BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Open Finance
Policy Document

Applicable to −
1. Licensed banks
2. Licensed investment banks
3. Licensed Islamic banks
4. Licensed insurers
5. Licensed takaful operators
6. Prescribed development financial institutions
7. Eligible e-money issuers

Issued on: 17 November 2026 BNM/RH/PD 028-145

TABLE OF CONTENTS

PART A OVERVIEW 3
1 Introduction 3
2 Applicability 5
3 Legal provision 5
4 Effective date 5
5 Interpretation 5
6 Related policy documents and legal instruments 9
7 Circulars superseded 10
PART B POLICY REQUIREMENTS 11
8 Governance 11
9 Participation and scope of information sharing 13
10 Transition arrangements 15
11 Consent management 15
12 Customer protection 20
13 Management of technology risk 25
PART C APPENDICES 27
Appendix 1 Definition of mandated FSP and scope of specified information 27
Appendix 2 Transition arrangements 28

PART A OVERVIEW

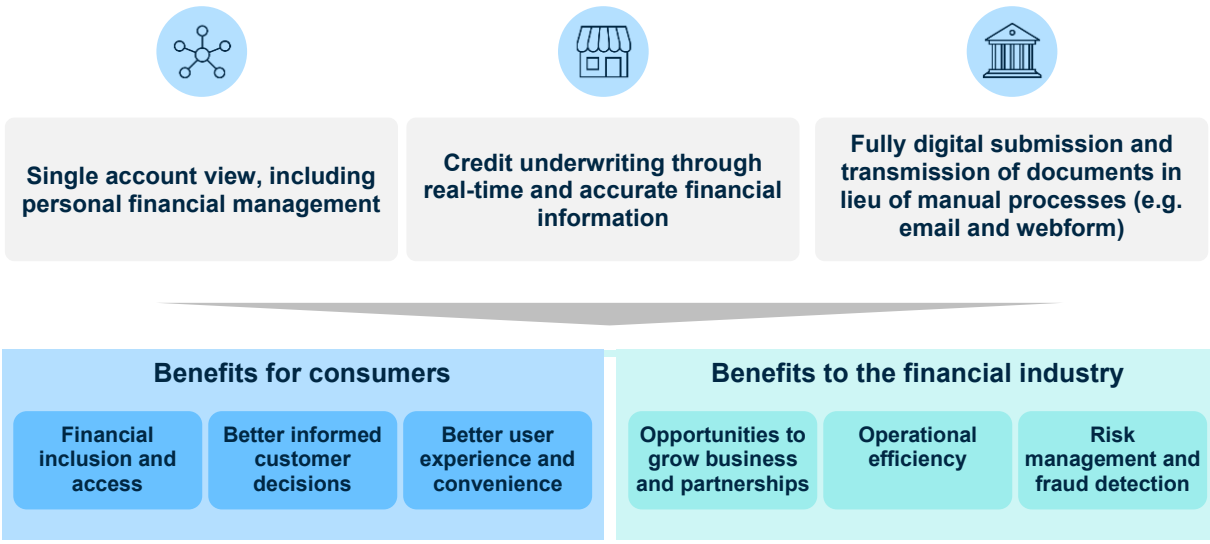
1 Introduction

1.1 As the financial sector continues to evolve in the digital age, the volume of customer information being processed has grown significantly alongside the increasing shift of transactions to digital platforms. This underscores the importance of having strong infrastructures that enable the secure access, sharing and processing of financial information, which is a critical foundation for maintaining trust and resilience in an increasingly digital financial system.

1.2 Open finance plays a pivotal role in advancing this vision by offering customers a safer and more structured framework for sharing their financial information compared to existing data sharing arrangements in Malaysia. By enabling consent-driven information sharing, open finance is intended to provide customers with greater control over their personal financial information, allowing them to actively determine and manage how their information is shared, accessed and used. Beyond empowering customers, open finance has the potential to unlock data-driven innovation that can enable customers to make better informed decisions about their finances, facilitate the delivery of more personalised financial services and promote greater financial inclusion as illustrated in Diagram 1.

Diagram 1

Illustrative* potential use cases



*Use cases listed are for illustrative purposes only and are neither exhaustive nor indicative of endorsement from Bank Negara Malaysia (BNM).

1.3 This policy document sets out the regulatory framework for open finance which seeks to ensure that it is implemented in an efficient, resilient and secure fashion. Taking into account requirements provided in the Personal Data Protection Act 2010 (PDPA) and other relevant data privacy and protection requirements, the policy document seeks to promote responsible data sharing that strikes an appropriate balance between financial innovation and prudent management of risks.

1.4 In this regard, this policy document sets out requirements and expectations relating to, among others –

(a) the criteria under which financial service providers are mandated to participate as data providers and data consumers in open finance, guided by the principle of reciprocity;
(b) the scope of customer information that data providers are required to share upon obtaining customer consent;
(c) the timeline for mandated participation and for the sharing of customer information;
(d) the management of customer consent throughout its lifecycle which encompasses the act of obtaining, monitoring, renewing and revoking consent;
(e) the measures and controls to safeguard customer information; and
(f) the management of technology and cyber risks associated with open finance.

1.5 Building an open finance ecosystem will be a multi-year journey and requires collective action from all stakeholders to ensure its orderly and secure implementation. As such, Bank Negara Malaysia (BNM) will gradually phase in the requirements in this policy document. This is intended to facilitate orderly adoption by the industry, while enabling customers and other ecosystem stakeholders to develop familiarity and confidence in open finance.

