WORLD BANK GROUP

Personal Data Annex

1. THE CONTRACT

1.01 This Personal Data 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 Section 9 of this Personal Data Annex has the meaning given to it in the Contract.

2. CONFIDENTIALITY AND COMPLIANCE WITH APPLICABLE LAW

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

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

3. DATA PRIVACY AND PROTECTION

3.01 As between Purchaser and Vendor, Purchaser will retain all right, title and interest in and to all Personal Data.

3.02 Vendor will only Process, or permit Processing of, Personal Data solely and exclusively for the Permitted Purpose in accordance with applicable law and in accordance with any other written instructions given by Purchaser.

3.03 Vendor will not, under any circumstances, sell, assign, lease, license, securitize or otherwise commercially exploit any Personal Data.

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

3.05 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: (a) notify the Data Subject and obtain consent, or ensure there is another legal basis, to Process such Personal Data; and (b) ensure that any such Personal Data is accurate and complete.

3.06 Vendor will 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.

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

4. DATA INCIDENT

4.01 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.

4.02 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.

4.03 Vendor will indemnify and hold harmless Purchaser from any and all liabilities arising out of or in connection with a Data Incident.

5. AUDIT

5.01 Purchaser, or an independent auditor appointed by Purchaser, has the right to conduct an audit of Vendor's, and any Subcontractor's, data protection practices to verify compliance with the obligations under this Personal Data Annex once per year, or at any time after a Data Incident, upon prior written notice.

5.02 Vendor will take all reasonable steps to, and will cause all Subcontractors 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.

6. THIRD PARTY REQUESTS

6.01 In the event of a Third Party Data Request affecting any Personal Data, 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 Personal Data in response to the Third Party 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 Personal Data; and

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

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

7.   RETURN OR DESTRUCTION

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

7.02   If Purchaser does not request the return and/or deletion of Personal Data under Section 7.01 within one (1) year of termination or expiration of the Contract, Vendor will immediately delete or destroy Personal Data in accordance with Section 7.01(b).

7.03   Vendor will, at Purchaser's request, provide Purchaser with written certification from a duly authorized officer attesting to Vendor's compliance with Sections 7.01 and 7.02, the date of the return, destruction or deletion of Personal Data and the methods used for such destruction or deletion.

7.04   Notwithstanding the above, Vendor may retain Personal 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 Personal 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 Personal Data.

8.   SUBCONTRACTING

8.01   Notwithstanding any other provision to the contrary in the Contract, Vendor will not subcontract any of its obligations under this Personal Data Annex, in whole or in part, without Purchaser's prior written consent in each and every instance.

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

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

9. DEFINITIONS

9.01 For the purposes of this Personal Data Annex:

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

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

(c) "**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, Personal 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 Personal Data.

(d) "**Data Subject**" means the natural living person whose Personal Data is Processed.

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

(f) "**Personal Data**" means any information disclosed by Purchaser to Vendor, or otherwise obtained by Vendor on behalf of Purchaser, in relation 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, physiological, genetic, mental, economic, cultural or social identity of an individual.

(g) "**Process**" means any operation or set of operations which is performed on Personal Data, or on sets of Personal 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 or otherwise making available, modifying, aligning or combining, restricting, erasing, deleting or destroying.

(h) "**Purchaser**" means the relevant member of the World Bank Group purchasing the Goods or Services from Vendor and described as the "Purchaser" in the Contract.

(i) "**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 Personal Data, including without limitation, pursuant to any applicable law, regulation, or other form of legal process or procedure.

(j) "**Vendor**" means the entity or individual providing the Goods or Services to Purchaser and described as "Vendor" or "Contractor" in the Contract.

(k) "**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 the 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.