



AMLC PRIMER NO. 1

Series of 2019

Frequently Asked Questions (FAQs)

**The Guidelines on Digitization of Customer Records (DIGICUR Guidelines),
Issued as AMLC Regulatory Issuance (ARI) A, B and C, No. 2, Series of 2018**

| Questions | Answers | | | | | | |
|--|---|----------------|--|---|-------------------|--------------|-----------------|
| I. IMPLEMENTATION | | | | | | | |
| 1. What are the relevant dates to remember about the DIGICUR Guidelines? | <table border="1"><tr><td>AMLC approval:</td><td>11 September 2018 Per AMLC Resolution No. 149, Series of 2018</td></tr><tr><td>Issuance as AMLC Regulatory Issuance (ARI) A, B and C, No. 2, Series of 2018:</td><td>11 September 2018</td></tr><tr><td>Effectivity:</td><td>13 October 2018</td></tr></table> | AMLC approval: | 11 September 2018 Per AMLC Resolution No. 149, Series of 2018 | Issuance as AMLC Regulatory Issuance (ARI) A, B and C, No. 2, Series of 2018: | 11 September 2018 | Effectivity: | 13 October 2018 |
| AMLC approval: | 11 September 2018 Per AMLC Resolution No. 149, Series of 2018 | | | | | | |
| Issuance as AMLC Regulatory Issuance (ARI) A, B and C, No. 2, Series of 2018: | 11 September 2018 | | | | | | |
| Effectivity: | 13 October 2018 | | | | | | |
| 2. Within what period should the covered person update its Money Laundering and Terrorist Financing Prevention Program (MLPP)? | The covered person must update its MLPP within six (6) months from effectivity of the DIGICUR Guidelines. Since the DIGICUR Guidelines took effect on 13 October 2018, the covered person must update its MLPP ¹ not later than 13 April 2019 (Section 6.a). | | | | | | |
| 3. After the covered person updates its MLPP, what step should it take next? | After its MLPP takes effect, the covered person must begin digitizing all customer records that it will receive, create or open. Thus, if the covered person's MLPP took effect on 1 March 2019, the covered person must, from that date, digitize the customer records of its new customers (Section 6.b). | | | | | | |
| 4. Within what period must the covered person complete digitization of customer records? | Within two (2) years after 13 April 2019, or until 13 April 2021, the covered person must completely digitize all existing | | | | | | |

¹ MTPP in the 2018 Implementing Rules and Regulations of the Anti-Money Laundering Act of 2001, as Amended.

| Questions | Answers |
|---|---|
| | customer records and establish the required central database (Section 6.b). |
| 5. If a covered person has already adopted a digital system for customer records even before the AMLC adopted the DIGICUR Guidelines, and stores these customer records in a central database, are there other requirements under these Guidelines that it must comply with? | If the covered person has already adopted a digital system for customer records even before the AMLC adopted the DIGICUR Guidelines, and stores these digital records in a central database, it should continue to follow its system. |
| 6. Do the DIGICUR Guidelines require covered persons to digitize the customer records of closed accounts? | <p>As a rule, the DIGICUR Guidelines require covered persons to digitize customer records of closed accounts if those records are within the five (5)-year retention period for record keeping under the AMLA (Section 3b).</p> <p>As an example, let us assume that Account No. 123 in Bank ABC was closed on 2 May 2015. Under the AMLA, Bank ABC must keep the records of Account 123 for five (5) years, or until 2 May 2020.</p> <p>If Bank ABC's MLPP took effect on 1 March 2019, Bank ABC should digitize the records of Account No. 123 because it falls within the five (5)-year record keeping period (2 May 2020). However, if the account was closed in May 2013, then it will not be required to digitize since the five (5)-year record keeping period has already expired.</p> <p>To clarify:</p> <p>The DIGICUR Guidelines must be fully implemented not later than 13 April 2021. Therefore, customer records of accounts closed on 13 April 2016 must still be digitized. Customer records of accounts closed on 12 April 2016 <i>need not</i> be digitized.</p> |
| II. SCOPE | |
| 7. Who are obliged to comply with the DIGICUR Guidelines? | <p>In general, all covered persons must comply with the DIGICUR Guidelines.</p> <p><i>However, the DIGICUR Guidelines do not apply to money service businesses (MSBs).</i></p> <p><i>But if the business model of the MSB is such that the customer</i></p> |

