BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Open Finance
Exposure Draft

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: 18 November 2025 BNM/RH/ED 028-36

TABLE OF CONTENTS

This Exposure Draft (ED) sets out Bank Negara Malaysia's (BNM)'s proposed regulatory requirements for open finance, which will serve as a foundational framework to facilitate consent-driven sharing of customer information across the financial sector in a secure, open, accessible, interoperable, and timely manner.

BNM invites written feedback on the proposed regulatory requirements in this ED, including suggestions for specific issues, areas to be clarified or elaborated further and alternative proposals that BNM should consider. The written feedback should be constructive and be supported with clear rationales and appropriate evidence, examples or illustrations to facilitate BNM's assessment. Where appropriate, please specify the applicable paragraph.

Feedback must be submitted electronically to BNM by 1 March 2026 through this Microsoft Form link (https://forms.office.com/r/QeT0k0Nje7). Submissions received may be made public unless confidentiality is specifically requested for the whole or part of the submission.

In the course of preparing your feedback, you may direct your queries to the openfinance@bnm.gov.my and address them to the following officers:

(a) Anneka Ng (annekang@bnm.gov.my)
(b) Elysia Lim (elysia@bnm.gov.my)
(c) Joshua Chin (joshuacsk@bnm.gov.my)
(d) Kelly Lua (yunxin.lua@bnm.gov.my)

PART A OVERVIEW

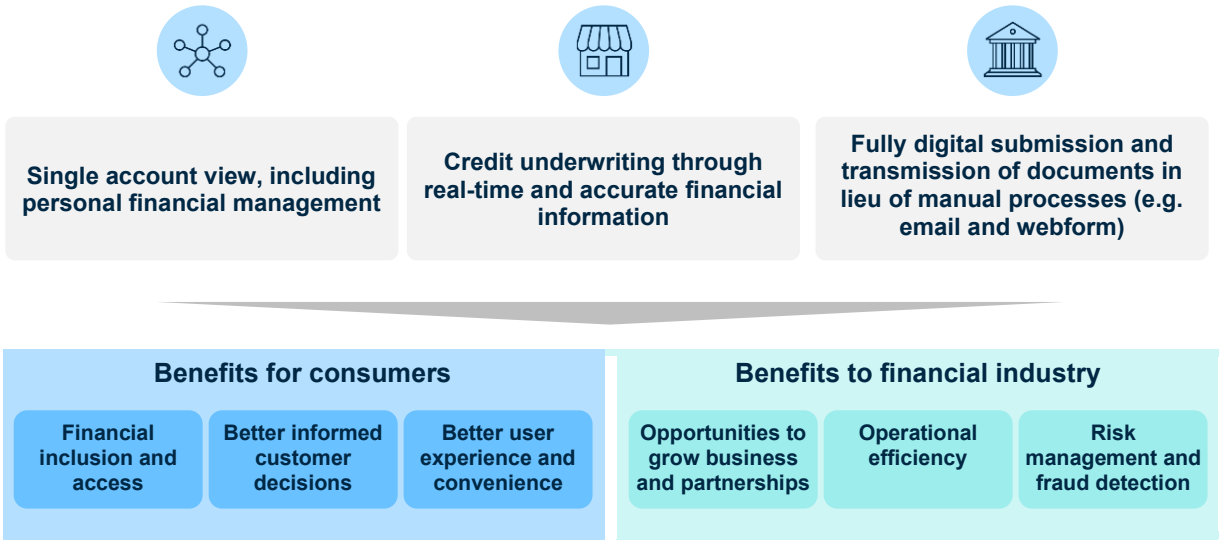
1 Introduction

1.1 As the financial sector continues to evolve in the digital age, the volume of customer information 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 provides 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 unlocks data-driven innovation that enables customers to make better-informed decisions about their finances, facilitates the delivery of more personalised financial services and promotes greater financial inclusion as illustrated in Diagram 1.

