Abridged Data Protection Annex

1. The Contract

1.01 This Data Protection Annex is incorporated into, forms part of, and is subject to the terms and conditions of the Contract.

1.02 Any capitalized term used but not defined in this Data Protection Annex has the meaning given to it in the Contract.

2. Confidentiality and Compliance with Applicable Law

2.01 Purchaser Data comprises Purchaser's confidential information and is subject to all protections and obligations applicable to Purchaser's confidential information under the Contract.

2.02 Vendor will comply with all applicable data privacy, data security, artificial intelligence, and other data protection related laws, regulations, or directives in connection with the performance of its obligations under the Contract.

3. Custodian of Purchaser Data and Use of Purchaser Data

3.01 Vendor is a custodian only of Purchaser Data and accordingly:

(a) the Contract does not create any right or license for Vendor or any third parties to use any Purchaser Data for their own benefit or for the benefit of any person or entity other than Purchaser,

(b) as between Purchaser and Vendor, Purchaser is the sole and exclusive owner of, and will retain all right, title, and interest in and to any Purchaser Data,

(c) regardless of the medium or form in which Purchaser Data is stored Vendor will not acquire or assert any right in, title to, or encumbrance over, any Purchaser Data for any reason,

(d) Vendor will not, under any circumstances, sell, assign, lease, license, securitize, otherwise commercially exploit any Purchaser Data,

(e) Vendor will not directly or indirectly disclose, transmit, comingle, or otherwise provide access to Purchaser Data to any person or entity other than Authorized Personnel without Purchaser's prior written consent in each and every instance,

(f) Vendor will only Process, or permit Processing of, Purchaser Data solely and exclusively for the Permitted Purpose and only for so long as is required to fulfill the Permitted Purpose and not for any other Purpose,

(g) Vendor will not Process, or permit Processing of, Purchaser Data for training, fine-tuning, or otherwise improving artificial intelligence or machine learning models, and

(h) Purchaser has the right to retrieve or delete, or require the retrieval or deletion of, any Purchaser Data at any time and Vendor will promptly comply, and cause any Subprocessors to comply, with a Purchaser request for retrieval or deletion of any Purchaser Data.

3.02 Vendor will not, unless expressly authorized to do so under the Contract: (a) track, store, analyze, distribute, disclose, sell, license, or otherwise transfer to any third party any user data (e.g., internet browser type, version, system specifications, access logs, IP address, MAC address) relating to Purchaser or captured by Vendor in the course of performing its obligations under the Contract and (b) target advertisements, promotions, offers, or other marketing based on user data relating to Purchaser or captured by Vendor in the course of performing its obligations under the Contract.

4. Archival and Other Immunities

4.01 Vendor agrees that Purchaser Data:

(a) are official archives of the relevant member of the World Bank Group, used to perform its core function,

(b) constitute the “archives” and “property” of the relevant member of the World Bank Group pursuant to applicable treaties and under applicable international and domestic laws, and

(c) are inviolable and subject to absolute and full immunity from legal and judicial process, search, seizure, confiscation, attachment, and discovery by others as set forth in such treaties and laws.

4.02 Vendor will take such actions as are requested by Purchaser from time to time to protect the World Bank Group’s archives and to preserve the World Bank Group’s privileges and immunities.

4.03 Vendor agrees that none of:

(a) Purchaser’s execution or performance of the Contract,

(b) Purchaser providing any Purchaser Data to Vendor or any third parties in connection with the Contract, or

(c) Purchaser requiring Vendor or any of its representatives to perform any obligations under the Contract,

will be construed as any member of the World Bank Group waiving, renouncing, modifying, or intending to waive, renounce, or modify, to any extent or in any manner whatsoever, any privileges or immunities under any treaty, international law, or domestics law, which privileges and immunities are specifically reserved.