1.6 BNM also envisions that the principles underpinning open finance can support broader arrangements for more open and secure data sharing beyond the financial industry. As set out in the Financial Sector Blueprint 2022-2026, BNM and the financial sector will continue to collaborate with stakeholders in other sectors and industries, including the public sector, to support and champion efforts to foster a thriving open data ecosystem at the national level. Such efforts will focus on improving accessibility to public data under the Government's open

data initiatives through a standardised approach to data governance, and supporting regional level data sharing initiatives by advancing best practices aligned with global standards and policies.

2 Applicability

2.1 This policy document is applicable to all FSPs as defined in paragraph 5.2.

3 Legal provision

3.1 The requirements in this policy document are issued pursuant to –

(a) sections 47, 123 and 143 of the Financial Services Act 2013 (FSA);

(b) sections 57, 135 and 155 of the Islamic Financial Services Act 2013 (IFSA); and

(c) sections 41, 42C and 116 of the Development Financial Institutions Act 2002 (DFIA).

3.2 The guidance in this policy document is issued pursuant to section 266 of the FSA, section 277 of the IFSA and section 126 of the DFIA.

4 Effective date

4.1 This policy document comes into effect upon its issuance date except where otherwise stated explicitly in this policy document.

5 Interpretation

5.1 The terms and expressions used in this policy document shall have the same meanings assigned to them in the FSA, IFSA and DFIA, as the case may be, unless otherwise defined in this policy document.

5.2 For the purpose of this policy document –

"S" denotes a standard, an obligation, a requirement, specification, direction, condition and any interpretative, supplemental and transitional provisions that must be complied with. Non-compliance may result in enforcement action;

"G" denotes guidance which may consist of statements or information intended to promote common understanding and advice or recommendations that are encouraged to be adopted;

"active customer" refers to any person who uses or has used any financial service or product offered by any FSP, excluding persons whose only accounts with the FSP are closed, suspended or dormant[1];

"active user" refers to an e-money user who conducts at least one financial transaction per month to make payment or funds transfer using e-money or to reload e-money into the e-money account;

"banking group" refers to a group comprising a banking institution and other banking institutions that control, or are controlled by, or are under common control with, the banking institution, excluding foreign branches and subsidiaries operating outside Malaysia;

"banking institution" refers to a licensed bank, licensed investment bank or licensed Islamic bank;

"board" refers to the board of directors of an FSP, including a committee of the board where the responsibilities of the board set out in this policy document have been delegated to such a committee;

"customer" refers to any person who uses or has used, or may be intending to use[2] any financial service or product offered by any FSP;

"customer information" refers to any information relating to the affairs or the account of any customer of any FSP in whatever form, including in the form of a record, book, register, correspondence, other document or material;

"data consumer" refers to an FSP that is authorised by the customer to access their information from a data provider upon obtaining the customer's consent for

[1] A dormant account is typically an account in which there have been no financial transactions or other activity, whether initiated by the customer or otherwise, for a period of at least one (1) year or more from the last date of transaction.

[2] Any person who may be intending to use refers to a potential customer who has provided their information to the FSP for purposes of using the FSP's financial service or product, including a person who subsequently withdraws their application or whose application has been rejected by the FSP.

the provision of any financial product or service in relation to an open finance arrangement;

"data provider" refers to an FSP that holds customer information and is responsible for responding to any authorised information sharing request initiated by the customer in relation to an open finance arrangement, by making available to the corresponding data consumer the customer information specified;

"electronic money" or **"e-money"** refers to a payment instrument or Islamic payment instrument as defined in the Policy Document on Electronic Money[3];

"e-money issuer" or **"EMI"** refers to a person approved by BNM under section 11 or section 15(1)(e) of the FSA or section 11 of the IFSA to issue e-money;

"financial service provider" or **"FSP"** refers to –

(a) a licensed bank under the FSA;
(b) a licensed investment bank under the FSA;
(c) a licensed Islamic bank under the IFSA;
(d) a licensed insurer under the FSA;
(e) a licensed takaful operator under the IFSA;
(f) a prescribed institution under the DFIA; and
(g) an eligible e-money issuer as defined[4] in the Policy Document on Electronic Money[3];

"individual" refers to a natural person aged 18 years and above, in respect of accounts which are under the sole control of that one person[5];

"mandated financial service provider" or **"mandated FSP"** refers to an FSP as specified in Appendix 1;

"open finance" refers to a framework that enables the permissioned sharing of customer information between a data provider and a data consumer in a secure,

[3] Issued on 31 January 2025, including any amendments and modifications made thereafter.

[4] For ease of reference, an "eligible e-money issuer" is defined as an approved issuer of electronic money with substantial market presence based on the criteria set out in Appendix 1 of the Policy Document on Electronic Money or such other criteria as may be specified by BNM from time to time.

[5] For the avoidance of doubt, an account that requires the authority or consent of more than one individual to disclose the relevant customer information (e.g. joint account) does not fall within the mandatory scope applicable to an individual under this policy document.

open, accessible, interoperable and timely manner;

"open finance arrangement" refers to a contractual relationship established between a data provider and a data consumer to enable the permissioned sharing of customer information through an open finance platform;

"open finance platform" or **"platform"** refers to a technical infrastructure, system or utility that enables consent capture and management, as well as facilitates the secure transmission of customer information in an open finance arrangement[6];

"open finance platform operator" or **"platform operator"** refers to any person who operates an open finance platform;

"scope of specified information" refers to the scope of financial information relating to a customer that a data provider is obligated to share with a data consumer, subject to the customer's consent as specified in Appendix 1;

"senior management" refers to the chief executive officer (CEO) and senior officers, who are employed by an FSP or an affiliate of the FSP. This includes, at minimum, senior management roles listed in Appendix 2 of the Policy Document on Responsibility Mapping[7];

"senior officer" refers to a person, other than the CEO, who is employed by an FSP or an affiliate of the FSP, having authority and responsibility for planning, directing or controlling the activities of the FSP;

"small and medium enterprise" or **"SME"** refers to an entity defined as such in the Guideline for New SME Definition issued by the SME Corporation Malaysia in October 2013, as amended or modified from time to time; and

"third-party service provider" refers to an external entity providing services to an FSP that involve the handling of customer information, whether or not those services are in relation to open finance.