Diagram 1

Illustrative* potential use cases



*Use cases listed are for illustrative purposes only and are not exhaustive nor indicative of endorsement from 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. In addition to ensuring that the sharing of data is conducted in full compliance with the Personal Data Protection Act 2010 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 along with the customer information required for sharing;
(d) the management of consent throughout its lifecycle encompassing 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, BNM will gradually phase in the requirements in this Policy Document. This allows for 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 will 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 with 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.

Question 1
Beyond the use cases illustrated in Diagram 1, how do you envisage the sharing of customer information facilitated through open finance being leveraged to enhance access to financial services, improve affordability and drive inclusion outcomes for customers? Please provide examples of potential use cases, anticipated benefits and any preconditions necessary to enable such outcomes.

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 and 123 of the Financial Services Act 2013 (FSA);

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

(c) sections 41 and 42C 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 on 1 January 2027, subject to the transition arrangements set out in paragraph 9.

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;

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

"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;

"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, has used or may be intending to use[1] 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 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;

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

[1] 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.

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

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

"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;

"eligible EMI" refers to an e-money issuer as defined in the Policy Document on Electronic Money;

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

(a) a licensed bank;
(b) a licensed investment bank;
(c) a licensed Islamic bank;
(d) a licensed insurer;
(e) a licensed takaful operator;
(f) a prescribed development financial institution; and
(g) an eligible EMI;

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

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

"scope of prescribed information" refers to the scope of personal 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;

"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;

"senior management" refers to the chief executive officer and senior officers of an FSP;

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

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

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

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 reissuance thereafter, in particular –

(a) Guidelines on Data Management and MIS Framework issued on 29 August 2011;
(b) Guidelines on Data Management and MIS Framework for Development Financial Institutions issued on 5 November 2012;
(c) Policy Document on Risk Governance issued on 1 March 2013;
(d) Policy Document on Operational Risk issued on 10 May 2016;
(e) Notification on Measures to Combat Fraud Monetised via Internet Banking and Mobile Banking issued 31 May 2022;
(f) Notification on Specifications Relating to Measures to Combat Electronic Banking Fraud issued 23 Aug 2022;
(g) Policy Document on Business Continuity Management issued on 19 December 2022;

(h) Policy Document on Risk Management in Technology issued on 1 June 2023;
(i) Notification on Specifications on Fraud Detection Standards to Combat Electronic Banking Fraud issued 27 March 2024;
(j) Policy Document on Fair Treatment of Financial Consumers issued on 27 March 2024;
(k) Notification on Specifications on Countermeasures to Combat E-Money Fraud issued 8 April 2024;
(l) Policy Document on Product Transparency and Disclosure issued on 2 December 2024;
(m) Policy Document on Electronic Money (E-Money) issued on 31 January 2025;
(n) Policy Document on Complaints Handling issued on 28 March 2025;
(o) Policy Document on Management of Customer Information and Permitted Disclosures issued on 31 October 2025.

6.2 In implementing an arrangement relating to open finance, an FSP shall also comply with the Personal Data Protection Act 2010 (PDPA), including any amendments made to the PDPA, in particular, the Personal Data Protection (Amendment) Act 2024, and any legal instruments, standards or codes issued under such law.

The rest of the page is intentionally left as blank

PART B POLICY REQUIREMENTS

7 Governance

S 7.1 The board and senior management shall exercise effective oversight of an FSP's implementation of arrangements relating to open finance to ensure its efficient, resilient and secure operations.

S 7.2 For the avoidance of doubt, the board and senior management shall satisfy key responsibilities arising from an FSP's participation in an open finance arrangement, as may be applicable in relevant policy documents outlined in paragraph 6.1.

Responsibilities of the board

S 7.3 The board shall ensure that a sound risk strategy and appropriate risk management framework is in place and implemented effectively to manage any operational, technology, cyber, fraud, conduct or other risk arising from an FSP's participation in an open finance arrangement, in line with the FSP's risk appetite. This includes for the board to evaluate the risks and opportunities arising from the FSP's participation in an open finance arrangement, and consider how these factors should be reflected in its strategies and business plan.