5. Third Party Data Requests

5.01 In the event of a Third Party Data Request, Vendor will, unless expressly prohibited by law:

(a) immediately notify Purchaser of the existence of the Third Party Data Request,

(b) use its best efforts to redirect the third party to Purchaser,

(c) refrain from disclosing or providing access to any Purchaser Data in response to the Third Party Data Request without first obtaining Purchaser’s prior and express written consent,

(d) provide Purchaser with sole and exclusive control over any response to the Third Party Data Request, including without limitation the sole and exclusive right to initiate or respond to any legal proceedings, in so far it affects any Purchaser Data, and

(e) take such actions as are reasonably requested by Purchaser to help protect Purchaser Data, including without limitation by initiating or responding to legal proceedings, at Purchaser’s request.

5.02 If, notwithstanding the above, Vendor remains compelled by applicable law to disclose or provide the third party with access to any Purchaser Data, Vendor will only disclose that portion of the Purchaser Data that is strictly required to discharge its obligations under applicable law and will use best efforts to ensure that the Purchaser Data is afforded appropriate protection.

6. Data Security Safeguards

6.01 Vendor will implement and, at all times maintain, administrative, physical, technical, and organizational safeguards appropriate to the risk represented by the nature of the Purchaser Data and the Processing of Purchaser Data permitted under the Contract.

6.02 In addition, Vendor will, at a minimum:

(a) encrypt all Purchaser Data at rest, including any backup, and in transit (using TLS 1.2 or later),

(b) treat any and all information relating to Purchaser's remote access and transmission protocols as Purchaser's confidential information in accordance with the Contract,

(c) take all necessary steps to maintain the integrity of Purchaser Data and to protect it against deterioration and degradation of its quality and authenticity, and

(d) ensure that its employees attend regular cybersecurity trainings.

6.03 Vendor will make periodic backup copies of Purchaser Data and store such backup copies in an immutable, encrypted, machine-readable, and widely portable format for a minimum period of ninety (90) days.

6.04 Vendor will adhere to role-based access control determined by the need to know and the principle of least privilege.

7. Data Protection Audit and Inquiries

7.01 Purchaser, or an independent auditor appointed by Purchaser, has the right to audit Vendor, and any Subprocessors, to verify compliance with the obligations under this Data Protection Annex once per year, or at any time after a Data Incident, upon prior written notice.

7.02 Vendor will take all reasonable steps to, and will cause all Subprocessors to, cooperate with any such audit, including without limitation, by making available any relevant records, policies, systems, or facilities, and granting access to any premises or personnel, involved in, or used for the performance of any data-related obligations under the Contract.

7.03 Vendor will, at Purchaser's request, provide timely and complete: (a) responses to Purchaser's cybersecurity inquiries related to procedural and technical controls that Vendor has implemented to protect against emerging and current cybersecurity threats, including ransomware attacks and software supply chain vulnerabilities, and (b) details on the actions that Vendor has taken or plans to take in order to remediate specified vulnerabilities.

8. Geographic Location of Purchaser Data

8.01 At Purchaser's request, Vendor will and will cause any Subprocessor to provide Purchaser with prior written notice of the location of any facilities that will be used to store Purchaser Data.

9. Data Incident

9.01 If Vendor becomes aware of a Data Incident, Vendor will:

(a) immediately, but in any event within 24 hours, notify Purchaser,

(b) take all necessary steps to investigate, contain, and mitigate the Data Incident and to restore normal functionality,

(c) cooperate with Purchaser's requests for information and assistance, including without limitation, by providing Purchaser with periodic written updates regarding the Data Incident and Vendor's response to the Data Incident,

(d) at Purchaser's request, prepare and send any notifications required under applicable law arising from the Data Incident,

(e) at Purchaser's request, cooperate with Purchaser with respect to any action by any regulatory body or any lawsuit arising from the Data Incident, and

(f) as soon as reasonably practicable, review Vendor's response to the Data Incident to identify and address any vulnerabilities, weaknesses, or failures in Vendor's response processes and report all planned and completed remediations to Purchaser.

9.02 Vendor acknowledges that a Data Incident may cause irreparable harm to Purchaser, other members of the World Bank Group, and third parties, for which monetary damages may be an inadequate remedy.