[6] Currently, the open finance platform refers to the Open Finance Malaysia (OFM) operated by Payments Network Malaysia Sdn. Bhd. (PayNet). Any changes to this arrangement will be communicated through this policy document or other supplementary documents, as the case may be.

[7] Issued on 29 December 2023, including any amendments and modifications made thereafter.

6 Related policy documents and legal instruments

6.1 Where applicable, this policy document must be read together with any relevant legal instruments, policy documents, guidelines, circulars and supplementary documents that have been issued by BNM, including any amendments or reissuances thereafter, in particular –

(a) Guidelines on Data Management and MIS Framework issued on 29 August 2011;
(b) Guidelines on Imposition of Fees and Charges on Financial Products and Services issued on 10 May 2012;
(c) Guidelines on Data Management and MIS Framework for Development Financial Institutions issued on 5 November 2012;
(d) Policy Document on Risk Governance issued on 1 March 2013;
(e) Policy Document on Operational Risk issued on 10 May 2016;
(f) Policy Document on Corporate Governance issued on 3 August 2016;
(g) Policy Document on Outsourcing issued on 23 October 2019;
(h) Policy Document on Business Continuity Management issued on 19 December 2022;
(i) Policy Document on Responsibility Mapping issued on 29 December 2023;
(j) Policy Document on Anti-Money Laundering, Countering Financing of Terrorism, Countering Proliferation Financing and Targeted Financial Sanctions for Financial Institutions issued on 5 February 2024;
(k) Policy Document on Fair Treatment of Financial Consumers issued on 27 March 2024;
(l) Notification on Specifications on Countermeasures to Combat E-Money Fraud issued on 8 April 2024;
(m) Notification on Specifications on Ensuring Fair Treatment for Victims of Unauthorised e-Banking Transactions issued on 28 June 2024;
(n) Policy Document on Product Transparency and Disclosure issued on 2 December 2024;
(o) Policy Document on Electronic Money (E-Money) issued on 31 January 2025;
(p) Policy Document on Complaints Handling issued on 28 March 2025;
(q) Policy Document on Management of Customer Information and Permitted Disclosures issued on 31 October 2025;
(r) Policy Document on Corporate Governance for Development Financial Institutions issued on 24 June 2026;

(s) Policy Document on Financial Institutions' Response to Fraud issued on 30 June 2026; and

(t) Policy Document on Risk Management in Technology issued on 25 September 2026.

6.2 In implementing an arrangement relating to open finance, an FSP shall also comply with the PDPA, and any other legal instruments, standards or codes issued under such law.

7 Circulars superseded

7.1 This policy document supersedes BNM's Industry Letter on Updates on Participation Timelines for Open Finance issued on 1 September 2026.

The rest of the page is intentionally left blank

PART B POLICY REQUIREMENTS

8 Governance

S 8.1 The board and senior management shall exercise effective oversight of an FSP's implementation of an open finance arrangement to ensure its efficient, resilient and secure operations.

S 8.2 For the avoidance of doubt, the board and senior management shall continue to discharge all applicable responsibilities under the relevant policy documents set out in paragraph 6.1, where such responsibilities relate to an FSP's participation in an open finance arrangement.

Responsibilities of the board

S 8.3 The board shall ensure that a sound risk strategy and appropriate risk management framework are in place and implemented effectively to manage any operational, technology, cyber, fraud, conduct, money laundering, terrorism financing, proliferation financing (ML/TF/PF) or other risk arising from an FSP's participation in an open finance arrangement, in line with the FSP's risk appetite. This includes ensuring that appropriate governance arrangements, processes and controls are in place for identifying, assessing and monitoring the risks and opportunities arising from the FSP's participation in an open finance arrangement, and considering how these factors should be reflected in the FSP's strategies and business plan.

Responsibilities of senior management

S 8.4 Senior management shall be responsible for developing and implementing the framework for managing risk arising from an FSP's participation in an open finance arrangement. The framework shall include policies, procedures and systems that enable the identification, measurement, control and ongoing monitoring of all relevant risks, including risks that the FSP is exposed to arising from information received from other data providers and that it poses to other data consumers through information it provides.

S 8.5 Senior management shall ensure that the risk management framework is developed and maintained having due regard to legal and regulatory requirements, including those set out in paragraph 6.

S 8.6 Senior management shall also have regard to relevant requirements as specified by the open finance platform operator, provided that such requirements are consistent with this policy document, as well as applicable legal and regulatory requirements.

S 8.7 Senior management must designate a senior officer with clear overall responsibility for overseeing the FSP's participation in an open finance arrangement, having regard to the size, complexity and risk profile of the FSP. This includes ensuring implementation readiness, compliance and the ongoing maintenance of policies, procedures and controls relating to open finance activities.