S 7.4 The board shall also ensure that the framework is in line with relevant legal and regulatory requirements, which include those set out in paragraph 6, as well as any applicable operating rules and procedures specified by an open finance platform operator.

Responsibilities of the senior management

S 7.5 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 enables 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 7.6 In discharging its responsibility in relation to paragraph 7.5, 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 operational resilience 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, system downtime, API outages, cyber risk incidents or third-party failures;

(c) conduct due diligence and oversight to ensure only consented customer information is transferred from the FSP acting as a data provider, in accordance with requirements in paragraph 10 of this Policy Document;

(d) ensure the ethical 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 of customers 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 internal audit function and external assurance arrangements are extended to cover its open finance activities, including but not limited to coverage over its open finance-related services and API integrations; 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.

8 Participation and scope of information sharing

S 8.1 An FSP may participate[2] as a data provider or a data consumer on an open finance platform, subject to meeting relevant requirements in this Policy Document and that specified by the platform operator.

G 8.2 Where feasible, an FSP should endeavour to adopt open finance as the

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

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 multilateral basis, subject to existing legal and regulatory requirements.

S 8.3 Any sharing of customer information on an open finance platform by an FSP either as a data provider or data consumer shall be made in accordance with relevant rules, standards and operating procedures, as the case may be, of the open finance platform.

S 8.4 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 FSP shall make available the scope of prescribed information to the relevant data consumer, subject to the scope of consent granted by the customer, as outlined in paragraph 10.1.

G 8.5 Notwithstanding paragraph 8.4, where industry standards and technological solutions permit, and with explicit consent obtained from the customer, a data provider may facilitate the sharing of additional customer information data points beyond the scope of prescribed information on a voluntary basis.[3]

S 8.6 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 customers 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,[4] in lieu of traditional methods of submitting documents (e.g. manual upload, emailing documents), for relevant processes (e.g. customer onboarding, on-going due diligence); and

[3] For example, this includes the sharing of customer information from shared savings accounts.
[4] As specified by the platform operator.

(b) Single account view, where the mandated FSP offers, as part of its internet banking and mobile banking interfaces, the option for a customer to display relevant information from their accounts with other data providers through the platform.

G 8.7 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 individuals with basic digital literacy and persons with disabilities) who may face challenges with overly sophisticated interfaces.

Question 2
The proposed participation requirement specified in Appendix 1 is intended to secure a critical mass of participation from the outset and ensure meaningful value creation for customers and the financial industry. In your view, is the proposed threshold reasonable and proportionate? If not, what alternative threshold(s) or approach would you suggest and why?

Question 3
What are your views on the proposed interfaces that a mandated data consumer is required to develop and operate as specified in paragraph 8.6? Please highlight any design, implementation and operational considerations of such interfaces including any potential challenges.

Question 4
Does the scope of prescribed information as specified in Appendix 1 sufficiently support the development of open finance use cases? If not, what additional customer information should BNM require data providers to share?

9 Transition arrangements

S 9.1 The obligations of a mandated FSP as specified under paragraph 8.4 shall commence in accordance with the timeline specified in Appendix 2.

S 9.2 A mandated FSP shall commence its obligation under paragraph 8.6 to provide document submission and single account view interfaces by 1 January 2028 or

the date on which the FSP's obligations under paragraph 8.4 commence, whichever is later.

Question 5
For licensed banks and licensed Islamic banks, do you anticipate that your institution, whether at an entity level or at the banking group level, will fall within the thresholds for the commencement of obligations as a data provider and data consumer by 1 January 2027 and/or 1 January 2028 as specified in Appendix 2? If yes, please indicate whether at entity or banking group level.

Question 6
What are your views on the proposed implementation timeline and phased approach outlined in Appendix 2 of this Exposure Draft? What operational or technical challenges do you foresee in developing the required technical interfaces as both data provider and data consumer in meeting the proposed timeline?

