THIRD PARTY DATA PROCESSING AGREEMENT

1. DEFINITIONS

Capitalized terms used herein shall have the meaning assigned to them in the Main Contract or in this Section.

Capitalized terms used herein shall have the meaning assigned to them in the Main Contract or below. Unless otherwise defined herein, the definitions of the Nigeria Data Protection Act (NDPA) 2023, and other relevant regulations in particular the terms "Data **Controller**", "Data Processor" "**Data Subject**", "**Personal Data**" and "**Processing**" shall apply.

Company means Lafarge Africa Plc and its subsidiaries, affiliates and parent company

Company Personal Data means Personal Data of the Company's personnel, suppliers, service providers, vendors, customers, or guests processed at the instruction and on behalf of the Company, pursuant to or in connection with the Main Contract.

Contract Data Processing means personal data processing required under this Agreement and the Main Contract

Main Contract means the agreement between the Third Party and the Company, for which personal data processing is required for its performance

Party means either Third Party or Company and "**Parties**" means collectively Third Party and Company

Third Party means the Vendor, Service Provider or Consultant

2. SUBJECT MATTER AND TERM OF AGREEMENT

2.1 The Third Party shall process Company Personal Data for the purpose of providing the services described in the Main Contract ("**Contract Services**") and any additional services defined in this Agreement ("**Processing Services**") to the Company ("**Admissible Purpose**"). The Parties agree and acknowledge that the Company will be qualified as Data Controller and the Third Party will be qualified as Data Processors when processing Company Personal Data hereunder. The Third Party shall not use or disclose Company Personal Data for any other than the Admissible Purpose.

2.2 Third Party shall adhere to purpose of processing, categories of Company Personal Data and Data Subjects stated in the Main Contract. In the event of changes to the Processing, the Company may make reasonable amendments, by written notice to the Third Party from time to time as Company reasonably considers necessary to meet statutory requirements.

2.3 Third Party shall process Company Personal Data only within the territory of Nigeria. Any transfer to a foreign country requires prior written consent of the Company and shall be in compliance with the NDPA and applicable Data Protection regulation /Law.

2.4 Third Party shall process Company Personal Data only on behalf of the Company and in strict accordance with the Company's documented instructions, including with regard to transfers of Personal Data to a foreign country or an international organisation. Where Nigerian law requires a transfer of personal data, Third Party shall immediately inform the Company of the legal requirement in writing, prior to commencing such processing, unless that law prohibits such information on important grounds of public interest or as contained in the Private Guard Companies Regulations, 2018 or any regulation issued by the Nigeria Security and Civil Defence Corps. For the avoidance of doubt, whenever this Agreement or the Main Contract include provisions relating to the Processing of Company Personal Data such Processing shall be considered an instruction of the Data Controller pursuant to this Agreement.

2.5 The Processing shall at all times be conducted in a professional manner and in compliance with the principles of personal data processing, the provisions of the Main Contract, this Agreement, the NDPA and applicable Data Protection regulations. Third Party shall immediately inform the Company if, in their

opinion, an instruction of the Company infringes the NDPA or any other applicable Data Protection regulation/Law.

2.6 Unless expressly provided otherwise herein, the Company shall not be liable for any additional charges for the Processing Services under this Agreement and Third Party acknowledge and agree that all costs, charges and fees in connection with the Processing Services are fully and adequately compensated by the fees and charges payable under the Main Contract.

2.7 The duration (term) of this Agreement is equal to the term of the Main Contract and this Agreement shall terminate automatically when the Main Contract terminates, with the exception of any provisions intended to survive termination hereof or the Main Contract. Any right to terminate this Agreement separately prior to such termination date shall be excluded to the extent permitted by applicable law.

3. REQUIRED TECHNICAL AND ORGANISATIONAL MEASURES

3.1 Third Party shall ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services as well as the ability to restore the availability and access to Company Personal Data in a prompt manner in the event of a physical or technical incident as required under applicable law.

3.2 Third Party shall implement appropriate technical and organizational measures as required by the NDPA and any other applicable Data Protection regulation /Law and in line with the state of technological development and applicable data security standards in order to

(a) prevent (i) unauthorised or unlawful processing of the Company Personal Data; and (ii) the accidental loss or destruction of, or damage to, the Company Personal Data and

(b) ensure a level of security appropriate to (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and (ii) the nature of the Company Personal Data to be protected;

("**Data Security Standards**").