S 8.8 In discharging its responsibility in relation to paragraph 8.7, senior management shall –

(a) ensure that risk management and other appropriate controls are in place and implemented effectively to ensure that customer information is properly safeguarded at all times, including against risks such as unauthorised access, modification or disclosure;

(b) develop and ensure effective implementation of business continuity plans as well as safeguards that support the overall technology risk and business continuity of an FSP's participation in an open finance arrangement. This includes, but is not limited to, ensuring the continuity of services in the event of disruptions, such as system downtime, application programming interface (API) outages, cyber risk incidents or third-party failures;

(c) where the FSP acts as a data provider, ensure that appropriate authentication, controls and oversight arrangements are in place to prevent the disclosure of customer information beyond what has been authorised by the customer, in accordance with paragraphs 11 and 12;

(d) ensure the responsible and legally-compliant use and handling of customer information obtained by the FSP as a data consumer;

(e) put in place an appropriate internal governance and control framework for handling customer complaints and disputes, as well as to provide customer support, in relation to the use of open finance, while ensuring such complaints and disputes are dealt with promptly, fairly and effectively;

(f) ensure that open finance activities are included within the scope of the FSP's risk-based internal audit arrangements, including but not limited to

the effectiveness of policies, procedures and control measures in protecting customer information and API integrations. The scope, frequency and intensity of the internal audit review shall be commensurate with the nature, scale, complexity and risk profile of the FSP's open finance activities. Where an external assurance arrangement is engaged by the FSP as part of its broader technology or control assurance review, the FSP may choose to include open finance in the scope of the arrangement, where deemed appropriate; and

(g) ensure that material issues and concerns relating to the FSP's open finance arrangements are promptly escalated to the board, which include but are not limited to breaches of customer information security and confidentiality.

9 Participation and scope of information sharing

S 9.1 An FSP that seeks to participate[8] as a data provider or a data consumer[9] in an open finance platform shall comply with the relevant requirements in this policy document. Where the platform operator specifies requirements in relation to matters governed by this policy document, the FSP shall comply with such requirements to the extent that they are consistent with this policy document and other applicable legal and regulatory requirements.

S 9.2 Any requirement specified by the platform operator for the purposes of this policy document shall be communicated to participating FSPs and shall be consistent with this policy document and other applicable legal and regulatory requirements. For the avoidance of doubt, compliance with any requirement specified by the platform operator shall not relieve an FSP from complying with its obligations under this policy document.

G 9.3 Where feasible, an FSP is encouraged to adopt open finance as the preferred arrangement for the permissioned sharing of customer information with other FSPs or third parties. For the avoidance of doubt, participation in open finance does not preclude the FSP from undertaking customer information sharing arrangements outside the scope of open finance whether on a bilateral or

[8] This includes mandated FSPs that wish to participate ahead of their timeline for commencement of obligations as a mandated FSP, as specified in Appendix 2, or those that wish to share types of information beyond those specified in Appendix 1.

[9] For the avoidance of doubt, an FSP that wishes to participate as a data consumer on a voluntary basis shall also participate as a data provider.

multilateral basis, subject to existing legal and regulatory requirements.

S 9.4 An FSP shall ensure that any sharing of customer information through an open finance platform is conducted in a secure, resilient and interoperable manner. For this purpose, the FSP shall comply with relevant requirements specified by the open finance platform operator, provided that such requirements are consistent with this policy document, as well as applicable legal and regulatory requirements. Such requirements include, but are not limited to, requirements relating to cyber and technology resilience, business continuity and API specifications.

S 9.5 A mandated FSP shall participate in an open finance platform as a data provider. Upon receiving a customer's request to share their information through the platform, the mandated FSP shall make available the scope of specified information to the relevant data consumer, subject to the scope of consent granted by the customer, as outlined in paragraph 11.1.

G 9.6 Notwithstanding paragraph 9.5, where industry standards and technological solutions permit, and with explicit consent obtained from the customer in the same manner as specified in paragraph 11.1, a data provider may facilitate the sharing of additional customer information beyond the scope of specified information on a voluntary basis[10], in a manner that is consistent with applicable laws and regulatory requirements.

S 9.7 A mandated FSP shall also participate in an open finance platform as a data consumer. In this regard, the mandated FSP shall establish, develop and maintain interfaces that allow a customer to interact with the platform and give permission to retrieve the customer's information from other data providers through the FSP as a data consumer. In its role as a data consumer, the mandated FSP shall develop and operate, at a minimum, the following interfaces:

(a) **Document submission**, where the mandated FSP offers appropriate interfaces that allow customers to direct the platform to request relevant information from other data providers through the platform in a machine-readable and standardised format[11], in lieu of traditional methods of submitting documents (e.g. manual uploading, emailing documents), for

[10] Example may include the sharing of customer information from shared savings accounts.

[11] As specified by the platform operator.

relevant processes (e.g. customer onboarding, ongoing due diligence); and

(b) **Single account view**, where the mandated FSP offers, as part of its digital channels or customer-facing application interfaces, the option for a customer to display relevant information from their accounts with other data providers through the platform.

G 9.8 An FSP participating in an open finance platform as a data consumer may consider adopting principles of inclusivity, accessibility and usability when designing customer-facing interfaces. Particular attention may be given to underserved segments (including customers with basic digital literacy and persons with disabilities) who may face challenges with overly sophisticated interfaces.

S 9.9 An FSP shall provide to BNM any document or information in relation to its participation in open finance upon request by BNM within a period, at such intervals, in the manner or form as may be specified by BNM.

10 Transition arrangements

S 10.1 The obligations of a mandated FSP as a data provider as specified under paragraph 9.5 and as a data consumer as specified under paragraph 9.7 shall commence in accordance with the timeline specified in Appendix 2.

11 Consent management

A. Obtaining consent

S 11.1 An FSP participating in an open finance arrangement, whether in its capacity as a data provider or a data consumer, shall ensure that a secure, verifiable and digital mechanism is in place to obtain consent from a customer prior to disclosing, accessing or processing any customer information. In line with the PDPA and paragraph 13.1 (item 8) of the Policy Document on Management of Customer Information and Permitted Disclosures[12], consent shall be sought and obtained in the following manner:

[12] Or such corresponding paragraph in any amendment or replacement of such policy document.

