

BID CORPORATION LTD

Registration Number: 1995/008615/06

DATA PRIVACY POLICY

1. OBJECTIVES

- 1.1. The protection of personal information of those that we engage with during day-to-day operations is a matter of importance for Bid Corporation Ltd ('*Bidcorp*' or '*the company*').
- 1.2. This Data Privacy Policy –
 - 1.2.1. is applicable to Bidcorp and its subsidiaries (*'the group'*), in their respective geographies;
 - 1.2.2. is the group's statement of principles setting out how we intend to manage personal information and it compliments relevant local legislation; and
 - 1.2.3. extends to the processing of all personal information. Where Bidcorp owns or has operations in countries where data from legal entities is protected to the same extent as personal information, this Data Privacy Policy will apply equally to the data of legal entities.
- 1.3. In the event of discrepancies between this Data Privacy Policy and the provisions of relevant local data protection legislation, the latter will prevail.

2. RESPONSIBILITIES

- 2.1. In keeping with the decentralised structure of the group, the management teams of Bidcorp's subsidiaries are responsible for -
 - 2.1.1. ensuring that the legal requirements in terms of applicable data protection legislation (if any) are met within their respective jurisdiction;
 - 2.1.2. ensuring data privacy is managed within their operations;
 - 2.1.3. implementing a data privacy policy and internal privacy and external privacy notices if required in terms of applicable data protection legislation within their operations; and
 - 2.1.4. designating individuals responsible for data privacy within their operations.
- 2.2. Bidcorp will provide oversight and guidance to its subsidiaries in respect of data privacy policies.
- 2.3. Compliance with the legal provisions on the protection of personal information is an obligation of every group employee, contractor and/or outsourced service provider.

3. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

The group is guided by the following principles in ensuring that personal information is adequately protected -

3.1. Legality and fairness

Personal information must be collected and processed legally and correctly in relation to data subjects, in order to protect their rights.

3.2. Limitation of purpose

Personal information must only be collected for determined, explicit and lawful purposes, defined prior to data collection and, where required in terms of applicable data protection legislation, communicated to the data subject. Subsequent changes to the purpose are possible only to a limited extent and usually require a valid explicit reason.

3.3. **Transparency**

The data subject must be informed of the manner in which their personal information is to be processed. Where possible, personal information must be collected directly from the data subject.

3.4. **Accurate and timely data**

Personal information must be accurate, complete and updated as and when necessary. Measures must be taken to ensure that inaccurate or incomplete data is deleted, corrected, supplemented, or updated.

3.5. **Reduce and minimise data**

Personal information must be appropriate, relevant, and limited. Before processing personal information, responsible parties must determine whether, and to what extent, the processing of personal information is necessary to achieve the purpose for which it is to be collected.

3.6. **Retention of personal information**

Personal information must be retained in a form that permits the identification of the data subjects concerned and only for as long as it is necessary to fulfil the purpose for which personal information was collected. The retention period of information will be determined by each responsible party in line with their local regulatory requirements. Personal information must also be deleted, destroyed or de-identified if the responsible party is no longer authorised to retain it.

3.7. **Removal of personal information**

Responsible parties must remove, delete or destroy personal information that is no longer required for the purposes for which it was collected, or if consent is withdrawn by a data subject and there is no other legitimate purpose for data processing to be carried out.

3.8. **Integrity and confidentiality**

Personal information must be protected against unauthorised or unlawful access, processing and disclosure.

3.9. **Rights of the data subjects**

The group respects the rights of all data subjects and will treat any personal information requests seriously, allowing data subjects to access, correct, delete, or restrict the processing of their personal information.

3.10. **Security of data and data processing**

Appropriate technical, operational and security measures must be adopted to prevent unauthorised access, processing, disclosure and safeguard against accidental loss, destruction, or deterioration of personal information. In the event of a data breach, the responsible party must notify any affected data subjects and restore the availability of and access to personal information, in a timely manner if so required in terms of applicable data protection legislation.

3.11. **Responsibility in the processing of personal information**

Group companies, as responsible parties, will be responsible for compliance with relevant local data protection legislation and must demonstrate compliance therewith.

4. **DISCLOSURE OF PERSONAL DATA**

4.1. Personal information may only be transferred under the following circumstances -

4.1.1. to employees and contractors of responsible parties, principal service providers or collaborators, for the processing of personal information for an intended purpose. The employees and contractors acting on behalf of any responsible party must do so only in accordance with instructions from the applicable responsible party, which must retain control of the personal information;

