HEIDELBERGCEMENT INDIA LIMITED

Personal Data Privacy Policy

1. Preface

HeidelbergCement India Limited (hereinafter referred to as the '**Company**') is committed to respect privacy of every person, including employees of the Company, business partners as well as vendors, dealers, customers and other stakeholders who share their sensitive personal data with the Company. This privacy policy ('**Policy**') is applicable to all stakeholders who disclose Sensitive Personal Data to the Company for fulfilling lawful business requirements of the Company.

The purpose of this Policy is to give the Information Providers an understanding on how the Company intends to collect, receive, possess, store, transfer, handle, deal with and use the Sensitive Personal Data provided.

2. Definitions:

Biometric data: means facial images, fingerprints, iris scans, or any other similar personal data resulting from measurements or technical processing operations carried out on physical, physiological, or behavioral characteristics of a data principal, which allow or confirm the unique identification of that natural person.

Financial data: means any number or other personal data used to identify an account opened by, or card or payment instrument issued by a financial institution to a data principal or any personal data regarding the relationship between a bank/financial institution and a data principal including financial status, income, wealth status and credit history.

Genetic data: means personal data relating to the inherited or acquired genetic characteristics of a natural person which provides unique information about the behavioral characteristics, physiology or the health of that natural person and which results, in particular, from an analysis of a biological sample from the natural person in question.

Data Protection Representative: means designated officer/employee of the Company who has been entrusted with the responsibility to ensure that adequate systems and procedures remain in operation that will maintain confidentiality of Sensitive Personal Data submitted to the Company by the Information Providers

In writing: includes any communication in electronic format as defined in clause (r) of sub-section (1) of section 2 of the Information Technology Act, 2000

Personal Data: Data from which an individual can be identified like name, address, sex, religion, caste, etc.

Sensitive Personal Data (SPD): Types of personal data such as financial, health, blood group, sexual orientation, biometric, genetic, transgender status, belief etc.

3. Scope of the Policy

Sensitive Personal Data of the Information Providers may be required to be collected, maintained and stored in India and may also need to be shared with Group Companies or third party, within and outside the country, as per lawful business requirements of the Company and its affiliates.

The Company shall ensure confidentiality of such Sensitive Personal Data and the complaints/issues, if any shall be resolved by the Data Protection Representative appointed by the Company for this purpose.

Having provided the Sensitive Personal Data to the Company, the Information Providers shall be deemed to have given their consent to its collection, storage, usage, disclosure, processing and transfer for the purposes mentioned in this Policy.

The Information Providers have the option of not providing their Sensitive Personal Data sought by the Company if they do not agree with this Policy or even otherwise. Further, the Information Providers may also submit an intimation in writing, requesting the Company to stop using their Sensitive Personal Data.

4. Collection of Data or Information

The Company may collect the following types of Sensitive Personal Data, including but not limited to:

- Name, address, contact numbers, email ID, details of past employment (in the case of employees, wherever relevant);
- Family details, their addresses, contact numbers, email ID, relationships, family history etc.
- Financial details such as bank account, pan card, salary slips, provident fund details, Income Tax Returns, other Tax Returns;
- Blood group, medical history, physiological and mental health condition, sexual orientation etc.
- Biometric information.

5. Sensitive personal data or information collection

The Company may collect, use, receive, possess, store, disclose, process and transfer the Sensitive Personal Data for various purposes, including but not limited, to the following:

- To enable functioning of the Company's business;
- In connection with a variety of purposes relating to employment or engagement of employees or training including but not limited to general HR administration; organization planning and management;
- Compliance with company's policies, code of conduct and internal policies and regulations;
- Business mergers and acquisitions; business transfers, business restructuring etc.;
- Legal & judicial proceedings, governmental and regulatory compliance;
- Tax administration and compliance;
- Overseas affiliates' compliance with foreign laws and cooperation with overseas regulators;
- To transfer to IT services providers/Software developers;
- To administer or otherwise carry out obligations in relation to any agreement which has been executed by the Information Providers with the Company; and
- To investigate, prevent, or take action regarding illegal activities, suspected fraud, violations of the law or as otherwise required by law.

6. Transferring and sharing of Sensitive Personal Data

The Information providers understand and consent that the Company may need to share the Sensitive Personal Data with group companies within and outside India, business associates and/ or third parties within and outside India in connection with the lawful purposes, as mentioned above.

The Information Providers authorize the Company to exchange, disclose, transfer, share, part with the Sensitive Personal Data and/or any information provided, within or outside India for the above purposes.

7. Confidentiality of the data processing

Only authorized employees or person/s authorized by the Company process personal data. It is in particular forbidden for employees to use personal data for own benefit/purpose, to transmit these to unauthorized persons or to make these accessible in any other manner.

8. Reasonable Security Practices and Procedures

The Company has adopted reasonable security practices and procedures to ensure that the Sensitive Personal Data is collected and preserved in a secured manner. Suitable measures are taken in order to protect the data against accidental or unauthorized destruction or against loss. In case the Information Providers wish to know more details about the adopted reasonable security practices and procedures, they may contact the Data Protection Representative of the Company for the same.

While the Company will endeavor to take all reasonable and appropriate steps to keep secure any information and prevent its unauthorized access and transfer, the information providers agree and acknowledge that the Company cannot provide any absolute assurance regarding the security of the Sensitive Personal Data. To the maximum extent permissible under applicable laws, the Company disclaims any liability in relation to any breach of security or loss or disclosure of information in relation to the Personal Information.

If the Information Provider needs to access update or correct the Sensitive Personal Data, he/she may contact the Data Protection Representative of the Company for the same.

9. Data Retention

It is the Company's policy to retain Sensitive Personal Data of the Information Providers only for as long as the Company believes it to be necessary for the purpose for which such Sensitive Personal Data was collected, subject to any legal requirements for the information to be retained for longer period, if any.

10. Changes in the Policy

The Company reserves the right to revise and update this Privacy Policy at any time without expressly informing the Information Providers. Any such revision will be effective on and from the date of posting the same on the intranet/internet website of the Company, and will apply to all information collected both prior to and following the effective date. Information Providers are advised to visit the website and intranet periodically to review the current policies with regard to Sensitive Personal Data.

11. Complaints

The Company has nominated Mr. Ajay Panwar, Head-Information Technology of the Company as the Data Protection Representative. The Information Providers may approach the Data Protection Representative if they have any complaint, question or concern with respect to the

processing and use of their Sensitive Personal Data. The Data Protection Representative can be contacted by mail at the email id ajay.panwar@heidelbergcement.in. The Company is committed to ensure a fair and rapid resolution of any complaint or dispute about privacy and handling the Information Providers data and will be happy to respond to their queries and comments.

Please note that the emails received @ ajay.panwar@heidelbergcement.in in respect of a context other than a Data Privacy issue will not be attended. Please do not send emails to this Id for queries, complaints related to Sales, Service, Recruitment, Procurement, Investor Services etc.

---o0o---