10. Return or Destruction of Purchaser Data

10.01 Upon termination or expiration of the Contract, Vendor will at Purchaser's request: (a) return Purchaser Data to Purchaser by transmitting Purchaser Data in a widely supported, commonly used, and machine-readable format, and in a secure and encrypted manner, and/or (b) delete or destroy Purchaser Data by rendering Purchaser Data permanently unusable, unreadable, or indecipherable using industry standard measures.

10.02 If Purchaser does not request the return and/or deletion of Purchaser Data under Section 10.01 within one (1) year of termination or expiration of the Contract, Vendor will immediately delete or destroy Purchaser Data in accordance with Section 10.01(b).

10.03 Vendor will, at Purchaser's request, provide Purchaser with written certification from a duly authorized officer attesting to Vendor's compliance with Sections 10.01 and 10.02, the date of the return, destruction or deletion of Purchaser Data, and the methods used for such destruction or deletion.

10.04 Notwithstanding the above, Vendor may retain Purchaser Data to the extent necessary for Vendor to comply with applicable law or Vendor's own mandatory record keeping policies, provided that, in each case, Vendor: (a) only retains Purchaser Data for the minimum period necessary to satisfy any such obligations, (b) notifies Purchaser of the duration of the retention period in writing, and (c) remains bound by all obligations in the Contract with respect to the retained Purchaser Data.

11. Personal Data

11.01 To the extent that Vendor Processes Personal Data in the course of performing the Contract, Vendor will:

(a) only Process Personal Data in accordance with applicable law and in accordance with any other written instructions given by Purchaser,

(b) to the extent that the Permitted Purpose requires Vendor to collect, extract, or receive Personal Data from a Data Subject, take commercially reasonable steps to: (i) notify the Data Subject and obtain consent, or ensure there is another legal basis, to Process such Personal Data, and (ii) ensure that any such Personal Data is accurate and complete,

(c) maintain a log documenting Vendor's Processing of the Personal Data for the Permitted Purpose, including without limitation, any disclosure to, transmission to, or accessing of the Personal Data by Authorized Personnel,

(d) at Purchaser's request, provide any assistance reasonably required for Purchaser to rectify any inaccurate Personal Data, update any Personal Data that is out of date, or delete any Personal Data,

(e) ensure its employees attend regular, appropriate privacy trainings, and

(f) indemnify and hold harmless Purchaser from any and all liabilities arising out of or in connection with any Data Incident affecting Personal Data.

12. Subprocessing

12.01 To the extent that Vendor engages Subprocessors, Vendor will only engage the Subprocessors included in Attachment 1 to this Data Protection Annex and will make information about such Subprocessors, including their function and location, available to Purchaser.

12.02 If Vendor subsequently engages a new Subprocessor or changes the function of an existing Subprocessor ("Subprocessor Change"), Vendor will inform Purchaser at least ninety (90) days in advance, unless the Subprocessor Change is made to address an imminent or existing risk, in which case Vendor will inform Purchaser as soon as reasonably possible. If Purchaser reasonably determines that a Subprocessor Change would materially increase Purchaser's risk, Purchaser may notify Vendor and request that Vendor replace the Subprocessor with a Subprocessor

reasonably acceptable to Purchaser; if Vendor does not take such action, Purchaser may terminate the Contract.

12.03 Vendor will ensure that any authorized Subprocessors are bound by data protection obligations that are substantially equivalent to, or more onerous than, the obligations set out in the Contract.

12.04 Vendor will remain responsible and liable to Purchaser for all acts and omissions of any Subprocessors in connection with the Contract and will ensure that any Subprocessors comply with all terms and conditions of the Contract.