3.3 Without prejudice to the generality of the foregoing, the Data Security Standards that Third Party shall implement and maintain, as determined and approved by the Company, are defined in Annex 2.

3.4 Third Party warrants to implement the Data Security Standards and that they will maintain such Data Security Standards during the term hereof. Third Party shall ensure by means of appropriate protective mechanisms that access to Company Personal Data is strictly limited to those employees who require access in order to fulfil the Admissible Purpose.

4. DATA SUBJECT RIGHTS

4.1 Third Party shall correct, delete, block or otherwise process Company Personal Data and shall take any other measures in relation to requests from Data Subjects in relation to their rights under the NDPA and any other applicable Data Protection regulation/Law ("**Data Subject Requests**") only in accordance with and subject to the documented instructions of the Company.

4.2 Where the Company is obliged to provide information to a Data Subject in relation to the Processing of Personal Data or take any other action required in its reasonable discretion to comply with Data Subject Requests, Third Party shall immediately make all required information available to the Company in a format and shall take all other action reasonably requested by the Company in order to comply with such Data Subject Requests. Third Party shall implement appropriate technical and organisational measures to respond to Data Subject Requests under applicable law.

4.3 The Company shall be solely responsible for dealing with Data Subject Requests. Third Party shall

(a) immediately notify the Company of any Data Subject Requests, compliance orders pursuant to the NDPA or other enquiries relating to this Agreement received by it or any Sub-Processor without responding to such requests or enquiries unless expressly otherwise instructed by the Company; and

(b) ensure that any Sub-Processors do not respond to any Data Subject Requests unless expressly otherwise instructed by the Company or required by applicable law, in which case Third Party shall to the extent permitted by applicable law inform the Company of that legal requirement before the Sub-Processor responds to the request.

4.4 In the event of a dispute with or other claims brought by a Data Subject concerning the Processing of Company Personal Data against the Third Party or both Third Party and Company, Third Party and Company shall promptly notify and inform each other and shall cooperate and coordinate with a view to effectively defend themselves against such claims or settling them amicably in a timely fashion.

5. FURTHER DATA PROTECTION OBLIGATIONS

5.1 Third Party shall maintain and make available to the competent Supervisory Authority on request, a proper written (electronic form sufficient) record of all categories of processing activities carried out on behalf of the Company.

6. THE THIRD PARTY'S PERSONNEL/DATA PROTECTION OFFICER

6.1 Third Party shall ensure that any personnel undertaking or involved in the Processing under this Agreement are properly qualified and trained, including a specific and appropriate data protection training, and have committed themselves to keep Company Personal Data confidential or are under an appropriate statutory obligation of confidentiality in accordance with the NDPA and any other applicable Data Protection regulation/ Law which shall survive termination of this Agreement. The Company may require at its reasonable discretion that Third Party's staff enter into a specific confidentiality undertaking in a format provided by the Company. Third Party shall ensure that access to Company Personal Data is strictly limited to those individuals who need to know or access the relevant Company Personal Data, as strictly necessary for the Admissible Purposes in the context of that individual's duties.

6.2 Third Party shall provide to the Company, the details of their data protection officers (DPO) in accordance with the NDPA and the Company shall liaise with the DPO's on the matters covered by this Agreement and the Data Processing Laws

7. SUB-PROCESSING

7.1 Third Party shall be authorized to engage other Processors in relation to the Contract Data Processing ("**Sub-Processor**") only in accordance with the Main Contract and subject to the following provisions.

7.2 Any engagement of a Sub-Processor requires prior written consent of the Company and a confidentiality undertaking by the Sub-Processors. Third Party shall provide the Company with a list of Sub-Processors required for performance of its obligations under the Main Contract. Third Party shall give the Company prior written notice of the intended appointment of any new Sub-Processor, including full details of the Processing to be undertaken by the Sub-Processor. If, within four weeks of receipt of that notice, the Company notifies the Third Party in writing of any objections on reasonable grounds to the proposed appointment, Third Party shall work with the Company in good faith to take reasonable measures to address the objections raised by the Company and where such measure cannot be agreed within four weeks from Third Party's receipt of the Company's notice, the Third Party shall not appoint (nor disclose any Company Personal Data to) the proposed Sub-Processor except with the prior written consent of the Company.

