Policy Document on Management of Customer Information and Permitted Disclosures

Frequently Asked Questions

No.	Paragraph and requirement	Question	Answer
1	Interpretation - Para 5.2 "**customer information**" refers to any information relating to the affairs or, in particular, the account, of any particular customer of any FSP in whatever form including in the form of a record, book, register, correspondence, other document or material.	In the event a FSP is unable to ascertain the details of the lost documents/information and unable to identify the details of affected customer(s) in a data breach, would the incident still fall within the definition of "customer information", thus requiring investigation and reporting to the Bank?	Yes. Customer information covers any information relating to any customer in whatever form. In the event of a customer information breach, an investigation is required to assess the impact of the breach, including the type and sensitivity of customer information involved and the estimated number of customers affected, even if the FSP is unable to identify the details of the affected customers.
2	Interpretation - Para 5.2 **"**staff" refers to persons employed by a FSP, including temporary or contract staff, and officers on attachment from an affiliate. Access controls - Para 10.25 FSPs must ensure that the role profile for each type of job includes a description of the access rights to customer information if relevant, for staff to perform the job.	If customer information is disclosed to a staff not based on a "need-to-know basis", would such disclosure be deemed as a customer information breach?	A customer information breach could be caused by the negligence or deliberate act of a FSP's staff. Para 10.25 requires a FSP to ensure that the role profile for each type of function includes a description of the access rights to customer information. Hence, if customer information is disclosed to staff who do not require access to customer information for the performance of their functions, such incident must be treated as a customer information breach.
3	Control environment - Para 10.22 FSPs must restrict access to web-based communication websites and social media platforms, particularly those which are encrypted from end-to-end (e.g. WhatsApp Desktop,	Is the requirement applicable to outsourced service providers (OSPs)?	While the requirement is imposed on a FSP's staff, the FSP must ensure that its OSPs have adequate and effective controls that are comparable to that of the FSP to ensure that customer information is safeguarded at all

No.	Paragraph and requirement	Question	Answer
	Facebook and Skype Messenger) for staff who handle customer information, to prevent unauthorised disclosure of customer information to external parties via internet services.		times. The FSP is expected to include such restrictions in the Service Level Agreement with its OSPs to provide clear expectations to the OSPs on the control measures required to safeguard customer information.
4	Control environment - Para 10.23 FSPs must implement mechanisms for the prompt detection of - (a) unauthorised access to customer information; (b) …	What is the scope of 'unauthorised access to customer information' under Para 10.23(a)?	Unauthorised access to customer information occurs when a staff who is not given access rights to customer information gains access to such information, be it deliberately through his own action or inadvertently due to system lapses or other issues.
5	Control environment - Requirements from Para 10.41 to Para 10.52	Are the requirements under Para 10.41 to Para 10.52 applicable to a FSP's representatives, agents and external vendor's personnel?	It is the obligation of a FSP to ensure that its representatives, agents and service providers comply with the requirements under Para 10.41 to Para 10.52. In addition, the FSP must ensure that its external vendors regularly remind their staff (e.g. security guards, cleaners, maintenance officers) on the possible actions that will be taken in the event of customer information theft. The FSP is expected to include such requirements and reminders pertaining to safeguarding customer information in the Service Level Agreement with its external vendors.

6	Customer information breaches - Para 11.5 FSPs must take appropriate mitigating actions to contain a customer information breach immediately.	What is considered as a customer information breach?	A customer information breach occurs when there is theft, loss, misuse, unauthorised access, unauthorised modification or unauthorised disclosure of customer information. The breach can be due to both accidental and deliberate causes.
7	Customer information breaches - Para 11.8 FSPs must complete the investigation within three months upon detecting a customer information breach, having regard to the complexity of the breach. FSPs must submit a detailed investigation report and Appendix I to the Bank within one working day upon tabling to the Board.	Does the three-month period include tabling the investigation report to the Board?	The 3-month timeframe specified under Para 11.8 includes tabling the investigation report to the Board. If a FSP is unable to table to the Board within the 3-month timeframe, the FSP must notify BNM and provide a summary of the customer information breach. The FSP must submit a detailed investigation report to BNM within 1 working day upon tabling to the Board.
8		Does the timeline for investigation start when the breach is suspected or only when a breach is confirmed?	When a FSP has established a reason to believe that a customer information breach has occurred, the specified timeframe under Para 11.8 commences from the date such breach is suspected.
9		For cases where customer information breaches are caused by an external party without any contributory negligence by the FSP, is the FSP still required to submit an investigation report on such cases to BNM?	Yes, a FSP must report all customer information breaches to BNM even though the breaches are caused by external parties. The FSP must notify BNM immediately upon the detection of an information breach if the incident is likely to pose reputational risk to the FSP or cause a threat to public confidence, even if the breach is caused by an external party.

