

Data Transfer Agreement

Between Bank Mandara (Indonesia) and Common Bank (Australia)

This Data Transfer Agreement ("Agreement") is entered into by and between:

Bank Mandara, a financial institution incorporated in Indonesia, with its principal office at Jl. Gelong Baru Utara I No.4 Blok A, RT.1/RW.8, Tomang, Kec. Grogol petamburan, Kota Jakarta Barat, Daerah Khusus Ibukota Jakarta 11440, ("Data Exporter"),

and

Common Bank, a financial institution incorporated in Australia, with its principal office at 195 Swanston St, Melbourne VIC 3000, Australia, ("Data Importer").

Collectively referred to as the "Parties".

1. Purpose and Scope

1.1 This Agreement governs the transfer of specific personal data types from Bank Mandara in Indonesia to Common Bank in Australia in compliance with applicable data protection laws, including Indonesia's Personal Data Protection Law (UU PDP) and Australia's Privacy Act 1988 (as amended).

1.2 The purpose of this data transfer is to support joint venture operations between Bank Mandara and Common Bank in areas including, but not limited to, joint customer account management, regulatory compliance, risk assessment, and reporting.

2. Definitions

For the purposes of this Agreement:

- **Personal Data:**

- Under Australia's Privacy Act 1988 (APP): Personal data, or "personal information," is information or an opinion about an identified individual, or an individual who is reasonably identifiable, regardless of whether the information is true or recorded in material form.

- Under Indonesia's Personal Data Protection Law (UU PDP): Personal data, or "data pribadi," refers to data about an identified or identifiable individual, directly or indirectly, and can be divided into General Personal Data (e.g., name, gender) and Specific Personal Data (e.g., health data, financial data).

- **Data Subject:** An individual whose Personal Data is being transferred between the Parties.

- **Data Exporter:** The entity transferring personal data out of its jurisdiction (here, Bank Mandara).
- **Data Importer:** The entity receiving personal data from another jurisdiction (here, Common Bank).
- **Processing:** Any operation or set of operations performed on Personal Data, including collection, storage, use, disclosure, or deletion.
- **Consent:** Freely given, specific, informed, and unambiguous indication of a Data Subject's wishes by which they agree to the processing of their personal data.
- **Data Breach:** A security incident that results in unauthorized access, disclosure, alteration, or destruction of Personal Data.
- **Sensitive Information:** A subset of personal data requiring additional protections, including financial, health, biometric, or other data specified as sensitive by local regulations or the joint venture agreement.

4. Typical Categories of Personal Data Involved

In connection with the cross-border data transfer and joint operations between Bank Mandara and Common Bank, the typical categories of personal data involved include:

- **Identity and Contact Information:**
 - Full Name
 - Date of Birth
 - Identification Numbers (e.g., passport number, national ID, or Social Security Number)
 - Phone Number
 - Email Address
 - Address (residential or business)
- **Financial and Transactional Data:**
 - Bank Account Details (account numbers, account types)
 - Transaction History (including transaction dates, amounts, counterparties)
 - Loan or Credit Information (credit scores, loan details, repayment history)
 - Tax Identification Numbers (TINs) and tax status
 - Investment Portfolio Information (if applicable)
- **Employment and Income Data:**
 - Employment Status (current job position, employer name)
 - Income Details (annual income, salary slips)
 - Work History (job tenure, prior employers)

- Family and Dependent Information:
 - Family Certificates or Household Registration (to verify family relationships)
 - Details of Dependents (for insurance or credit considerations)
- Compliance-Related Data:
 - KYC (Know Your Customer) Information (source of funds, purpose of account, risk profile)
 - AML (Anti-Money Laundering) Checks (results of screenings against watchlists)
 - Sanctions and Politically Exposed Person (PEP) status (if applicable)
- Digital Identifiers and Authentication Data:
 - IP Addresses and location data
 - Device Information (used for authentication or access verification)
 - Login Credentials (such as usernames; typically, passwords are excluded due to security policies)
- Health Information:
 - Only when relevant for specific financial products, such as insurance.

Due to the sensitive nature of this data, the Parties shall implement strict security protocols and require specific consent from data subjects, ensuring compliance with Indonesian and Australian privacy laws.

5. Data Transfer and Processing

3.1 Bank Mandara (Data Exporter) shall transfer Personal Data to Common Bank (Data Importer) solely for the purposes specified in Section 1.2.

3.2 Common Bank shall process Personal Data strictly according to the instructions of Bank Mandara and solely for the purposes outlined in this Agreement.

3.3 The Data Importer agrees to implement appropriate technical and organizational measures to ensure the security and confidentiality of the Personal Data during transfer and processing, in accordance with applicable data protection laws.

6. Legal Basis for Transfer

4.1 The transfer of Personal Data is necessary for the performance of this Agreement and the management of joint banking activities. The Parties will ensure compliance with all requirements under Indonesia's and Australia's data protection laws for cross-border data transfers.

4.2 Bank Mandara has obtained necessary consents from Data Subjects or otherwise ensured a lawful basis for the cross-border transfer of Personal Data.

7. Data Subject Rights

5.1 Common Bank agrees to assist Bank Mandara in responding to Data Subject requests related to access, correction, deletion, or restriction of their Personal Data, as required by applicable laws.

5.2 Any Data Subject request received directly by Common Bank shall be forwarded to Bank Mandara within 5 business days.

8. Data Security and Breach Notification

6.1 Common Bank shall implement appropriate security measures to protect Personal Data from unauthorized access, use, disclosure, alteration, or destruction.

6.2 In the event of a data breach, Common Bank shall notify Bank Mandara within 24 hours and assist in any required notifications to regulators or affected Data Subjects.

9. Audit and Compliance

7.1 Common Bank agrees to permit Bank Mandara, or an appointed auditor, to conduct audits to verify compliance with this Agreement, provided such audits occur with reasonable notice and during normal business hours.

10. Liability and Indemnification

8.1 Each Party agrees to indemnify and hold harmless the other Party from any losses, claims, damages, or liabilities arising from its failure to comply with obligations under this Agreement.

11. Termination

9.1 This Agreement shall remain in effect as long as Personal Data is transferred or retained by Common Bank for the purposes outlined herein.

9.2 Upon termination of this Agreement, Common Bank shall return or securely destroy all Personal Data transferred under this Agreement, per applicable data protection laws.

12. Governing Law

10.1 This Agreement shall be governed by and construed in accordance with the laws of Australia.

IN WITNESS WHEREOF, the Parties have executed this Agreement on the dates indicated below:

[Signature of Bank Mandara Representative]

Date: 29 November 2022

[Signature of Common Bank Representative]

Date: 29 November 2022