(a) **Specific**[13] – The data consumer must ensure that the terms seeking a customer's consent are clear, concise and written in plain language. The relevant terms must be specific in relation to the following:
   (i) the person to whom the disclosure will be made[14];
   (ii) the purpose of such disclosure; and
   (iii) the information that will be disclosed;

(b) **Voluntary**[15] – The data consumer shall not, as a condition of providing a financial product/service, compel, coerce or mislead a customer to give consent of their information to third parties beyond what is necessary for the provision of the financial product/service or the performance of the contract with the customer. The data consumer is prohibited from obtaining a customer's consent by asking the customer to indicate consent to a statement or term that combines agreement to the disclosure of their information with other matters in a single statement of consent[16]. For the avoidance of doubt, bundled or blanket consent, such as asking the customer to indicate consent to a statement or term that combines agreement to the disclosure of their information with other matters in a single statement of consent, is prohibited;

(c) **Explicit and deliberate**[17] – A customer must explicitly opt in or deliberately agree[18] to the disclosure of their information to a data consumer by taking an active step to indicate consent. Hence, silence or

[13] For example, where a customer applies for a financial product/service offered by the data consumer, separate and distinct consent must be obtained by the data consumer before disclosing the customer's information to a third party engaged (e.g. data analytics partner) to support the offering of that product or service.

[14] It would be sufficient for the FSP to indicate the categories of third parties to whom the customer information will be disclosed subject to controls in place to protect the information. For example, disclosure to business partners for the promotion of financial products/services. It is unacceptable to use descriptions of third parties which are too broad or vague, such as disclosure to any third parties as the financial institution deems fit.

[15] Consent is not considered as "voluntary" if customers are unable to refuse to provide their consent or feel compelled to give their consent for the disclosure of their information to a data consumer beyond what is necessary for the provision of the financial product/service or the performance of the contract. For example, this includes the disclosure of customer information to a data consumer where consent is secured using a pre-ticked option box which requires customers to opt-out of such an arrangement.

[16] Where consent is sought as a condition for the provision of a financial product/service, the consent does not meet the requirement of being "voluntary" since customers are unable to refuse giving their consent. For example, a data consumer must not require a customer, as part of granting consent for the sharing of customer information under an open finance arrangement, to also consent to the use or disclosure of that information for marketing and promotional purposes. In other words, consent for such additional purposes must be obtained separately and independently of the open finance arrangement.

[17] For consent to be valid, customers must have taken a deliberate action to provide consent to the disclosure of their information. A customer's failure to opt out of a consent statement or term is not considered a valid consent as it does not involve an explicit and deliberate action by the customer.

[18] For example, signing a consent form, ticking an opt-in box electronically, or clicking an opt-in button online.

inaction on the part of the customer does not constitute an explicit and deliberate consent by the customer. The data consumer is prohibited from obtaining a customer's consent using pre-ticked[19] consent statements; and

(d) **Revocable upon request** – A customer must be allowed to revoke their consent given for the disclosure of information at any time unless such disclosure is necessary for the data consumer to comply with any legal or contractual requirements[20]. Furthermore, the customer must be informed of their rights to revoke the consent and how to effect such revocation of consent. The process for revoking consent must be as straightforward as it was to obtain the consent.

B. Managing and monitoring consent

S 11.2 An FSP participating in an open finance arrangement, whether in its capacity as a data provider or a data consumer, shall establish and maintain a digital dashboard accessible to the customer for the purpose of managing and monitoring consent granted under the arrangement. This consent dashboard shall enable the customer to –

(a) view all active and past consents granted, subject to the period determined by the open finance platform;

(b) review the scope (i.e. type of information shared), purpose and duration of each consent; and

(c) revoke consent at any time.

S 11.3 In addition to the functionalities specified in paragraph 11.2, a data consumer shall ensure that its consent dashboard enables the customer to –

(a) renew consent at any time; and

(b) receive timely notifications of consent expiry.

S 11.4 An FSP shall ensure that the consent dashboard reflects the real-time status of consent and is updated immediately upon any renewal, revocation or expiry of consent.

[19] A pre-ticked consent box in a product/service application form does not meet the requirement of being an "explicit and deliberate" consent by a customer as there is no way to definitively establish that the customer consented to the pre-ticked box and the applicable statement/term.

[20] For the avoidance of doubt, where a customer revokes consent to continue with the service, the data consumer may only continue to access the customer's personal data to the extent necessary to cease the service or administer any residual rights and obligations arising from the contractual relationship such as audit or dispute resolution.

C. Consent validity, expiry and renewal

S 11.5 A data consumer shall ensure that any customer consent granted under an open finance arrangement is time-bound and remains valid only for the duration necessary to fulfil the specific purpose for which it was granted.

S 11.6 Where consent is obtained for the purpose of one-time data access, a data consumer shall ensure that such consent is used strictly to retrieve customer information on a single occasion only, in accordance with the specific purpose for which the consent was granted. For the avoidance of doubt, such consent shall expire immediately once the information consented for access has been retrieved by the data consumer.

S 11.7 Where consent is obtained for the purpose of recurring data access (including continuous or repeated access to customer information for activities such as personal financial management), a data consumer shall ensure that such consent remains valid for no longer than six (6) months from the date it was granted, unless revoked earlier by the customer.

S 11.8 Upon the expiry of the consent period, the data provider shall immediately cease any further disclosure of customer information previously authorised by the customer and the data consumer shall cease all access to customer information unless a renewed consent is obtained from the customer. The renewed consent shall be obtained in the same manner and subject to the same conditions applicable to the original consent as specified in paragraph 11.1.

