GDPR SCHEDULE

This GDPR Schedule applies subject to clause 13.4 of the Terms and Conditions.

This GDPR Schedule forms part of the Terms and Conditions and shall be effective from the date ANZ opens an Account for, or provides an ANZ Service to, Correspondent pursuant to those Terms and Conditions.

The Terms and Conditions are amended, supplemented and varied as follows. Capitalized terms used in this GDPR Schedule and not otherwise defined have the meanings ascribed to them in the Terms and Conditions.

ANZ and the Correspondent hereby enter into the Applicable SCC and Module (as identified below). The Applicable SCC shall be deemed completed as set out in the following table.

SCC Reference	Details
Applicable SCC and Module *EU SCC* *UK SCC Part 1, Table 2* *Jersey SCC* *Guernsey SCC*	☑ Standard Contractual Clauses (Module 1) issued by the European Commission on 4 June 2021 ("**EU SCC**") ☑ UK International Data Transfer Addendum issued by the Information Commissioner's Office effective on and from 31 March 2022 ("**UK SCC**") ☑ Bailiwick of Jersey Addendum issued by the Jersey Data Protection Authority ("**Jersey SCC**") ☑ Bailiwick of Guernsey Addendum issued by the Office of the Data Protection Authority ("**Guernsey SCC**") together the "**SCC**"
Data exporter(s) name, address and commercial identifiers *EU SCC Annex I A* *UK SCC Part 1, Table 1 and Table 3* *Jersey SCC Clause 2*	See the AUD account opening request document.
Data exporter(s) contact person's name, position and contact details *EU SCC Annex I A* *UK SCC Part 1, Table 1* *Jersey SCC Clause 2*	See the AUD account opening request document.
Data exporter(s) role *EU SCC Annex I A*	Controller
Data exporter(s) activities relevant to the data transferred *EU SCC Annex I A*	The activities specified in the Terms and Conditions.

SCC Reference	Details
Data importer(s) name, address and commercial identifiers *EU SCC Annex I A* *UK SCC Part 1, Table 1 and Table 3* *Jersey SCC Clause 2*	Australia and New Zealand Banking Group Limited ABN 11 005 357 522, Level 9, 833 Collins St, Docklands VIC 3008, Australia (**ANZBGL**)
Data importer(s) contact person's name, position and contact details *EU SCC Annex I A* *UK SCC Part 1, Table 1* *Jersey SCC Clause 2*	Michelle Pinheiro CRO Data and Technology Australia and New Zealand Banking Group Limited Dataeventresponseteam@anz.com
Data importer(s) role *EU SCC Annex I A*	Controller
Data importer(s) activities relevant to the data transferred *EU SCC Annex I A*	The activities specified in the Terms and Conditions.
Categories of data subjects concerned *EU SCC Annex I B* *UK SCC Part 1, Table 3*	☑ Customers of the Correspondent ☑ Beneficiaries ☑ Representatives, advisors and other personnel □ Other, please specify:
Categories of personal data *EU SCC Annex I B* *UK SCC Part 1, Table 3*	☑ Personal data of the Beneficiaries, such as name, age, gender, date of birth, place of birth, nationality, marital status, private contact details, country of residence ☑ Business contact details of either party's staff, advisors or other personnel such as work address, work phone number, work email, company, job title and department ☑ Anti-money laundering, counter terrorism-financing, Sanctions risk and other regulatory checks data, including identification documents, employment data, such as employment history, financial information such as income, assets and investments, liabilities, credit history, benefits and pensions, grants or insurance details ☑ Correspondent data, including tax ID and tax residence ☑ Payment data, including SWIFT information such as Account details, Beneficiary Account details, Beneficiary Bank, Payment time and date and Payment amount □ Other personal data derived from or generated by pursuing the purposes (see below), please specify:

