

Data Protection Annex

1. APPLICATION

- 1.01 This Data Protection Annex applies in the event that Vendor is required to Process Personal Data on behalf of Purchaser under the Contract.

2. DEFINITIONS

- 2.01 For the purposes of this Data Protection Annex:

- (a) **“Authorized Personnel”** means only those of Vendor’s employees, agents, advisors or Subcontractors: (i) who have a need to know or to Process Personal Data, for the Permitted Purpose; (ii) who are bound by legal obligations to protect the Personal Data they Process which are no less rigorous than the obligations imposed on Vendor under this Contract; and (iii) in the case of Subcontractors, who have been pre-approved by Purchaser in writing.
- (b) **“Contract”** means, collectively, the following documents between Purchaser and Vendor: the Purchaser Order, the General Terms and Conditions, any special conditions, this Data Protection Annex and any other documents referred to in the Purchase Order.
- (c) **“Data Breach”** means any breach of Purchaser’s obligations under Article 4 (Data Protection and Privacy) or Article 5 (Data Security) of this Data Protection Annex.
- (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 strictly in accordance with its terms and conditions.
- (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”** or **“Processing”** or **“Processed”** 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) **“Purchase Order”** means the Purchase Order issued by Purchaser for the provision of goods or services by Vendor.
- (i) **“Purchaser”** means the International Bank for Reconstruction and Development or the International Finance Corporation as identified in the Purchase Order.

- (j) **“Vendor”** means the entity or individual named as the “Vendor” or “Contractor” in the Purchase Order.

3. COMPLIANCE

- 3.01 Vendor shall comply with all applicable data privacy, protection, security, data breach and related laws, regulations and directives.

4. PROTECTION AND PRIVACY

- 4.01 As between Purchaser and Vendor, Purchaser shall retain all right, title and interest in and to all Personal Data.
- 4.02 Vendor shall 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 or unless expressly permitted to do so under this Contract.
- 4.03 Vendor shall only Process, or permit Processing of, Personal Data solely and exclusively for the Permitted Purpose and only for so long as is required to fulfil the Permitted Purpose.
- 4.04 Vendor shall not, under any circumstances, sell, assign, lease, license or securitize any Personal Data, unless expressly permitted to do so under this Contract.
- 4.05 Vendor shall comply with all applicable data privacy, protection and security laws, regulations and directives.
- 4.06 To the extent that the Permitted Purpose requires Contractor to collect, extract or receive Personal Data from a Data Subject, collect Personal Data only according to the parameters set by Purchaser and take commercially reasonable steps to: (i) notify the Data Subject; and (ii) ensure that any such Personal Data is accurate and complete.

5. SECURITY

- 5.01 Vendor shall implement administrative, physical and technical safeguards appropriate to the risk represented by the nature of the Personal Data and the permitted Processing activities in order to protect Personal Data from a Data Breach.
- 5.02 Vendor shall, at Purchaser’s request: (a) either conduct and make available, or permit Purchaser to conduct, a vulnerability scan and formal penetration test of any of Vendor’s systems, networks and facilities used to Process Personal Data for the purposes of this Contract; (b) provide Purchaser with any third party certifications, or results of information security audits, of any of Vendor’s systems, networks and facilities used to Process Personal Data for the purposes of this Contract.

6. DATA BREACH

- 6.01 In the event Vendor becomes aware of a Data Breach, Vendor shall, at Vendor’s expense: (a) immediately notify Purchaser; (b) take reasonable steps to investigate, mitigate and remediate the impact of the Data Breach at Vendor’s expense; and (c) cooperate with

Purchaser's reasonable requests for information and assistance regarding the Data Breach.

7. AUDIT

7.01 In addition to any other audit rights granted to Purchaser under this Contract, Vendor shall, at Purchaser's request, make available to Purchaser or an independent third party on Purchaser's behalf, all information and records necessary to demonstrate or assess Vendor's compliance with its obligations under this Data Protection Annex.

8. THIRD PARTY REQUESTS

8.01 In the event Vendor receives any demand by a third party to exercise legal rights in respect of Personal Data, Vendor shall immediately notify Purchaser so that Purchaser may seek, at its own expense, appropriate remedies to protect the Personal Data.

8.02 If, notwithstanding Purchaser's efforts, Vendor remains legally compelled to disclose the Personal Data, Vendor shall: (a) only disclose that portion of the Personal Data that is necessary to satisfy the applicable legal obligation; (b) take all reasonable steps to ensure the Personal Data is afforded adequate protection.

9. RETURN OR DESTRUCTION

9.01 Upon termination or expiration of the Contract, Vendor shall: (a) promptly return to Purchaser or destroy all Personal Data in its possession, custody or control; and (b) at Purchaser's request, confirm in writing that it has complied with its obligation under this Section.

9.02 Notwithstanding the above, Vendor may retain Personal Data to the extent necessary for Vendor to comply with: (a) applicable law; or (b) Vendor's internal record keeping policies, but provided that, in each case, Vendor only retains the Personal Data for the minimum period necessary to satisfy any such obligations.