10		If a FSP's customer information was involved in a customer information breach that occurred at another FSP, is the FSP required to submit an investigation report to BNM?	No, it is the responsibility of the FSP in which the customer information breach occurred to take appropriate mitigating actions to contain the breach immediately, complete investigations within 3 months upon detecting such breach and submit a detailed investigation report to BNM within 1 working day upon tabling to the Board. Nevertheless, the FSP whose customers are impacted by this customer information breach incident should also notify BNM upon being informed by the other FSP of the breach.
11		Can a FSP consider tabling the customer information breach to its management committee instead of to the Board?	No, a FSP must table customer information breaches to the Board or a committee that is set up by the Board.
12	Customer information breaches - Para 11.9 Where the customer information breach is likely to pose reputational risk to FSPs or a threat to public confidence and trust, FSPs must notify the Bank immediately upon discovery of the breach.	For a customer information breach that involves the information of other FSPs' customers, which FSP is required to notify the Bank?	The FSP in which the customer information breach occurred must notify the Bank immediately upon discovery of the breach. The other FSPs whose customers are impacted must also notify the Bank upon being informed about the breach, if the incident is likely to pose reputational risk to the FSPs or cause a threat to public confidence.
13	Conditions in relation to permitted disclosure - Para 13.1: A financial institution, its directors and officers must comply with the conditions specified below in relation to permitted disclosures of any	Are the conditions on permitted disclosure under Para 13.1 applicable for all FSPs?	Para 13.1 is applicable to financial institutions (FIs) as defined under section 131 of the FSA, section 143 of the IFSA and section 3(1) of the DFIA. These FIs are: (a) a licensed bank; (b) a licensed Islamic bank;

	customer information as set out under Schedule 11 of the FSA and IFSA as well as Fourth Schedule of the DFIA.		(c) a licensed investment bank; (d) a licensed international Islamic bank; (e) a prescribed development financial institution; (f) an approved operator of a payment system; (g) a registered operator of a payment system; (h) an operator of a designated payment system; (i) an approved issuer of a designated payment instrument; and (j) an approved issuer of a designated Islamic payment instrument.
14	Para 13.1, item 1 Compliance with an order or request made by an enforcement agency in Malaysia under any written law for the purposes of an investigation or prosecution of an offence under any written law.	Is the disclosure of customer information to Jabatan Audit Negara permitted under the law?	The provision in section 7 of the Audit Act 1957 prevails over secrecy provisions in section 133 of the FSA, section 145 of the IFSA and section 119 of the DFIA. As such, a financial institution (FI) may disclose customer information to the Auditor General or an officer authorised by Auditor General in the course of performing its duties under the Audit Act.
15	Para 13.1, Item 1(b): The request must be made in writing using the application forms in Appendix II, III and IV, as applicable.	If a FI receives a request order from a law enforcement agency (LEA) via FINS 2.0, does the FI need to ask the LEA to complete the form in Appendix II, III or IV?	For requests received from a LEA via FINS, the FI is not required to request the LEA to resubmit its request using the forms in Appendix II, III or IV. For any other requests received from LEAs, the FI must ensure that the LEAs complete the relevant application form in Appendix II, III and IV.