SCC Reference	Details
Sensitive data *EU SCC Annex I B* *UK SCC Part 1, Table 3*	□ Racial or ethnic origin □ Political opinions (if collected in connection with regulatory checks) □ Religious beliefs □ Philosophical beliefs □ Trade union membership □ Genetic data □ Biometric data (e.g. from ID documents) □ Health data □ Data revealing sex life or sexual orientation □ Criminal convictions and offences
Restrictions or safeguards applied to processing of sensitive data *EU SCC Annex I B*	See the Data Security Standards in Schedule 1.
Frequency of the transfer *EU SCC Annex I B* *UK SCC Part 1, Table 3*	☑ One-off transfer ☑ Continuous transfer □ Other, please specify
Nature of processing Purpose(s) of the transfer and further processing *EU SCC Annex I B* *UK SCC Part 1, Table 3*	☑ As set forth in the Terms and Conditions and this GDPR Schedule ☑ To comply with applicable Laws, codes of practice and external payment systems ☑ To tell the Correspondent about similar products and services ☑ Manage complaints and concerns by the Correspondent and data subjects against ANZ ☑ Identify, prevent or investigate any actual or suspected fraud, unlawful activity or misconduct ☑ Establish, defend and exercise legal claims against ANZ
Applicable retention periods *EU SCC Annex I B*	As long as necessary for the purposes (see above) or where required or permitted under applicable Laws.
For transfers to processors: subject matter, nature and duration of the processing *EU SCC Annex I B*	**ANZ'S PROCESSORS:** ANZ Operations and Technology Private Limited, Indian Company No. 08-010490, whose registered office is located at RMZ Ecoworld, Campus 5A, Ground Floor and Levels 4 to 9, Sarjapur-Marathahalli Outer Ring Road, Devarabeesanahalli Village, Varthur Hobli, Bengaluru East Taluk, Bengaluru, 560103 India (**ANZOT**) ANZ Support Services India Private Limited, Indian Company No. U72200KA2007PTC043986, whose registered office is located at "Eucalyptus", Manyata, Embassy Business Park - SEZ, Outer Ring Road, Nagavara & Rachenahalli Village, K R Puram Hobli, Bangalore 560045 India (**ANZSSI**) ANZ Global Services and Operations (Manila), Inc., Company Registration No. CS201004050, whose registered office is located at Level 11, Solaris One, Dela Rosa Street, Makati City, Philippines (**ANZGSOM**) ANZ Pacific Operations Pte Limited, Fiji Company No. 14503, whose registered office is located at Building 5, Kalabu Tax Free Zone, Valelvu, Suva, Fiji (**ANZPOL**)

SCC Reference	Details
	SUBJECT MATTER AND NATURE: The processors may process any personal data referred to in this GDPR Schedule to manage the Correspondent's banking activity including processing payments, opening accounts, conducting KYC, on-going due diligence and sanctions screening and regulatory reporting. **DURATION:** For as long as required to comply with data retention requirements in Australia or any other geography in which an ANZ Group Member operates or a Beneficiary holds an account.
Competent supervisory authority *EU SCC Annex I C*	☑ The supervisory authority of the Correspondent □ Federal Data Protection and Information Commissioner (Switzerland only) □ Isle of Man Information Commissioner (Isle of Man only) □ Other, please specify
Data importer's technical and organisational measures *EU SCC Annex II* *UK SCC Part 1, Table 3*	See Data Security Standards in Schedule 1.
Addendum EU SCC *UK SCC Part 1, Table 2*	The second option applies.
Docking option *EU SCC Clause 7* *UK SCC Part 1, Table 2*	☑ Shall apply □ Shall not apply
Redress option *EU SCC Clause 11a* *UK SCC Part 1, Table 2*	□ Shall apply ☑ Shall not apply
Personal data received by data importer combined with personal data collected by the data exporter *UK SCC Part 1, Table 2*	☑ Yes □ No
Supervision *EU SCC Clause 13a*	The first option applies. The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C (see above), shall act as competent supervisory authority.