| Questions | Answers |
|--|--|
| | is able to open, keep and maintain an account as an electronic wallet or other similar electronic product or service, then that MSB must still observe the DIGICUR Guidelines (Section 3). |
| III. PURPOSE AND OBJECTIVES | |
| 8. Why did the Anti-Money Laundering Council (AMLC) approve the DIGICUR Guidelines? | <p>The AMLC approved the DIGICUR Guidelines to:</p> <ul style="list-style-type: none"> (a) Maintain the confidentiality of the financial investigations of the AMLC by preventing tipping off to customers under investigation; and (b) Ensure swift retrieval of customer records by covered persons. This in turn ensures promptness in the AMLC's financial analysis, investigations and legal actions (Section 1). |
| 9. Did the DIGICUR Guidelines replace, supersede or amend the record-keeping requirement under the Anti-Money Laundering Act of 2001, as amended (AMLA)? | No. The DIGICUR Guidelines did not replace, supersede or amend the record-keeping requirement under the AMLA. Covered persons must, therefore, continue to observe this record-keeping requirement under the AMLA and its implementing rules and regulations, which remain in force and effect. The AMLA and its implementing rules require covered persons to observe the five (5)-year retention period for all transactions and customer records (Section 7). |
| IV. DEFINITION | |
| 10. What are customer records? | <p>Under the DIGICUR Guidelines, <i>customer records</i> refers to:</p> <ul style="list-style-type: none"> (a) Customer Due Diligence (CDD) records/documents such as customer information files, copies of official identification documents or similar documents that establish the true and full identify of customers; account files and business correspondences; results of the covered person's analysis to establish the background and purpose of complex and large transactions; and (b) Account transaction histories or statements of accounts, whether in Philippine pesos or other currency (Section 2). |
| 11. Are deposit and withdrawal slips, fund transfer slips, checks, passbooks, and debit and credit memos included as customer records under the DIGICUR Guidelines? | No, because these documents are neither CDD records nor transaction histories or statements of accounts, the DIGICUR Guidelines do not require covered persons to digitize them. |

| Questions | Answers |
|---|---|
| | However, covered persons must still keep records of these documents as part of the record-keeping requirement (Section 2). |
| 12. Why must account files, business correspondences and analysis of the background and purpose of a customer's complex and large transactions required to be digitized? | These documents must be digitized because they form part of the CDD process for high-risk customers, whose true and full identities must be determined following enhanced due diligence (EDD) (Section 2). However, if these documents are not being required by the covered person or form part of the customer information file (e.g., analysis of the background and purpose of transactions), then digitizing the Customer Information Form (CIF) will suffice. |
| V. REQUIREMENTS | |
| 13. In general, what do the DIGICUR Guidelines require? | In general, the DIGICUR Guidelines require covered persons to digitize customer records and to establish a central database where these digitized records can be uploaded and retrieved (Section 3c). |
| 14. What does <i>digitizing</i> customer records entail? | Digitizing customer records entails rendering customer records in digital format that may be stored in the covered person's database, and retrieved, if the AMLC requires the covered person to submit the digitized customer records (Section 3b). |
| 15. Do the DIGICUR Guidelines require a specific digital format? | <p>No. The covered person is free to adopt its own digital format. However, digitized customer records must be in a form that may be used as evidence in court, and in such form as the AMLC may require (Section 3e).</p> <p>For example, Bank QRS may opt to digitize customer records from the very beginning, that is, when customer XYZ opens an account, and submits customer due diligence documents. Thus, XYZ's customer records, which would later include her statements of accounts, are already in digital form ("end to end"). These may be uploaded in Bank QRS's central database. If the AMLC requests for XYZ's customer records, Bank QRS would retrieve them from its central database and upload these digitized customer records to the AMLC portal.</p> <p>As another example, if Bank KLM requires customer DEF to fill out a customer information form (in paper), Bank KLM may later scan the filled-out and signed form and store this, along with the statements of accounts (whether scanned, in an Excel/MS word file, or other form) and store these in Bank KLM's central database. Bank KLM may later retrieve these</p> |