16	Para 13.1, Item 5: Performance of any supervisory functions, exercise any of supervisory powers or discharge any of supervisory duties by a relevant authority outside Malaysia which exercises functions corresponding to those of the Bank under the FSA or IFSA.	If an overseas supervisory authority of a FI's parent company requests for customer information of the FI and such information already resides with the parent company, is the FI still required to notify BNM?	The FI must comply with all the conditions imposed under item 5 for the disclosure of customer information to an overseas supervisory authority. This includes notifying the relevant Pengarah of Jabatan Penyeliaan Konglomerat Kewangan or Jabatan Penyeliaan Perbankan, as required under subparagraph (d).
17	Para 13.1, Item 6: Conduct of centralised functions, which include internal audit, risk management, finance or information technology or any other centralised function within the financial group.	Does the disclosure of customer information to external auditors of the head office fall under the scope of conduct of centralised functions?	Centralised functions refer to functions established at the head office for the purposes of group oversight and this generally includes functions relating to group compliance, internal audit and risk management. External auditors of the head office do not fall under the permitted disclosure for the conduct of centralised functions.
18	Para 13.1, Item 8: Effective from 1 January 2024, a financial institution seeking a consent from the customer, executor, administrator or legal personal representative of the customer must comply with the following conditions: (a) Specific (b) Voluntary (c) Explicit and deliberate (d) Revocable upon request	Are the conditions under item 8 only applicable for the disclosure to third party for marketing purposes?	These conditions are applicable when a FI discloses its customer information to any third party based on the customers' consents. It is not confined to the disclosure of customer information to a third party for marketing purposes.
19		Can customer's consent still be considered as 'voluntary' if a FI is unable to provide the product or service without the customer's consent?	Consent is deemed as voluntary so long as the FI does not compel customers to give their consents for the disclosure of their information beyond what is necessary for the FI to provide the product or service to the customers.

20		If a FI enters into a data sharing arrangement with a third party for the purposes of fraud prevention, is the FI still required to meet all the conditions?	Where a FI has an obligation to share customer information with a third party for the purposes of fraud prevention or detection, the FI can disclose customer information by seeking the customers' consents. The four conditions can still be met by- a) Specific - clearly indicating to whom the disclosure will be made, the purpose of such disclosure and the information that will be disclosed; b) Voluntary - informing customers that the disclosure of their information is necessary for the provision of the product or service to the customers; c) Explicit and deliberate - allowing customers to provide their consents for the disclosure of their information to the third party; d) Revocation upon request - clearly informing customers that the withdrawal of their consents for the disclosure of their information will affect the provision of the product or service to the customers.
21		For product campaign or contest, a vendor is commonly involved to provide the gifts. Could customers' participation in the promotion be deemed as consent since the customers are aware that their information will be disclosed?	At the point when customers participate in a product campaign or contest, the FI must obtain the customers' consent to disclose their information to any third party. The FI must meet the conditions specified under subparagraphs (a) and (c) by-

			a) Specific - clearly indicating the type of customer information to be disclosed to the vendor and the purpose for such disclosure; c) Explicit and deliberate - allowing customers to provide their consents for the disclosure of their information to the vendor. A customer's signature alone in the product campaign or contest form does not satisfy the conditions for a valid consent as it does not involve a deliberate action of the customers to provide their consents.
22		For disclosure of customer information to third parties, do third parties include entities within a FI's financial group?	Yes, third parties include entities within a FI's financial group.
23		Are the conditions applicable in scenarios where the disclosure of customer information to a third party is already permissible under the law?	The conditions under item 8 are only relevant to the disclosure of customer information based on a customer's consent. These conditions do not apply to the disclosure of customer information which is already permitted under Schedule 11 of the FSA/IFSA and Schedule 4 of the DFIA.

24		Since the conditions under item 8 came into effect on 1 January 2024, does condition (d) apply to consents given by customers before the effective date?	Yes, condition (d) is applicable to consents obtained from customers prior to the effective date of 1 January 2024. A FI must allow existing customers to withdraw their consents given before the effective date, unless the withdrawal affects the ability of the FI to comply with any legal or contractual requirements.