SCC Reference	Details
Governing law *EU SCC Clause 17* *Guernsey SCC Clause 5.2.7*	☑ Option 2 applies. The EU SCC shall be governed by the law of the EU Member State in which the data exporter is established. □ Option 1 applies. The EU SCC shall be governed by the law of the following jurisdiction (Switzerland, Isle of Man and Guernsey only): □ Switzerland (Switzerland only) □ Isle of Man (Isle of Man only) □ Guernsey (Guernsey only) □ Alderney (Guernsey only) □ Sark (Guernsey only)
Choice of forum and jurisdiction *EU SCC Clause 18*	The competent courts shall be the courts of ☑ Hesse, Germany □ Switzerland (Switzerland only) □ Isle of Man (Isle of Man only)
Ending the UK SCC when the Approved UK SCC change *UK SCC Part 1, Table 4*	Data importer (ANZ) may end the UK SCC.
Additional EU SCC adjustments for Swiss and Isle of Man transfers *EU SCC*	□ Not applicable □ The following adjustments shall apply (Switzerland and Isle of Man only): (a) References to the "Union", "EU" and "EU Member State" are replaced by references to: □ Switzerland (Switzerland only) □ Isle of Man (Isle of Man only) (b) References to "Regulation (EU) 2016/679" and "General Data Protection Regulation", including to specific articles in that Regulation, are replaced by references to the (equivalent articles of and as amended and replaced): □ Federal Act on Data Protection (Switzerland only) □ Data Protection (Application Of GDPR) Order 2018 and the GDPR and LED Implementing Regulations 2018 (Isle of Man only)
Supplementary safeguards	**Limitation of purpose** ANZ shall process EEA, UK, Switzerland, Isle of Man, Bailiwick Jersey or Bailiwick of Guernsey personal data (**Relevant Personal Data**) strictly only for the purposes expressly agreed between the parties unless otherwise approved in writing by the Correspondent or required by or permitted under EEA, UK, Switzerland, Isle of Man, Bailiwick Jersey or Bailiwick of Guernsey Data Protection Laws (**Relevant Data Protection Laws**). **Data minimisation** The parties shall ensure that the scope of Relevant Personal Data transferred is limited to the absolute minimum required to achieve the legitimate purposes agreed between the parties. Dedicated specific user roles must be implemented for relevant ANZ staff who need to have access to Relevant Personal Data in all relevant systems or applications carrying Relevant Personal Data. Access rights assigned to such user roles must be limited to the absolute minimum required in performance of the individual's duties and responsibilities.

SCC Reference	Details
	Data subject rights ANZ shall comply with the obligations under Clause 10 of the EU SCC in relation to any requests by a EEA, UK. Switzerland, Isle of Man, Bailiwick Jersey or Bailiwick of Guernsey data subject (**Relevant Data Subject**), including, any requests of Relevant Data Subjects to exercise their rights under Relevant Data Protection Laws against ANZ. **Ad-hoc access notification** ANZ shall comply with the obligations under Clause 15.1 (a) of the EU SCC in relation to any legally binding requests by a public authority under the laws of Australia for disclosure of Relevant Personal Data. Notification must be made in accordance with Clause 15 of the EU SCC and shall, as a minimum, include information about the Relevant Personal Data requested, the requesting authority, the legal basis for the request and the response provided. ANZ acknowledges and agrees that, in the event of any such notifications, the Correspondent will consider the risks for the rights and freedoms of Relevant Data Subjects arising from the transfer of Relevant Personal Data to ANZ and, if appropriate, stop or restrict transfers of Relevant Personal Data or request further mitigating measures to protect Relevant Personal Data against unauthorized access. **Access reporting** ANZ shall comply with the obligations under Clause 15.1 (c) of the EU SCC in relation to regular reporting on requests by public authorities under the laws of Australia for disclosure of Relevant Personal Data. ANZ will submit an annual report to the Correspondent about any specific public access requests (including number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.) and any publicly available information related to the access practice of the public authorities in Australia. On the basis of this annual report, the Correspondent will consider the related risks for the rights and freedoms of Relevant Data Subjects arising from the transfer of Relevant Personal Data to ANZ and take further mitigating measures, if appropriate. ANZ will, in coordination with the Correspondent, will notify the competent data protection authority or any other data protection supervisory authority concerned of any risks identified, if appropriate or required under Relevant Data Protection Law. **Cooperation with supervisory authorities** ANZ shall comply with the obligations under Clause 13 (b) of the EU SCC in relation to submitting itself to the jurisdiction, cooperate and comply with any audit requests, orders, inquiries or other measures, including remedial and compensatory measures taken or issued by the competent supervisory authority concerning the processing of Relevant Personal Data. ANZ shall, to the extent permitted under Relevant Data Protection Laws, promptly notify the Correspondent of any related interaction with the supervisory authority. **Training** ANZ staff who have access to Relevant Personal Data are required to access a regular data protection training with a focus on risk mitigating measures: ANZ managers are trained on the following: • Applicable policies to mitigate risk for Relevant Personal Data; and • Applicable retention schedules for local copies of Relevant Personal Data.