S 11.9 The data consumer shall issue timely notifications to the customer of the upcoming expiry of consent, in accordance with paragraph 11.3, and where appropriate or relevant, notify the customer of the option to renew the consent.

S 11.10 Where a customer does not renew the consent, the data consumer shall ensure that, after the expiry of the remaining consent, the affected customer information is disposed of accordingly, or if such customer information is otherwise continued to be processed, such processing must be carried out solely for the purpose of complying with, and in a manner that is consistent with, applicable laws and regulatory requirements. The data consumer shall implement appropriate safeguards to ensure that the affected customer information is not used or

disclosed for any purpose[21] other than as permitted under such laws and regulatory requirements.

D. Consent revocation

Revocation of consent through data consumer's consent dashboard

S 11.11 Upon receipt of a customer's request to revoke consent through a data consumer's consent dashboard under an open finance arrangement, the data consumer shall immediately cease any further access to customer information previously authorised under the revoked consent and promptly notify the corresponding data provider of the consent revocation.

S 11.12 Upon receipt of a consent revocation notification, the data provider shall immediately cease any further disclosure of customer information to the affected data consumer and take all necessary measures to prevent any subsequent disclosures.

S 11.13 Where a customer revokes consent, the data consumer shall ensure that the affected customer information is handled in the same manner as specified in paragraph 11.10.

S 11.14 The data consumer shall provide the customer with an electronic confirmation[22] that the revocation has been implemented and specify the actions taken in response, including the cessation of access, use and disclosure of the customer information.

Revocation of consent through data provider's consent dashboard

S 11.15 Upon receipt of a customer's request to revoke consent through a data provider's consent dashboard under an open finance arrangement, the data provider shall immediately cease any further disclosure of customer information previously authorised under the revoked consent and promptly notify the corresponding data consumer of the consent revocation to ensure that the data consumer also ceases any further access to the customer's information.

[21] For the avoidance of doubt, the data consumer shall not retain and continue to process the affected customer information (e.g. historical transactions) to enable the customer to access or view such information through its interface, including for activities such as personal financial management, unless the data consumer has obtained the customer's separate consent in the same manner as specified in paragraph 11.1 for such purpose.

[22] For example, electronic confirmation may be provided through in-app notification.

S 11.16 The data provider shall notify the customer of any consent revocation processed through its systems, including relevant timestamps and affected data categories.

S 11.17 Where consent has been revoked, any data sharing under an open finance arrangement shall be permitted only upon obtaining fresh consent from the customer. Such consent shall be obtained in the same manner and subject to the same conditions applicable to the original consent as specified in paragraph 11.1.

E. Record-keeping and audit

S 11.18 An FSP shall log all consent records and actions, including obtaining, revoking and renewing consent, in an auditable format and retain such records for a period of seven (7) years or as required under any applicable laws and regulatory requirements.

S 11.19 In addition to paragraph 11.18, an FSP shall make available to customers relevant data access logs, including when and by whom their information was accessed.

S 11.20 An FSP shall properly document the consent records and management processes, while ensuring that they are readily accessible for review upon request by BNM.

12 Customer protection

A. Management of customer information

Data privacy and confidentiality

S 12.1 In line with paragraph 10.6 of the Policy Document on Management of Customer Information and Permitted Disclosures[23], an FSP shall establish and implement data governance and privacy policies and procedures to safeguard the confidentiality and integrity of customer information collected, accessed, shared, transmitted, disclosed, stored and used through an open finance arrangement.

S 12.2 In addition to paragraph 12.1, the data governance and privacy policies and procedures shall at a minimum –

[23] Or such corresponding paragraph in any amendment or replacement of such policy document.

(a) limit access to customer information to a data consumer on a need-to-know basis;
(b) prohibit the use or disclosure of customer information beyond the purposes and scope for which consent has been granted, except where such use or disclosure is permitted or required under applicable laws or regulatory requirements;
(c) include retention schedules that ensure customer information is not kept longer than necessary; and
(d) mandate secure disposal of customer information when it is no longer required for the purpose for which it was obtained, subject to applicable laws and regulatory requirements.

S 12.3 An FSP shall continually review its data governance and privacy policies to ensure that they remain adequate, relevant and operate effectively in response to changes in the operating environment.

Data security

S 12.4 In line with paragraph 10.12 of the Policy Document on Management of Customer Information and Permitted Disclosures[24], an FSP shall implement technical and operational safeguards to –
(a) prevent theft, loss, misuse or unauthorised access, modification or disclosure of customer information in relation to an open finance arrangement; and
(b) detect and resolve errors and irregularities when they occur.

S 12.5 An FSP shall ensure that any transmission of customer information through an open finance arrangement is conducted through secure means, in line with the relevant requirements set out in the Policy Document on Risk Management in Technology.

S 12.6 Without limiting the generality of paragraphs 12.4 and 12.5, a data provider shall, before authorising the disclosure of customer information, authenticate the customer, using a reliable and effective authentication procedure (e.g. multi-factor authentication) to ensure that the disclosure request originates from the

[24] Or such corresponding paragraph in any amendment or replacement of such policy document.

customer of the data provider[25].

S 12.7 An FSP that is a data consumer shall ensure that customer information received through an open finance arrangement is subject to safeguards that are at least equivalent to those applicable to the FSP's own customer information.

S 12.8 An FSP shall regularly monitor the effectiveness of these controls to ensure that they remain responsive to changing threats.