7.3 With respect to each Sub-Processor, Third Party shall

(a) where processing may result in high risk within the context of the NDPA conduct a data privacy impact assessment before any Company Personal Data are transferred to the Sub-Processor, and carry out adequate due diligence to ensure that the Sub-Processor is capable of providing the level of protection for Company Personal Data required by this Agreement and the Main Contract;

(b) enter into a written agreement with the Sub-Processor which imposes the same obligations on the Sub-Processor in relation to the protection of Company Personal Data as are imposed on Third Party under the NDPA and this Agreement. This shall apply in particular, but shall not be limited to, the confidentiality obligations and the Data Security Standards to be observed pursuant to Section **Error! Reference source not found.**;

(c) immediately upon request provide the Company with the sub-contracting agreement and any other documentation reasonably requested by the Company (it being understood that the Third Party shall be permitted to redact any commercial terms which are confidential and not required by the Company to assess compliance with their obligations under this Agreement);

7..4 Third Party shall at all times and without being so requested provide the Company with an up to date list of Sub-Processors, detailing company name, address, contact details, the specific area of Contract Data Processing operations outsourced and the location of the Processing.

7.5 In case of non-compliance of the Sub-Processor with its contractual obligations, the Third Party shall remain fully liable to the Company for any damages caused by such non-compliance and shall indemnify and hold harmless the Company against any claims or damages in connection with or resulting from the engagement of the Sub-Processor.

8. INSPECTIONS AND AUDITS

8.1 Third Party shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement and the NDPA, and shall allow for and contribute to audits in relation to the Processing of Company Personal Data, including inspections of the data-processing facilities of the Third Party by the Company or an auditor mandated by the Company in accordance with this Section **Error! Reference source not found.**.

8.2 Company shall give Third Party reasonable notice of any audit or inspection to be conducted and shall make (and ensure that each of its mandated auditors makes) reasonable endeavours to avoid causing (or, if it cannot avoid, to minimise) any damage, injury or disruption to the Service Providers' premises, equipment, personnel and business in the course of such an audit or inspection. Audits or inspections shall not be conducted outside normal business hours, unless Company has given notice to the Third Party that the audit or inspection needs to be conducted on an emergency basis.

8.3 Company shall notify Third Party about any deficiencies or irregularities related to the Processing of Company Personal Data discovered during such audits or inspections and the Third Party shall promptly take any action required or reasonably requested by the Company to remedy such findings and provide Company with written documentation evidencing that the audit findings has been remedied as required by applicable law and this Agreement.

9. PERSONAL DATA BREACHES AND INCIDENTS

9.1 Third Party shall immediately notify the Company of any actual or suspected technical, organizational or other incidents (including incidents at Sub-Processors) which have resulted or may result in a Personal Data Breach or otherwise have an adverse effect on the integrity and security of Company Personal Data or the Contract Data Processing ("**Data Security Incident**"). Data Security Incidents include in particular, but are not limited to, the following:

(a) Any actual or suspected unauthorized access, disclosure, loss, download, theft, blocking, encryption or deletion by malware or other unauthorized action in relation to Company Personal Data by unauthorized third parties;

(b) any operational incidents which may have an impact on the Processing of Company Personal Data;

(c) any actual or suspected breach of this Agreement, NDPR or any other Data Protection Law by the Third Party, their employees or other vicarious agents to the extent that such breach relates to Company Personal Data or the Service Providers' obligations under this Agreement; or

(d) any legally binding request for disclosure or seizure of Company Personal Data by a law enforcement or other public authority unless Third Party is prohibited by statutory law to notify such incident to the Company. In this case, Third Party must notify the Company immediately upon such prohibition having ceased.

9.2 Third Party must notify the Company immediately, but in any case no later than 24 hours after becoming aware of a Data Security Incident. Third Party's notification to Company must be comprehensive and include any information the Company specifically requests or which may reasonably be expected to be required or appropriate in order to comply with its legal obligations in relation to the Data Security Incident. This includes in particular as a minimum the following:

(a) the nature of the Data Security Incident, the categories and numbers of Data Subjects concerned, and the categories and numbers of Personal Data records concerned;

(b) the name and contact details of the Third Party's data protection officers or other relevant contact from whom more information may be obtained;

(c) the likely consequences of the Data Security Incident; and

(d) the measures taken or proposed to be taken to address the Data Security Incident.