SCHEDULE 1
DATA SECURITY STANDARDS

ANZ Technical and Organisational Measures for GDPR

1. PURPOSE

This document describes the Technical and Organisational Measures (TOMs) generally and variously implemented by Correspondent (during transmission to ANZ) and ANZ to appropriately protect personal data of European Union (EU) and United Kingdom (UK) data subjects, including in response to the EU's General Data Protection Regulation (Regulation 2016/679) and the UK General Data Protection Regulation (including as tailored by the UK Data Protection Act) (collectively the GDPR), including subsequent changes to the GDPR and any new data protection and privacy regulations within EU and UK.

ANZ reserves the right to modify or revise these TOMs at any time at its discretion without notice, provided that such modification or revision does not result in a material degradation in the protection provided for personal data that ANZ processes in providing its various services.

2. DATA SECURITY

2.1 Secure transfer of personal data

In accordance with the Terms and Conditions, communications between Correspondent and ANZ in relation to Payments and Instructions (as those terms are defined in the Terms and Conditions) shall be sent as a SWIFT Message. Messages sent and received under SWIFT are encrypted end to end.

2.2 Security Organisation and Programme

ANZ has a Security Domain team that is led by ANZ's Chief Information Security Officer, and has dedicated staff responsible for the development, implementation, and maintenance of ANZ's data security program.

All ANZ employees and individual contractors, consultants, and other personnel of ANZ (together, contingent workers) are bound by ANZ's internal policies regarding maintaining the confidentiality of personal data.

2.3 Configuration Management

ANZ data systems are configured and hardened in compliance with configuration management standards that reflect industry and platform supplier recommended practices.

ANZ end-point computing is protected by hard disk encryption, malware software, firewall software, remote administration, security patching and screen lock timeout.

2.4 Cryptography

ANZ uses cryptographic methods to protect data based on its confidentiality and integrity classification in storage and in transit.

2.5 Data Security Education

ANZ educates its employees and contingent workers on their accountabilities, responsibilities, and appropriate data security practices.

2.6 Data Handling

ANZ has mechanisms for securing data traffic and communication, including firewalls, intrusion detection and prevention systems (IDS / IPS), Virtual Private Networks (VPNs) and Data Loss Prevention (DLP) capabilities.

ANZ configures platforms to prevent unauthorised transfer of data to portable storage media.

ANZ protects data on portable storage media, including workstations, using encryption, access control and physical security as appropriate.

ANZ disposes of data securely.

2.7 Identity and Access Management

ANZ protects data from unauthorised access.

ANZ establishes the identity of users prior to providing access to data.

ANZ provides access to data only when justified by a business need, and periodically reviews access and removes access when no longer needed.