If the proposed timeline and/or phasing is deemed unfeasible, BNM invites feedback on –

a) Potential challenges or constraints, including those related to technical and operational issues or customer readiness;
b) Other considerations that BNM should take into account in finalising the phasing of implementation; and
c) Recommendations to support timely institutional and customer readiness, including alternative timelines to facilitate a more inclusive and effective implementation.

Question 7
Should BNM consider additional criteria beyond the customer count threshold (e.g. compliance history, data breach management record, system readiness and other operational factors) when determining the mandated? If so, what specific criteria should be included?

Question 8
Should a mandated FSP be required to share credit data[5] immediately upon the commencement of its obligation to participate in open finance? BNM invites feedback on the benefits and potential concerns arising from such a requirement.

[5] Credit data refers to the account, transaction, and balance information of all loan/financing products for individual and SME customers, except credit card.

10 Consent management

A. Obtaining consent

S 10.1 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, consent shall be sought and obtained in the following manner:

(a) **Specific**[6] – 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) to whom the disclosure will be made;

(ii) the purpose of such disclosure; and

(iii) the information that will be disclosed;

(b) **Voluntary**[7] – 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.[8] 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

[6] 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.

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

[8] Where consent is sought as a condition for the provision of a financial product/service, the consent does not meet the requirement of "voluntary" since customers are unable to refuse giving their consent. For example, combining the request for consent to disclose customers' information to a data consumer under an open finance arrangement within a clause to inform customers that their information are collected for the provision of the product/service. In other words, the request for customers' consent must be a standalone clause/term.

single statement of consent, is prohibited;

(c) **Explicit and deliberate**[9] – A customer must explicitly opt in or deliberately agree[10] to the disclosure of their information to a data consumer through affirmative action. Hence, silence or 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[11] 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. 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 10.2 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 consent 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 10.3 In addition to the functionalities specified in paragraph 10.2, a data consumer shall ensure that its consent dashboard enables the customer to –

(a) renew consent at any time; and

(b) receive notifications of consent expiry.

[9] 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.

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

[11] A pre-ticked consent box in a product/service application form does not meet the requirement of "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.

S 10.4 An FSP shall ensure that the consent dashboard reflects the real-time status of consent and is updated immediately upon any renewal, revocation or expiration of consent.

C. Consent validity, expiry and renewal

S 10.5 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 10.6 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 10.7 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 months from the date it was granted, unless revoked earlier by the customer.

S 10.8 Upon the expiry of the consent period, 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 10.1.

S 10.9 The data consumer shall issue timely notifications to the customer on the upcoming expiry of consent, in accordance with paragraph 10.3, and where appropriate or relevant, notify the customer of the option to renew the consent.

S 10.10 Where consent is not renewed, the data consumer shall delete all customer information obtained under the expired consent, unless retention is permitted or required under applicable laws or regulatory requirements.

D. Consent revocation

S 10.11 Upon receipt of a customer's request to revoke consent under an open finance arrangement, the data consumer shall immediately cease any access to customer information that was previously authorised under the revoked consent. The data consumer shall also promptly notify the corresponding data provider of the consent revoked.

S 10.12 Upon receipt of a consent revocation notification, the data provider shall immediately cease any further disclosure of the customer's information to the data consumer and take all necessary measures to prevent any subsequent disclosures.

S 10.13 The data consumer shall, without undue delay, securely delete all customer information that was obtained under the withdrawn consent, unless retention is required under applicable laws or regulatory requirements.

S 10.14 The data consumer shall provide the customer with an electronic confirmation of the revocation of consent and the actions taken in response, including the cessation of data disclosure.

S 10.15 Where a customer's consent is revoked through a data provider's consent dashboard under an open finance arrangement, the data provider shall immediately cease any further disclosure of customer information to the affected data consumer and promptly notify the data consumer of the revocation without undue delay to ensure that the data consumer also ceases any further access of the customer's information.

S 10.16 The data provider shall notify the customer of any consent revocation processed through its systems, including relevant timestamps and affected data categories.

S 10.17 Any renewal of data sharing under an open finance arrangement shall be permitted only upon re-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 10.1.