Third-party arrangements

S 12.9 A data consumer shall not onward disclose customer information obtained from a data provider to another data consumer or any other third or fourth party for that party's own purposes, except where –

(a) explicit customer consent has been obtained in line with the requirements stipulated in paragraph 11.1; and

(b) the data consumer has complied with the requirements applicable to third-party arrangements set out in paragraph 12.10.

S 12.10 An FSP that is a data consumer shall ensure that any third-party service provider involved in handling customer information, regardless of whether it is related to an open finance arrangement, including that associated with data consumer interfaces, outsourcing arrangements or cloud computing services, complies with relevant requirements relating to data privacy, confidentiality and security, as set out in the Policy Document on Management of Customer Information and Permitted Disclosures, the Policy Document on Risk Management in Technology, and the Policy Document on Outsourcing.

S 12.11 For the purposes of paragraph 12.10, an FSP shall ensure that the obligation to safeguard customer information and, where applicable, to dispose of such information is adequately reflected in the service level agreement with the third-party service provider, in line with paragraph 12.4 of the Policy Document on Management of Customer Information and Permitted Disclosures[26].

[25] For the avoidance of doubt, this does not require the data provider to verify or reconcile customer identity information maintained by the data consumer. Each party remains responsible for maintaining its own customer records and authenticating the customer within its respective systems, channels and interfaces.

[26] Or such corresponding paragraph in any amendment or replacement of such policy document.

Customer information breaches

S 12.12 When an FSP experiences a customer information breach arising from an open finance arrangement, the FSP shall comply with all requirements as stipulated in paragraph 11 of the Policy Document on Management of Customer Information and Permitted Disclosures[26] on customer information breaches, and all other obligations as specified under applicable law (e.g. PDPA).

S 12.13 In relation to paragraph 12.12, an FSP shall have in place a customer information breach handling and response plan in the event of theft, loss, misuse or unauthorised access, modification or disclosure of customer information associated with an open finance arrangement. The plan must, at a minimum, include escalation procedures and a clear line of responsibility to contain the customer information breach and take remedial action.

B. Handling disputes and complaints

Clear accountability and liability

S 12.14 An FSP shall ensure that the accountabilities and responsibilities in relation to its participation in an open finance arrangement are clearly stipulated and documented through appropriate arrangements, such as contractual agreements with the open finance platform operator, terms and conditions with customers, or other relevant instruments. Such responsibilities shall include ensuring that customers do not suffer loss or detriment as a result of weaknesses, failures or misconduct on the part of the FSP.

S 12.15 In relation to paragraph 12.14, an FSP shall ensure that the open finance arrangement includes a clear delineation of responsibilities between all parties, particularly with respect to the handling and resolution of customer complaints and disputes, and that each party shall be liable for acts or omissions within their control. This arrangement shall be in accordance with any relevant protocols as may be determined by the platform operator, provided that such protocols are consistent with this policy document, as well as applicable legal and regulatory requirements.

Complaint handling and redress

S 12.16 In line with paragraph 8.1 of the Policy Document on Complaints Handling[27], an FSP shall formulate and implement effective and transparent complaints

[27] Or such corresponding paragraph in any amendment or replacement of such policy document.

handling policies, procedures and processes for timely and fair handling of customer complaints arising from any open finance activities.

S 12.17 For purposes of paragraph 12.16, an FSP shall ensure that the procedures incorporated in its complaint handling policies are compliant with the relevant requirements set out in the Policy Document on Complaints Handling.

S 12.18 Where a complaint or dispute involves more than one FSP, the FSPs concerned shall cooperate in good faith to ensure a coordinated and timely resolution in line with relevant complaints handling protocols as may be determined by the platform operator, and take reasonable measures to ensure that the affected customer is not unduly prejudiced by delays arising from the investigation or determination of responsibility between the relevant parties.

G 12.19 Where practicable, an FSP may endeavour to ensure that channels made available for customers to lodge complaints and access redress are customer-centric and inclusive. These channels should be designed to accommodate varying levels of digital literacy, including providing customers with the option to interact with human personnel where needed.

C. Other business conduct requirements

S 12.20 An FSP shall ensure that the provision of any service arising from any open finance arrangement is conducted in a way that engenders trust and confidence of customers. In this regard, the FSP shall observe relevant consumer and market conduct requirements, which include, but are not limited to –

(a) providing a customer with relevant, clear and timely information, including details on fees, charges, risks and benefits associated with open finance, in line with the Policy Document on Product Transparency and Disclosure, which includes provisions related to electronic banking services; and

(b) ensuring that services associated with an open finance arrangement are rendered in a manner that ensures fair treatment and equitable access for customers, in accordance with the Policy Document on Fair Treatment of Financial Consumers. This includes for the FSP to manage relevant risks and potential harm (e.g. exclusion risk), and where relevant, implement appropriate safeguards. For the avoidance of doubt, the FSP shall not restrict, deter, influence or impose differential treatment on any customer solely due to their decision to grant or withhold their consent under an open finance arrangement, except where it materially affects their

eligibility for such products or services.

S 12.21 An FSP shall ensure that any fees or charges imposed on a customer in connection with open finance are fair and transparent and do not create unreasonable barriers to the customer's access to open finance products or services. Such fees and charges shall also be guided by the principles set out in the Guidelines on Imposition of Fees and Charges on Financial Products and Services.

G 12.22 Where practicable, an FSP may develop and make available a simplified digital and financial literacy guide to support customers in understanding and using products or services enabled by open finance in a safe manner. This guide should be accessible and user-friendly, designed to accommodate varying levels of digital and financial literacy. It should –

(a) introduce customers to the concept of open finance including how their information is shared and used;

(b) provide clear, step-by-step instructions on how to grant, manage and revoke consent; and

(c) include information on available support channels such as customer assistance, complaints handling and redress mechanisms.