ANZ authenticates users before granting access to data systems.

ANZ maintains appropriate segregation of duties so that users are not in a position to perpetrate and conceal unauthorised activities in the normal course of their roles.

2.8 Data Classification

ANZ classifies all data for confidentiality and integrity. These classifications are taken into consideration when designing and applying data security controls.

2.9 Incident Management

ANZ monitors and manages data security events and incidents.

ANZ records and responds to security incidents in a timely manner to prevent further damage, restore business services, recover to business-as-usual and prevent recurring incidents.

2.10 Networking Security

ANZ protects networks and communications from unauthorised access, fraudulent insertion of data, malicious code and denial of service.

ANZ places data systems in appropriate network segments and controls the flow of data across network boundaries.

2.11 Security Patch Management

ANZ identifies, assesses, prioritises, and tests security patches for data systems.

ANZ deploys and activates security patches or compensating controls according to data system and patch importance, within acceptable timeframes.

2.12 Policy & Standards Management

ANZ has an enterprise-wide Information Security Policy and supporting global and country standards for meeting ANZ and regulatory requirements.

2.13 System Vulnerability Identification

ANZ scans and tests data systems to check that security controls have been effectively designed and are effective in operation, and report vulnerabilities for remediation.

ANZ security measures include vulnerability scanning; periodic penetration testing; patch management; anti-virus and anti-malware software; and threat notification advisories.

2.14 Third Party Security

ANZ does not allow third parties to access ANZ non-public data until their security posture is assessed by ANZ and the business risk resulting from the data security exposure is accepted.

ANZ enters into written agreements with its suppliers, which include confidentiality, privacy, and security obligations that provide an appropriate level of protection for personal data that these suppliers may process, and which are designed to comply with the GDPR where applicable.

3. DATA MANAGEMENT

3.1 Data Quality

ANZ manages data quality throughout the data lifecycle, using ANZ data quality dimensions.

ANZ have controls to maintain and measure the quality of data.

ANZ de-duplicates and masters critical identification data elements to create a comprehensive single customer view.

4. RECORDS MANAGEMENT

4.1 Records Retention, Retrieval & Disposal

ANZ will manage records including retaining records, having capability to retrieve records, and to dispose of records in accordance with applicable legal obligations and regulatory requirements, including the GDPR.

5. PRIVACY

ANZ maintains policies and procedures to manage and protect personal data collected or handled during its business activities. Further information can be found on the ANZ website, at https://www.anz.com.au/privacy/centre/.

ANZ anonymises data it processes where feasible.

5.1 ANZ's Data Protection Officer maintains oversight of the Group's privacy compliance.

5.2 Data Breach Management

ANZ has processes in place to manage data breach incidents including reporting any reportable breaches to the relevant regulatory bodies.

6. PHYSICAL SECURITY

ANZ provides a secure environment protecting people, property, and operations.

ANZ facilities are separated into access zones that restrict unauthorised access and include data security and data protection requirements.

Access to ANZ data centres is controlled and segregated based on employee responsibilities and are subject to additional approvals and audits.

7. TECHNOLOGY

7.1 Backup and Recovery

ANZ data systems are subject to a comprehensive Data Backup & Recovery standard and associated processes including data recovery testing to ensure ongoing availability and access to such data.

7.2 Incident Management

ANZ maintains a Security Operations Centre that provides monitoring of ANZ managed environments to identify and respond to cyber security incidents related to malicious activity.

8. TESTING AND ASSESSING TOMS

Effective implementation of the data security programme is driven by a framework of policies and standards and is overseen by ANZ's risk and internal audit functions.

ANZ reviews various aspects of the TOMs from time to time to ensure they remain appropriate and to address any shortcomings in either their implementation or their success in protecting personal data.

anz.com

Australia and New Zealand Banking Group Limited (ANZ) ABN 11 005 357 522. Item No. 98 739 05.2024 WZ140806