1. INTRODUCTION

Binding corporate rules (BCR) are data protection policies adhered to by companies for transfers of personal data within a group of undertakings or enterprises. Such rules must include all general data protection principles and enforceable rights to ensure appropriate safeguards for data transfers. They must be legally binding and enforced by every concerned member of the group.

2. OBJECTIVE

CBMM complies with privacy and data protection laws around the world and applies the highest possible standards in a consistent way to provide protections to its employees, partners, and customers.

CBMM has developed these Binding Corporate Rules (“Corporate Rules”) to ensure its commitment with Privacy throughout all aspects of its operations and to set guidelines to enforce the protection of Personal Data by CBMM and its subsidiaries (collectively, “CBMM Entities”) globally.

CBMM Entities must comply with the Corporate Rules when Processing Personal Data of any nature and/or origin.

CBMM Corporate Rules will be available at CBMM´s website for public consultation.

3. FIELD OF APPLICATION

The Corporate Rules apply to the Processing of Personal Data by all CBMM Entities.

The list of CBMM Entities and their contact Information can be found in EXHIBIT 1

4. BINDING NATURE

Corporate Rules set obligations that apply to and are enforced by all CBMM Entities. Additionally, employees are trained to follow the Corporate Rules.

If applicable law imposes a higher level of protection than those set forth in these Corporate Rules, CBMM Entities will comply with applicable law.

If, however, applicable law is less protective, these Corporate Rules shall apply to the Processing by CBMM Entities.

In case of discrepancies in these Corporate Rules, its terms shall be interpreted in a way that is most consistent with the basic concepts of the principles of EU Directive 95/46/EC.

5. DATA PROTECTION PRINCIPLES

All CBMM's Entities' Processing activities, despite the nature or origin of the Personal Data, are guided by the following principles.

- ADEQUACY: Data collection supports reasonable business requirements and is proportionate to CBMM´s Entities needs.

- DATA MINIMISATION: CBMM Entities do not use unnecessary, disproportionate, or excessive Personal Data in relation to the purposes for which it is collected.

- DATA QUALITY: All Personal Data is kept accurate and up to date as reasonably possible.

- DATA PROTECTION BY DESIGN: CBMM Entities takes all the necessary safeguards since the conception and throughout its processes to meet the privacy requirements of the applicable legislation, its Policies, and the rights of data subjects.

- DATA PROTECTION BY DEFAULT: The security and organizational measures taken to ensure data protection are embedded by default and require an individual intervention to control the access to personal data.

- INFORMATION SECURITY: the adoption of procedures, technologies and solutions that guarantee greater protection of personal data in order to avoid unauthorized access and/or accidental or unlawful situations of destruction, loss, alteration, communication, disclosure or any other action that may compromise Integrity, Availability or Confidentiality of such.

- LEGAL BASIS FOR PROCESSING: Every CBMM data processing activity have its lawfulness ensured since are grounded in a legal basis according to the applicable data protection legislation.

- STORAGE PERIODS: Personal Data is stored for the shortest period regarding the intended purpose and in compliance with legal requirements that regulate such Processing activity.

- NON-DISCRIMINATION: CBMM's Entities do not use Personal Data for discriminatory or abusive purposes.

- PURPOSE LIMITATION: Processing of Personal Data only takes place to achieve legitimate and specific purposes previously informed to Data Subjects.

- SENSITIVE OF PERSONAL DATA: The few activities that involve Processing of Sensitive Personal Data, mainly regarding the protection of vital interests of the data subject and legal obligations, receive the maximum-security priority and, after a rigorous assessment, were deemed lawful and legitimate under the applicable laws.

- TRANSFER OF PERSONAL DATA TO THIRD PARTIES (NOT BOUND BY CBMM'S Corporate Rules): Before any transfer of personal data to third parties not bound by this Corporate Rules CBMM's Entities will assess the third parties' level of maturity in data protection. Also, the third parties must ensure the appropriate Information security measures to protect the personal data involved. In case of international transfers, the specific legal requirements, such as specific contractual clauses or standard clauses, for example, should be met.

6. DATA SUBJECTS' RIGHTS

Clear, accurate and easily accessible Information on the Processing and on their rights is provided to Data Subjects and can be found in the Company's Privacy Notices at https://cbmm.com/pt/Privacy-Policy..