13 Management of technology risk

S 13.1 An FSP shall ensure that relevant technology requirements in the Policy Document on Risk Management in Technology are observed in respect of its open finance activities.

S 13.2 An FSP shall ensure that its technology operations management practices are appropriately extended to support its open finance activities. This includes, but is not limited to, controls for ensuring effective and safe implementation of IT systems and robust third-party service provider management to ensure the availability, integrity and confidentiality of data exchanged through open finance arrangements.

S 13.3 An FSP shall ensure that its cyber risk management capabilities and cybersecurity controls are also appropriately extended to govern, identify, prevent, detect, respond to and address cyber risks associated with open finance activities. This includes for the FSP to implement robust API security

controls, strengthen digital fraud detection and management, as well as take steps to secure its technology networks and internal systems from potential external risks arising from the FSP's participation in an open finance arrangement.

S 13.4 An FSP shall adhere to relevant regulatory notification and consultation processes applicable to its participation in an open finance arrangement, in line with expectations as set out in paragraphs 16 and 17 of the Policy Document on Risk Management in Technology, where relevant[28].

S 13.5 An FSP participating in an open finance arrangement shall also comply with technology and operational requirements of the open finance platform in which the FSP is a participant, provided that such requirements are consistent with this policy document, as well as applicable legal and regulatory requirements. These requirements may include, but are not limited to, requirements relating to user journeys, API specifications, uptime and service availability, and operational procedures of its technology functions.

The rest of the page is intentionally left blank

[28] Or such corresponding paragraphs in any amendment or replacement of such policy document.

PART C APPENDICES

Appendix 1 Definition of mandated FSP and scope of specified information

1. A mandated FSP[29] is an FSP that meets any of the following criteria:
   (a) a licensed bank, or a licensed Islamic bank, with an aggregate distinct count[30] of individual and SME active customers[31] larger than two hundred and fifty thousand (250,000), whether at an entity level or at the banking group level; or
   (b) a prescribed development financial institution, with an aggregate distinct count of individual and SME active customers larger than two hundred and fifty thousand (250,000); or
   (c) an eligible EMI operating a network-based e-money solution with an aggregate distinct count of active users larger than five million (5,000,000).

2. A scope of specified information refers to –
   (a) transaction information for the most recent twelve (12) months, including the date, time, amount, currency, description, debit or credit indicator and such other information as may be specified by BNM from time to time; and
   (b) the current outstanding balance of an account.

[29] For the avoidance of doubt, licensed investment banks and licensed insurers and takaful operators do not fall within the definition of "mandated FSP" under paragraph 5 of this policy document.

[30] Taking the maximum such distinct count in the last 12 months. For the avoidance of doubt, this shall apply whenever distinct count is referenced in this policy document.

[31] Where a customer maintains both an individual account and an SME account, the customer shall be counted as an individual customer and separately as an SME customer for the purpose of determining the distinct count of active customers.

Appendix 2 Transition arrangements

1. The obligations of a mandated FSP as a **data provider** as specified under paragraph 9.5 shall commence as follows:

Timeline for Commencement of Obligations	**Mandated FSP**
By 1 January 2028	A licensed bank, or a licensed Islamic bank, with an aggregate distinct count of individual and SME active customers larger than one million (1,000,000), whether at an entity level or at the banking group level.
By 1 January 2029	A licensed bank, or a licensed Islamic bank, with an aggregate distinct count of individual and SME active customers larger than two hundred and fifty thousand (250,000), whether at an entity level or at the banking group level. An eligible EMI operating a network-based e-money solution with an aggregate distinct count of active users larger than five million (5,000,000).
By 1 January 2030	A prescribed development financial institution, with an aggregate distinct count of individual and SME active customers larger than two hundred and fifty thousand (250,000).

2. The obligations of a mandated FSP as a **data consumer** as specified under paragraph 9.7 shall commence as follows:

Timeline for Commencement of Obligations	**Mandated FSP**
By 1 January 2029	A licensed bank, or a licensed Islamic bank, with an aggregate distinct count of individual and SME active customers larger than two hundred and fifty thousand (250,000), whether at an entity level or at the banking group level. An eligible EMI operating a network-based e-money

	solution with an aggregate distinct count of active users larger than five million (5,000,000).
By 1 January 2030	A prescribed development financial institution, with an aggregate distinct count of individual and SME active customers larger than two hundred and fifty thousand (250,000).

3. In relation to items 1 and 2, the threshold for a mandated FSP to commence its obligations is based on the maximum distinct count of active customers or users at any point within the twelve (12) months preceding the effective commencement date. For the avoidance of doubt, where an FSP exceeds the applicable customer count threshold at any point after the commencement date specified for that category of mandated FSP, the FSP shall comply with the corresponding obligations no later than twelve (12) months from the date on which it first meets the applicable threshold.

4. An FSP that is mandated as a data provider shall commence the sharing of the following types of information based on the following timeline:

Timeline	**Customer information mandated for sharing**
By 1 January 2028	For all mandated FSPs where obligations are in force, account and transaction information of deposit account[32], e-money account, charge card, and credit card, where relevant, for individual customers.
By 1 January 2030	For mandated FSPs with an aggregate distinct count of SME active customers or users larger than thirty thousand (30,000)[33], account and transaction information of deposit account, e-money account, charge card, and credit card, where relevant, for SME customers.

[32] This includes savings accounts, current accounts, fixed deposits, and Islamic deposit products.

[33] For the avoidance of doubt, other FSPs, mandated or otherwise, with an aggregate distinct count of SME customers lower than thirty thousand (30,000) may still participate in the sharing of SME information on a voluntary and reciprocal basis.