13. AI Technology

13.01 To the extent Vendor uses AI Technology in the course of performing the Contract, Vendor will:

(a) use its best efforts to ensure that the AI Technology and its outputs: (i) are not deceptive, misleading, or inaccurate, (ii) are free of bias and discrimination, and (iii) comply with industry standards,

(b) periodically test the AI Technology for compliance with any applicable laws, regulations, and industry standards (e.g., ISO 42001) and, at Purchaser's request and to the extent available, promptly provide Purchaser with copies of any current certifications demonstrating Vendor's compliance,

(c) clearly distinguish any of the AI Technology's generative outputs from human-created content, e.g., via disclaimers or labelling, and

(d) at Purchaser's request promptly provide to Purchaser: (i) to the extent available, any current model cards or equivalent information for the AI Technology, and (ii) explanations of the AI Technology's outputs, as well as replies to Purchaser's reasonable questions regarding such explanations.

14. Definitions

14.01 For the purposes of this Data Protection Annex:

(a) "AI Technology" means any machine learning, deep learning, large language models, neural networks, or other artificial intelligence methods.

(b) "Authorized Personnel" means only those of Vendor's employees, agents, advisors, or Subprocessors who have a need to know, or to Process, Purchaser Data for the Permitted Purpose.

(c) "Contract" means any agreement or purchase order between Purchaser and Vendor that references, attaches, or otherwise incorporates this Data Protection Annex, together with the terms of this Data Protection Annex, and any other Purchaser documents referenced in, or otherwise incorporated into, the agreement or purchase order.

(d) "Data Incident" means any actual or reasonably suspected unauthorized or unlawful: (i) use, modification, alteration, disclosure, transfer, interception, corruption, destruction, deletion, loss, or other Processing of, or access to, Purchaser Data, or (ii) access to, or damage, attack, corruption, or loss of any systems or devices that are used to access, host, maintain, transfer, or otherwise Process any Purchaser Data.

(e) "Data Subject" means a natural living person whose Personal Data is Processed.

(f) "Permitted Purpose" means the Processing of Purchaser Data solely and exclusively to the extent necessary for Vendor to perform its obligations under the Contract.

(g) "Personal Data" means any information relating to an identified or identifiable individual. An identifiable individual is one who can be identified by reasonable means, directly or indirectly, by reference to an attribute or combination of attributes within the data or combination of the data with other available information. Attributes that can be used to identify an identifiable individual include, but are not limited to, name, identification number, location data, online

identifier, metadata, and factors specific to the physiological, genetic, mental, economic, cultural, or social identity of an individual.

(h) “Process” means any operation or set of operations that is performed on information or data, or on sets of information or data, whether or not by automated means, such as accessing, capturing, collecting, extracting, recording, organizing, structuring, storing, adapting, retrieving, intercepting, using, disclosing by transmission, dissemination, hosting, transmitting, or otherwise making available, modifying, aligning or combining, restricting, erasing, deleting, or destroying.

(i) “Purchaser” means the relevant member of the World Bank Group described as the “Purchaser” in the Contract.

(j) “Purchaser Data” means any and all information or data, regardless of its form, that: (i) is provided by or on behalf of any member of the World Bank Group or any of its clients to Vendor or any of its representatives in connection with the Contract, (ii) is accessed by Vendor or any of its representatives via World Bank Group systems, (iii) is generated by Vendor or any of its representatives for or on behalf of any member of the World Bank Group or any of its clients, including through the use of AI Technology, in connection with the Contract, or (iv) comprises Personal Data Processed at the request, or on behalf, of the World Bank Group in connection with the Contract.

(k) “Subprocessor” means any person or entity to which Vendor (or its Subprocessor) has provided Purchaser Data or who otherwise Processes Purchaser Data on behalf of Vendor.

(l) "Third Party Data Request” means any actual or threatened request or demand by any person or entity for access to, or the production or disclosure of, any Purchaser Data, including without limitation, pursuant to any applicable law, regulation, or other form of legal process or procedure.

(m) “Vendor” means the entity or individual described as “Vendor” or “Contractor” in the Contract.

(n) “World Bank Group” means the International Bank for Reconstruction and Development, the International Finance Corporation, the International Development Association, the Multilateral Investment Guarantee Agency, and the International Centre for Settlement of Investment Disputes, each of which may be referred to as a member of the World Bank Group and collectively as members of the World Bank Group.

Attachment 1 – List of Subprocessors

[INTENTIONALLY LEFT BLANK]