The abovementioned online tool can also be used by Data Subjects to request access, revision, and rectification of their Personal Data, as well as to object the Processing of Personal Data and claim right to data deletion, portability, or the rights regarding decisions based solely on automated processing, amongst others.

Additionally, Data Subjects are entitled to enforce their rights with regard to the Processing of their Personal Data by contacting CBMM's DPO through https://cbmm.com/pt/privacy-policy/direitos-dos-titulares.

CBMM Entities will comply with requests as soon as reasonably possible in accordance with applicable law.

Before replying to a request, CBMM Entities may need to confirm the identity of the Data Subject and, in order to do so, may ask for an ID document. If the requestor is not the Data Subject himself, a written confirmation shall be necessary to determine that the requestor is authorized to act on behalf of the Data Subject (for example, a power-of-attorney, document proving that the requestor is the legal representative of the minor Data Subject etc.).

Data Subjects whose Personal Data is processed by CBMM Entities acting as a Controllers are entitled to enforce their rights as thirty-party beneficiaries directly before the CBMM's Entity responsible for Processing them. If the request concerns a Processing activity of which the CBMM Entity is acting as a Processor on behalf of a Controller, the CBMM Entity will notify the Controller of such request and will cooperate with the Controller Information if needed.

CBMM Entities may not be able to comply with requests for deletion of Personal Data if they are required by law to retain such Information or if there is any other reason why the request can´t be satisfied (such as fraud prevention, dispute resolutions, investigations, compliance with legal requirements and other actions otherwise permitted by applicable law).

If the response given by CBMM's Entity is not deemed satisfactory and/or if Data Subjects understand that the data Processing carried out by any CBMM Entity is irregular, the Data Subject is entitles to lodge a complaint before the competent Data Protection Authority or file a lawsuit before a competent Court to claim enforcement of the Corporate Rules or liability as third-party beneficiaries and, where appropriate, compensation in accordance with the terms set up in the Corporate Rules and applicable law.

7. BINDING OBLIGATIONS TO COMPETENT AUTHORITIES

CBMM Entities are ready and willing to collaborate with any competent authority in order to cease irregular or illegal data Processing, as well as compensate Data Subjects for any damages arising from the violation of the Corporate Rules by the Company. If administrative or legal proceedings take place, CBMM will bear the burden of proof to demonstrate the violations did not occur, if the case may be.

The enforcement rights and mechanisms described above and throughout these Corporate Rules are in addition to other remedies or rights provided by CBMM or available under applicable law.

8. PRIVACY GOVERNANCE STRUCTURE

CBMM Entities have a permanently appointed DPO and a Privacy Office responsible for Privacy matters for all CBMM Entities globally, whose responsibilities include:

- Evaluate, review, and approve the legal bases of Processing of Personal Data;

- Foster organization compliance with the personal data protection laws through activities that include, but are not limited to, audits, awareness activities and training of personnel involved in Processing operations;

- Guide the collection and Processing of Personal Data;

- Evaluate the possibility to start the Processing activity upon the conclusion of a DPIA;

- Stimulate and apply the Privacy by design principle in Privacy activities;

- Advise and support the Privacy Office on the response to Data Subjects' requests;

- Notify the competent Data Protection Authority and the Data Subjects in case of Security Incident when necessary and/or requested by applicable law.

The DPO is assisted by a Privacy Office appointed by the DPO himself. Amongst other activities, the Privacy Office will manage the collection flow of Personal Data, the requests from Data Subjects and the registries of operations related to the Processing of Personal Data as well as evaluate third parties involved in the activities of Processing of Personal Data of CBMM.

The DPO and the Privacy Office interacts with all other departments of CBMM, such as legal, Information security, risk, and internal audit to ensure compliance with Privacy.

The DPO responds to the Privacy Commission, a collegiate body composed of members of different departments of the company and in charge of discussions regarding Privacy issues and Processing activities. In its turn, the Privacy Commission may revert the decisions to CBMM´s Executive Committee/ Board depending on the risk of the activity.

9. PERSONAL DATA FLOW MANAGEMENT

To make sure that the Personal Data flow used in CBMM Entities business processes comply with legal and internal requirements, the steps below are followed when Processing Personal Data.

Collection of Personal Data - Collection of Personal Data is made in accordance with the principles mentioned above, including but not limited to, purpose limitation, adequacy and data quality.

