Digital Amanah, Privacy by Design, cybersecurity governance, institutional accountability, and transparency and public trust. Its distinctive contribution lies not in replacing conventional privacy law with religious norms, but in explaining how Islamic ethical objectives can guide the responsible implementation of legal and technical privacy controls in zakat, waqf and related digital social-finance activities.

This article provides practical guidance for regulators, Islamic financial institutions, and Fintech providers in developing governance practices that balance technological innovation with Islamic ethical principles. Future research should empirically validate the proposed framework across different Islamic social finance institutions and jurisdictions to assess its practical applicability and effectiveness. Ultimately, embedding Maqasid al-Shariah into data privacy governance ensures that digital innovation serves not only regulatory compliance but also the broader objectives of justice, human dignity, and *maslahah*, thereby supporting a trustworthy and sustainable Islamic digital financial ecosystem.

ACKNOWLEDGEMENT

This paper is part of the research grants supported by Selangor Islamic University under the UIS Innovation Research Grant No. 2025/P/GPIU/GPI-003 and managed by the Research and Innovation Management Centre (RIMC) Selangor Islamic University (UIS), Bandar Seri Putra, 43000, Kajang, Selangor, Malaysia.

REFERENCES

Ahmad, N., Arshad Ayub, R. I. R., & Arshad Ayub, N. F. S. N. (2021). Analysing the drivers affecting the intention to use online zakat payment among Muslim in Shah Alam, Selangor. International Journal of Islamic Business, 6(1). https://doi.org/10.32890/ijib2021.6.1.3

Alam, N., Gupta, L., & Zameni, A. (2019). Fintech and Islamic Finance: Digitalization, Development and Disruption. Palgrave Macmillan.

Al-Ghazali, A. H. (1993). *Al-Mustasfa min 'Ilm al-Usul* (Vols. 1–2). Dar al-Kutub al-'Ilmiyyah.

Alshater, M. M., Saba, I., Supriani, I., & Rabbani, M. R. (2022). Fintech in Islamic finance literature: A review. Heliyon, 8(9), e10385. https://doi.org/10.1016/j.heliyon.2022.e10385

Auda, J. (2008). *Maqasid al-Shariah as philosophy of Islamic law: A systems approach*. International Institute of Islamic Thought.

Bank Negara Malaysia. (2020). *Risk Management in Technology (RMiT)*. Bank Negara Malaysia.

Beekun, R. I. (1997). *Islamic business ethics*. International Institute of Islamic Thought.

Chapra, M. U. (2008). *The Islamic vision of development in the light of Maqasid al-Shariah*. International Institute of Islamic Thought.

Floridi, L. (2013). *The ethics of information*. Oxford University Press.

Haniffa, R., & Hudaib, M. (2007). Exploring the ethical identity of Islamic banks via communication in annual reports. *Journal of Business Ethics, 76*(1), 97–116. https://doi.org/10.1007/s10551-006-9272-5

Hassan, R., & Muneeza, A. (2014). Shariah corporate governance: The need for a special governance code. Corporate Governance, 14(1), 120–129.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: Doctrinal legal research. Deakin Law Review, 17(1), 83-119. https://doi.org/10.21153/dlr2012vol17no1art70

Ibn Ashur, M. T. (2006). *Treatise on Maqasid al-Shariah* (M. El-Mesawi, Trans.). International Institute of Islamic Thought.

Insani, N., Rohaya, N., Mutiara, U., & Maguchu, P. (2024). Legal protection for personal data security and muzakki financial transactions on digital zakat platform. Jurnal Hukum Novelty, 15(1), 70-86.

Iqbal, Z., & Mirakhor, A. (2011). *An introduction to Islamic finance: Theory and practice* (2nd ed.). Wiley.

Kamali, M. H. (2008a). Maqasid al-Shariah made simple. International Institute of Islamic Thought.*Maqasid al-Shariah made simple*. International Institute of Islamic Thought.

Kamali, M. H. (2008b). Shari'ah law: An introduction. Oneworld Publications.*Shari'ah law: An introduction*. Oneworld Publications.

Kamaruddin, M. I. H., Hanefah, M. M., Shaharuddin, A., Ayedh, A. M. A., & Othman, N. A. (2023). Development of FinTech in Islamic social finance in Malaysia. International Journal of Economics, Management and Accounting, 31(1), 177-204. https://doi.org/10.31436/ijema.v31i1.1143

Kasmon, B., Ibrahim, S. S., Daud, D., Raja Hisham, R. R. I., & Prajanti, S. D. W. (2024). FinTech application in Islamic social finance in Asia region: A systematic literature review. International Journal of Ethics and Systems, 41(1), 213-237. https://doi.org/10.1108/IJOES-07-2023-0155

Lewis, M. K. (2001). Islam and accounting. *Accounting Forum, 25*(2), 103–127. https://doi.org/10.1111/1467-6303.00058

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, 10(2), 55-68. https://doi.org/10.53840/myjict10-2-234

Otoritas Jasa Keuangan. (2023). Peraturan OJK Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan. https://ojk.go.id/id/regulasi/Pages/Pelindungan-Konsumen-dan-Masyarakat-di-Sektor-Jasa-Keuangan.aspx

Patton, M. Q. (1999). Enhancing the quality and credibility of qualitative analysis. Health Services Research, 34(5 Pt 2), 1189-1208.

Rahmatullah, I., Suwadi, P., & Purwadi, H. (2024). Legal reform of zakat management based on personal data protection law in Indonesia. Mazahib, 23(1), 199-236. https://doi.org/10.21093/mj.v23i1.5917

Solove, D. J. (2008). Understanding Privacy. Harvard University Press.

Statutes/Standards/Guidelines

Jabatan Wakaf, Zakat dan Haji (JAWHAR). (2020). Pekeliling Am Bilangan 1 Tahun 2020: Tatacara Pelaksanaan Sumbangan Wakaf Tunai Melalui Potongan Gaji Secara Sukarela Bagi Pegawai Awam Yang Berkhidmat di Wilayah Persekutuan dan Negeri.

Personal Data Protection Commissioner of Malaysia. (2024). Personal Data Protection (Amendment) Act 2024 (Act A1727). https://www.pdp.gov.my/ppdpv1/en/akta/personal-data-protection-amendment-act-2024/

Personal Data Protection Commissioner of Malaysia. (2025). Personal Data Protection Guidelines on Data Breach Notification. https://www.pdp.gov.my/ppdpv1/en/akta/personal-data-protection-guidelines-on-data-breach-notification-dbn/

Republic of Indonesia. (2004). *Law No. 41 of 2004 concerning Waqf*.

Republic of Indonesia. (2008). *Law No. 21 of 2008 concerning Sharia Banking*.

Republic of Indonesia. (2011). *Law No. 23 of 2011 concerning Zakat Management*.

Republic of Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Republic of Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022