E. Record-keeping and audit

S 10.18 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

minimum period of seven years.

S 10.19 In addition to paragraph 10.18, an FSP shall make available to customers relevant data access logs, including when and by whom their information was accessed.

S 10.20 An FSP shall properly document the consent records and management processes, while ensuring that they are readily accessible for review upon requested by BNM.

Question 9
What are your views on the need for FSPs to securely delete customer information once consent has expired or been revoked, taking into account that legal and regulatory obligations have already been considered? Beyond such obligations, what challenges, if any, would arise in implementing such a requirement? Please also share whether there are existing expectations within your organisation or financial group to do so, and if not, what current practices are in place for handling customer information when consent is revoked.

Question 10
For FSPs which are part of groups with operations in the European Union, what are the operational practices, governance arrangements and technical mechanisms adopted to comply with the right to erasure under the General Data Protection Regulation (GDPR) – including on conditions and exceptions?

11 Customer protection

A. Management of customer information

Data privacy and confidentiality

S 11.1 In line with paragraph 10.6 of the Policy Document on Management of Customer Information and Permitted Disclosures, an FSP shall establish and implement data governance and privacy policies and procedures to safeguard the confidentiality and integrity of customer information shared, transmitted, disclosed, stored and used through an open finance arrangement.

S 11.2 In addition to paragraph 11.1, the data governance and privacy policies and procedures shall at a minimum –

(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;
(c) include retention schedules that ensure customer information is not kept longer than necessary; and
(d) mandate secure disposal of customer information upon expiry of its use.

S 11.3 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 11.4 In line with paragraph 10.12 of the Policy Document on Management of Customer Information and Permitted Disclosures, 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 11.5 An FSP shall ensure that any transmission of customer information through an open finance arrangement is conducted through secure means, in line with relevant requirements set out in the Policy Document on Risk Management in Technology. Without limiting the generality of paragraph 11.4, a data provider shall authenticate the customer and authorise consent using a reliable and effective authentication procedure (e.g. multi-factor authentication) before granting a data consumer access to the customer's information.

S 11.6 An FSP that is a data consumer shall ensure that customer information received from another FSP 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 11.7 An FSP shall regularly monitor the effectiveness of these controls to ensure that they remain responsive to changing threats.

Third-party arrangements

S 11.8 An FSP that is a data consumer shall ensure that any third-party service provider involved in handling customer information, whether related to an open finance arrangement (including that associated with outsourcing or cloud computing arrangements), 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 and Information Technology, and the Policy Document on Outsourcing.

S 11.9 An FSP shall ensure that customer information is not shared with any third-party service provider without the customer's explicit consent, in line with the requirements stipulated in paragraph 10.1 of this Policy Document.

S 11.10 For the purposes of paragraph 11.8, an FSP shall ensure the obligation to safeguard customer 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.

Customer information breaches

S 11.11 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 on customer information breaches, and all other obligations as prescribed under the law (e.g. PDPA).

11.12 In relation to paragraph 11.11, 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 actions.

Handling disputes and complaints

Clear accountability and liability

S 11.13 An FSP shall ensure that the accountabilities and responsibilities in relation to

its participation in an open finance arrangement are clearly stipulated, and that such responsibilities include ensuring customers do not suffer loss or detriment as a result of weaknesses, failures or misconduct on the part of the FSP.

S 11.14 In relation to paragraph 11.13, 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.

Complaints handling and redress

S 11.15 In line with paragraph 8.1 of the Policy Document on Complaints Handling, an FSP shall formulate and implement effective and transparent complaints handling policies, procedures and processes for timely and fair handling of customer complaints arising from any open finance activities.

S 11.16 For purposes of paragraph 11.15, 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 11.17 Where a dispute involves more than one FSP, the parties shall collaborate to ensure a coordinated and timely resolution, in line with relevant complaints handling protocols as may be determined by the platform operator. Where there are no relevant protocols in place for dealing with disputes involving one or more FSP, the FSP that first receives the complaint shall lead the investigation and resolution process, unless the parties agree otherwise.