| Questions | Answers |
|---|--|
| | <p>records from its central database and upload them to the AMLC portal, upon request.</p> <p>Acceptable digital formats for scanned documents include pdf, jpeg, and bmp, to name a few.</p> |
| 16. In Section 3.e of the DIGICUR Guidelines, what does <i>admissible in court</i> mean? | <p>It means that the digitized customer records may be admitted (or used) as evidence in a court case. This is especially true where the customer records are electronic or digital from “end to end”, as discussed in Answer 15. If these are uploaded in the AMLC portal, and downloaded by the AMLC from there, the printed copies are deemed originals. In this case, the printed copies are considered electronic evidence that are admissible under the Rules on Electronic Evidence.</p> <p>If the digitized customer records are scanned copies of the original records in paper, the scanned copies cannot be used as evidence in court. To be admissible, copies of the originals must be obtained from the covered person. These copies must be authenticated and their due execution must be proven, as required under the Rules of Court.</p> |
| 17. In Section 3.e of the DIGICUR Guidelines, what does <i>in such other form as may be prescribed by the AMLC</i> mean? | <p>It means that the AMLC may recognize and require other forms of digitized customer records, particularly where new technologies create other digital formats that are acceptable under the DIGICUR Guidelines. The AMLC may also disallow certain digital formats that have become obsolete, easily tampered or unsecured, or can no longer be used as evidence in court.</p> |
| 18. To comply with the DIGICUR Guidelines, should covered persons print and scan transaction histories and statements of accounts that are already stored in their database? | <p>Since these transaction histories and statements of accounts are already in digital format in the covered person’s database, they need not be scanned. However, the compliance officer or any duly authorized officer who is independent from operations should be able to access and retrieve the same whenever the AMLC requests their production. (Section 3c).</p> |
| 19. Can covered persons keep the transaction histories and statements of accounts in MS Excel or MS Word format? | <p>Yes, provided that:</p> <ul style="list-style-type: none"> (a) those documents can no longer be edited by any user, or are otherwise locked for editing; (b) the compliance officer of the covered person must have direct and unimpeded access to those files; |

| Questions | Answers |
|--|--|
| | <p>(c) those documents must not be obtained from branches or other offices, and must be obtained only from the central database, if requested by the AMLC; and</p> <p>(d) confidentiality of the AMLC's investigation is otherwise observed, and tipping off is avoided (Section 3d).</p> |
| 20. Where should the digitized customer records be stored? | The digitized customer records must be stored in the covered person's central database. It should be maintained in the head office or the main branch of foreign banks operating in the Philippines (Section 3c). |
| 21. In what manner should the covered person submit customer records to the AMLC? | The covered person must ensure complete, accurate, timely and secure submission of requested customer records to the AMLC (Section 4b). |
| 22. What is the covered person's first task in implementing the DIGICUR Guidelines? | The covered person must first update its Money Laundering and Financing of Terrorism Prevention Program (MLPP) to ensure that its duties under the DIGICUR Guidelines are established and controls are in place (Section 3f). |
| 23. If the AMLC requests customer records, what should the covered person do? | <p>If the AMLC requests customer records, the covered person, through its compliance officer or any duly authorized officer or representative shall extract those digitized customer records from the central database and upload these to the AMLC's portal (or the File Transfer and Reporting Facility [FTRF]), using the covered person's log-on credentials.</p> <p>The compliance officer may also submit the requested customer records in such other modes that the AMLC may prescribe (Section 4a).</p> |
| VI. CENTRAL DATABASE | |
| 24. Does a <i>central database</i> mean that the covered person must have only one database system? | No. A <i>central database</i> under the DIGICUR Guidelines does not mean that the covered person must have only <i>one central database</i> . A covered person may have more than one database. The DIGICUR Guidelines only require that the <i>central database</i> must be maintained in the head office or the main branch of foreign banks operating in the Philippines (Section 3c). |
| 25. Who shall have access to the central database? | The compliance officer or any duly authorized officer or representative must have direct, immediate and unimpeded access to the database. This means that the compliance officer or the duly authorized officer need not have to request |

| Questions | Answers |
|---|---|
| | other persons, including branch personnel, to access the central database (Section 3c). |
| VII. PENALTIES AND SANCTIONS | |
| 26. What sanctions and penalties may be imposed on covered persons for non-compliance with the DIGICUR Guidelines? | Non-compliance with the DIGICUR Guidelines, a grave violation under the AMLC's list of administrative offenses, shall be subject to fines as provided under the AMLC's Rules of Procedure in Administrative Cases (RPAC) (Section 8, as amended by the RPAC). |

---Nothing follows---