- 4.1.2. to Bidcorp's board of directors (*'board'*), on a need-to-know basis, with the implementation of appropriate safeguards, to ensure the integrity and security of personal information;
 - 4.1.3. if personal information which has been collected in the course of the provision of services to another customer within the group, such data may be communicated to that customer and, if permitted by law, to other persons for the purpose of rendering such services;
 - 4.1.4. to companies providing anti-money laundering, fraud prevention and/or crime prevention services as well as companies providing other similar services, including financial institutions, credit bureaus and/or regulatory authorities with which personal information may be required to be shared;
 - 4.1.5. to any third party that Bidcorp or its subsidiaries assigns or identifies any rights or obligations; and/or
 - 4.1.6. to courts of law, law enforcement authorities, lawyers, or other persons, if it proves to be justly necessary to establish, exercise or defend a right to a fair hearing.
- 4.2. Operators processing personal information on behalf of responsible parties must comply with their relevant local data protection legislation and this Data Privacy Policy. Responsible parties must enter into contracts with operators that will process personal information on their behalf. An appointed operator must only process personal information in accordance with instructions from the responsible party. Operators must undertake to use appropriate safeguards, in accordance with relevant local data protection legislation, to ensure the integrity and security of personal information. Operators must notify the relevant responsible party if there is reason to believe that personal information was disclosed or obtained by an unauthorised person. When selecting and appointing an operator to process personal information on behalf of Bidcorp or its subsidiaries, the responsible party must -
- 4.2.1. request the operator to provide details of its safeguards in place with respect to compliance with data security requirements;
 - 4.2.2. select an operator based on its ability to provide the necessary technical and organisational data safeguards;
 - 4.2.3. ensure that instructions for processing information as well as the responsibilities of the responsible party and the operator are documented; and
 - 4.2.4. in relation to employees, take account of the contractual standards for the protection of personal information implemented at company level.

5. DIRECT MARKETING

- 5.1. Responsible parties will ensure that any direct marketing complies with applicable data protection legislation and where required will allow data subjects to opt out from receiving such marketing.

6. REGISTRATION AND PRIOR AUTHORISATION

- 6.1. Responsible parties will comply with registration and prior authorisation requirements as may be required in terms of applicable data protection legislation.

7. TRANSBORDER TRANSFERS OF PERSONAL INFORMATION

- 7.1. Responsible parties will ensure that any transborder transfer of personal information occurs in compliance with applicable data protection legislation and will, by way of example, obtain consent from the relevant data subject prior to such transfer.

8. SUPERVISORY AUTHORITY

- 8.1. Responsible parties will cooperate with supervisory authorities as and when required to do so in terms of applicable data protection legislation.

9. CONTROL OF DATA PROTECTION

- 9.1. Compliance with data protection policies and legislation across the group may be verified through periodic data protection control audits carried out by Internal Audit or other assurance providers.
- 9.2. The results of the data protection control audits will be reported to the Bidcorp Group Audit and Risk Committee ('GARC') via the Divisional Audit and Risk Committee. Upon request, the results of the data protection control audits will be made available to the relevant supervisory authority.

10. RELATED DOCUMENTS

- 10.1. The Bidcorp Data Privacy Policy is to be read in conjunction with Bidcorp's Code of Ethics and the Bidcorp Group Fraud Prevention, Anti-Bribery and Corruption Policy.

11. REVIEW OF THE POLICY

- 11.1. This policy was approved and adopted by the board and will be reviewed by the GARC on a biennially basis, or sooner should new business requirements come into place, to ensure alignment with regulations, relevance and applicability.

Mr S Koseff
Chairman: Bidcorp Board
Reviewed and approved: August 27th 2024

Mrs H Wiseman
Chairman: Bidcorp GARC

Terminology -

"**Consent**" the explicit consent of the data subject to have their personal information processed, which must always be express and unambiguous.

"**Data subject**" includes all living individuals and juristic persons about whom Bidcorp or its subsidiaries hold personal information. All data subjects have legal rights in relation to their personal information.

"**Disclosure**" means the action of transmitting, disseminating, making available in any other way personal information outside the responsible party.

"**Operators**" include any person who processes personal information on behalf of a responsible party. Employees of responsible parties are excluded from this definition, but it could include suppliers which handle personal information on behalf of Bidcorp or its subsidiaries.

"**Personal information**" means information relating to an identifiable, living, natural person, and (where applicable) an identifiable, existing juristic person, including the name, race, gender, marital status, address and identifying number of a person, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person. It may also include any special information concerning religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life or biometric information of a data subject; or the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.

"**Processing**" is any activity that involves the use of personal information. It includes any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including—

- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation, or use;
- dissemination by means of transmission, distribution, or making available in any other form; or
- merging, linking, as well as restriction, degradation, erasure, or destruction of information.

"**Responsible parties**" are the people who or organisations which determine the purposes for which, and the manner in which, any personal information is processed, which have a responsibility to establish practices and policies in line with applicable local data protection legislation.

"**Supervisory authority**" means the national authorities for the surveillance of personal information processing or any other authority to which data protection responsibilities are assigned under the data protection legislation of any country.

"**Third party**" means a natural or legal person, public authority, agency or body other than the data subject, the operator and persons under the direct authority of the operator.