G 11.18 Where practicable, an FSP may endeavour to ensure 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.

Other business conduct requirements

S 11.19 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 include provisions related to electronic banking services; and

(b) ensuring that services associated with an open finance arrangement are rendered in a manner that ensure 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), including by implementing 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.

G 11.20 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.

Question 11

Do you foresee any gaps in the proposed liability provisions as specified in paragraphs 11.13 and 11.14? If so, please specify the nature of these gaps and how they may be addressed.

12 Management of technology risk

S 12.1 An FSP shall ensure that relevant technology requirements in the Policy Document on Risk Management in Technology and the Policy Document on Technology Requirement for Payment Services Regulatees are observed in

respect of its open finance activities.

S 12.2 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, robust third-party service provider management, and operational resilience measures to ensure the availability, integrity and confidentiality of data exchanged through open finance arrangements.

S 12.3 An FSP shall ensure that its cyber risk management capabilities and cybersecurity controls are also appropriately extended to govern, identify, prevent, detect, respond and address cyber risks associated with open finance activities. This includes for the FSP to implement robust API security controls, strengthening digital fraud detection and management, as well as take steps to secure technology networks and internal systems from potential external risks arising from the FSP's participation in an open finance arrangement.

S 12.4 An FSP shall adhere to relevant regulatory processes applicable to its participation in an open finance arrangement, in line with expectations as set out in Part C of the Policy Document on Risk Management in Technology, as may be applicable.

S 12.5 An FSP participating in an open finance arrangement shall also comply with technology and operational requirements of the open finance platform for which the FSP is a member. This may include, but is not limited to, requirements in relation to the user journey, API specifications, uptime requirements, operational procedures and requirements for independent review relating to the operational resilience of its technology functions.

PART C APPENDICES

Appendix 1 Definition of mandated FSP and scope of prescribed information

1. A mandated FSP is an FSP that meets any of the following criteria:
   (a) a licensed bank, or a licensed Islamic bank, with an aggregate distinct count[12] of individual and SME customers larger than one hundred thousand, whether at an entity level or at the banking group level; or
   (b) a prescribed development finance institution, with an aggregate distinct count of individual and SME customers larger than one hundred thousand; or
   (c) an eligible EMI operating a network-based e-money solution with an aggregate distinct count of active users[13] larger than five million.

2. A scope of prescribed information refers to –
   (a) transaction information for the most recent 12 months including the date, description, and value; and
   (b) the current outstanding balance of an account.

[12] Taking the maximum such distinct count in the last 12 months.
[13] As defined in the Policy Document on Electronic Money.

Appendix 2 Transition arrangements

1. The obligations of a mandated FSP as specified under paragraph 8.4 shall commence as follows:

Timeline for Commencement of Obligations	Mandated FSP
By 1 January 2027	A licensed bank, or a licensed Islamic bank, with an aggregate distinct count of individual customers larger than one million, whether at an entity level or at the banking group level.
By 1 January 2028	A licensed bank, or a licensed Islamic bank, with an aggregate distinct count of individual and SME customers larger than one hundred thousand, whether at an entity level or at the banking group level.
By 1 January 2029	A prescribed development finance institution, with an aggregate distinct count of individual and SME customers larger than one hundred thousand. An eligible EMI and operating a network-based e-money solution with an aggregate distinct count of active users larger than five million.

2. A mandated FSP shall commence the sharing of the following types of information based on the following timeline:

Timeline	Customer information mandated for sharing
By 1 January 2027	Account and transaction information of deposit account,[14] e-money account, charge card, and credit card, where relevant, for individual customers.
By 1 January 2028	Account and transaction information of deposit account, e-money account, charge card, and credit card, where relevant, for individual and SME customers.

3. For the avoidance of doubt, the scope of customer information mandated for

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

sharing by a mandated FSP whose obligation to commence as a data provider falls on or after 1 January 2028 shall include both individual and SME customers.