Notification must be made by email to: ng-m-dataprotection@lafarge.com

9.3 Third Party is not authorized to notify a Data Security Incident to a Supervisory Authority or other authority, the data subjects concerned or any other third parties unless they are required to do so under applicable law (e.g. if the Data Security Incident results in a Personal Data Breach for which the Third Party is responsible as Data Controllers). In such event, Third Party shall, to the extent permitted under applicable law, liaise and coordinate with Company prior to making a notification. Best efforts shall be utilised to agree on a joint approach with a view to prevent any contradicting or inconclusive notifications. This includes providing each other with the details of any notification and the date and time on which notification will be made.

9.4 In the event of a Data Security Incident, Third Party shall immediately and in coordination with Company take any measures required and adequate under applicable law and technical standards to restore the confidentiality, integrity and availability of Company Personal Data and the resilience of the processing systems and services and to mitigate the risk of harm and/or any detrimental consequences for the data subjects affected or potentially affected by the Data Security Incident. Third Party shall promptly provide Company with a written incident report detailing such measures taken and specific measures taken to prevent similar incidents in the future.

10. COMMUNICATION WITH AUTHORITIES

To the extent permitted under applicable law,

(a) Third Party shall immediately notify Company in the event of any audits, enquiries, investigations, requests, orders or other proceedings or matters which may relate to Company Personal Data or Third Party's obligations under this Agreement by a Supervisory Authority or any other public body in relation to the Processing of Company Personal Data ("**Authority Enquiries**").

(b) in the event of a dispute with, orders or fines imposed or other claims brought by a Supervisory Authority or other competent authority concerning the Processing of Company Personal Data against either or both Company and Third Party, the Parties shall promptly notify and inform each other and shall cooperate and coordinate with a view to effectively defend themselves against such claims or settling them amicably in a timely fashion.

11. RETURN AND DELETION OF COMPANY PERSONAL DATA

11.1 Upon termination of the Main Contract or anytime upon request of the Company, the Third Party shall promptly delete and procure the deletion of all copies of Company Personal Data. Company may in its absolute discretion by written notice require the Third Party to return a complete copy of all Company

Personal Data to Company by secure file transfer in such format as is reasonably notified by Company to Third Party. Third Party shall comply with any such written request.

11.2 Third Party may retain Company Personal Data for the duration of the Main Agreement and/or to the extent and period required by applicable law. Provided that Third Party shall ensure that such retained Company Personal Data is (i) kept confidential and protected against unauthorized access, disclosure or use and (ii) only Processed as necessary for the purpose(s) specified in the applicable law requiring its storage and for no other purpose.

11.3 Third Party shall not have any right of retention in this respect and shall, upon request of Company, immediately confirm full compliance with the above obligations in writing. If so reasonably requested by the Company, Third Party shall allow for and contribute to audits, including inspections, conducted by the Data Controller in accordance with Section **Error! Reference source not found.**.

11.4 Third Party shall promptly ensure that all Sub-Processors comply with this Section accordingly.

12. BREACH OF THIS AGREEMENT

12.1 In the event of a material breach of duties and obligations by the Service Providers under this Agreement which affects the integrity and security of Company Personal Data, the Company shall be entitled to terminate this Agreement and the Main Contract for cause with immediate effect. Any liability cap under the Main Contract shall not preclude, remove or adversely affect the legal liability incumbent on any party according to the NDPA and applicable data protection regulation /law.

13. AMENDMENT FOR DATA PROTECTION COMPLIANCE

13.1 In the event of any changes of applicable law or guidance by supervisory authorities or any specific instructions or orders by competent supervisory authorities in relation to this Agreement, the Parties shall promptly amend this Agreement as reasonably required and appropriate to ensure compliance with such changed legal requirements.

14. FINAL PROVISIONS

14.1 *Order of precedence.* This Agreement varies the terms of the Main Contract and the provisions of this Agreement are incorporated into and form part of the Main Contract as if set out in the Main Contract in full. In the event of any conflict or inconsistency, the provisions of this Agreement shall take precedence over the provisions of the Main Contract. Otherwise, the provisions of the Main Contract shall remain in full force.

14.2 *Written form.* No change of or amendment to this Agreement and any of its terms shall be valid and binding unless made in writing and unless they make express reference to being a change or amendment to this Agreement. The foregoing shall also apply to the waiver of this mandatory written form.

14.3 *Severance.* Should any provision of this Agreement be invalid or unenforceable, then the remainder of this Agreement shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein. This shall apply accordingly in the event of any unintended gaps.