Whenever Personal Data is provided by Data Subjects themselves, they are informed, prior to collection, of all details related to the Processing activity, as well as to their rights. Personal Data may only be collected by other means if (i) the database is notoriously reliable (for example, from public and official bodies or entities) and the lawfulness of the origin can be ensured; (ii) there is an agreement between the database provider and the Company containing adequate Privacy provisions and guarantees; or (iii) the DPO and/or Information the Privacy Commission have expressly authorize such collection.

Personal Data provided by third parties may only be received upon the execution of an agreement with appropriate Privacy provisions.

Use of Personal Data - The use of Personal Data is limited to the Information purpose previously informed to the Data Subject.

Storage of Personal Data - Personal Data is kept for the shortest period regarding the intended purpose unless there is a legitimate reason to retain it for a longer period, provided such storage is approved by the DPO and/or the Privacy Commission as the case may be.

Disposal of Personal Data - Once the purpose and the storage term are reached, according to our Policies, Personal Data may either disposed properly or undergoes a permanent anonymization process, becoming impossible to be associated to an individual, considering reasonable technical means available at the time of the process.

Sharing Personal Data with Third Parties - CBMM Entities may share Personal Data with third parties worldwide acting as Controllers or Processors (such as service providers or vendors) to allow the provision of a specific service or to meet a specific demand of the Company. These sets of transfer only as an exception will involve

sensitive data, as above-mentioned, and could refer to legal representatives of CBMM Entities or third parties, employees or data subjects connected to the Company's activities.

CBMM Entities mandatorily execute proper agreements foreseeing standard Privacy provisions in order to ensure the Integrity, Confidentiality, Availability, and security of the Information shared, as well as the compliance with Privacy laws and regulations.

CBMM Entities may also share Personal Data with law enforcement, regulatory authorities or other third parties if required by law, if it is necessary to protect CBMM Entities' rights or if there is a legitimate purpose.

In case of transfer of Personal Data to third parties in foreign countries without levels of protections of Personal Data considered adequate by the competent Data Protection Authority, CBMM Entities adopt specific or standard provisions in agreements to ensure the Integrity, Availability and Confidentiality of Personal Data.

Although unusual in its daily activities, CBMM may also rely on one of the following safeguards to make said transfers: (i) proper safeguards regulated by the competent Data Protection Authority; (ii) global corporate rules; (iii) seals, certificates and codes of conduct regularly issued; (iv) specific consent from the Data Subjects; (v) requirement by law for health protection and/or for other specific circumstances; and (vi) express authorization from the competent Data Protection Authority.

Data Transfers between CBMM Entities - CBMM Entities share Personal Data in the normal course of business with other CBMM Entities worldwide. All data transfers made between CBMM Entities globally are under strict security rules and systems, according with CBMM internal Information Security and Privacy Policy. The mentioned standards and rights are enforceable in the terms of this Corporate Rules.

10. PRIVACY PRACTICES

10.1. Register of Processing Activities

All CBMM Entities keep a register with all Processing of Personal Data activities with, at least, the following Information on each operation:

- Description of Information flow in each phase of its lifecycle (collection, storage, use, transfer – and, in this case, the purpose of transfer – and disposal);
- Legal basis for the Processing;
- Types of Personal Data collected;

- Purpose for which Personal Data is processed;
- Logical location (cloud, server, computer etc.) and geographic, where the Processing takes place;
- Retention period of Personal Data; and
- Amount of Personal Data.

10.2. Data Protection Impact Assessment (DPIA)

DPIA is a document that describes Processing activity pertaining to a Personal Data that, due to its nature, may impact rights and freedoms of the Data Subjects.

The DPIA contains the risk mitigation measures proposed to ensure proper protection of Data Subject's rights and freedoms.

10.3. Training

Employees having permanent or regular access to Personal Data Processing receive periodical and appropriate Privacy and Information security awareness training on (i) general concepts of Personal Data Privacy; (ii) specific guidance on Personal Data Privacy applied to the activities in the Company; and (iii) the terms of the Corporate Rules and how to comply with it.

Employees are also required to review these Corporate Rules and other CBMM´s relevant privacy and security policies.

10.4. Internal Audits

CBMM Entities undergo periodical checks to assess its conformity with the applicable legislation.

CBMM may appoint independent external auditors for further resolution to the extent matters are not resolved properly.

The results of such audits may be shared with Data Protection Authority and/or any other administrative or judicial authority upon request when necessary and relevant for the due process of law and investigations.

10.5. Security

In order to ensure the security of Personal Data processed during the activities and prevent undue or non-authorized access, loss, destruction, or any other action that may compromise the Integrity, Availability or Confidentiality of said Information, CBMM adopt procedures and tools that meet the highest standards of technical regulations related to Information security.

All CBMM employees work together to keep the personal Data processed always secure, maximizing the prevention to exposure, leaks, and undue access.

To ensure that the security measures deployed by CBMM Entities are always updated and in compliance with the best practices and tools currently available in the market, the procedures undergo periodic reviews to identify and correct eventual failures.

10.6. Security Incident Communication

At https://cbmm.com/pt/privacy-policy/direitos-dos-titulares anyone, from employees to third parties, can noy only make request regarding their Personal Data, but also inform the occurrence of an Information Security Incident.

Incidents that involve Personal Data may be identified from the dealings of an Information Security Incident and/or registered directly through request in ITSM tool.

In the event of an Information Security Incident involving Personal Data, the DPO will notify the Data Protection Authority and the Data Subjects according to the applicable laws.

11. LIABILITY

All CBMM's Entities accept liability for any breaches of the Corporate Rules as if the violation was caused by any Company activity. CBMM Entities may not rely on a breach of a Processor or Sub-processor that is under obligation to comply with these rules to avoid their own liability.

11.1. Conflicts of law

Whenever CBMM Entities have reason to believe that applicable laws (i) prevent CBMM Entities from complying with its obligations under the Corporate

Rules; (ii) have a substantial impact on the guarantees provided by the Corporate Rules, CBMM Entities will report such conflict to the competent authority.

If CBMM Entities are prevented from disclosing such conflict, CBMM Entities will use commercially reasonable efforts to obtain a right to surpass such prohibition and provide as much Information as possible to the competent authority.

If, despite having used its best efforts, the CBMM Entity is not authorized to notify the competent authority, it shall, on an annual basis, publish general Information on the requests received.

CBMM Entities shall ensure that any disclosure made to competent authorities in response to a request are made in accordance with applicable data protection laws.

12. REVISION OF THE CORPORATE RULES

CBMM reserves the right to review and modify its Corporate Rules at its discretion, however at least within a two (2) year term.

Changes to the Corporate Rules shall be applicable to all existing CBMM Entities on the effective date of implementation.

All changes to the Corporate Rules, when relevant, will be reported to the ANPD as soon as such Authority starts analyzing and approving corporate documents.

13. EXHIBITS

EXHIBIT 1

List of CBMM Entities and their contact information

CBMM INTERNATIONAL BV
WTC H-Tower - Zuidplein 96 / 1077 XV
Amsterdam, Netherlands
Phone: +31 (0) 20 881-3140

CBMM BRASIL AND SOUTH AMERICA
Avenida Brigadeiro Faria Lima, 4285, 9º andar
São Paulo, SP, Brasil 04538-133
Phone: +55 (11) 3371-9222 ou +55 (11) 2107-9222
Fax: +55 (11) 3845-2090

Córrego da Mata, s/n
Araxá, Minas Gerais, Brasil 38183-903
Phone: +55 (34) 3669-3000/3201-4500
Fax: +55 (34) 3669-3100

CBMM ASIA
10 Collyer Quay #26-10 Ocean Financial Centre
Singapore 049315
Phone: +65 6303-0290
Fax: +65 6303-0299

CBMM Europe BV
WTC H-Tower - Zuidplein 96 / 1077 XV
Amsterdam, Netherlands
Phone: +31 (0) 20 881-3140

CBMM North America, Inc.
1000 Omega Drive, Suite 1110
Pittsburgh, PA 15205 USA
Phone: +1 (412) 221-7008

CBMM Technology Suisse SA
Avenue Pictet-de-Rochemont, 8
1207 Geneve
Switzerland
Phone: +41 22 318-4050

EXHIBIT 2

Glossary

ANPD: Brazilian Data Protection Authority.

Availability: ensure that authorized personnel have access to the Information whenever needed.

CBMM: Companhia Brasileira de Metalurgia e Mineração.

CBMM Entities: CBMM and its subsidiaries listed in EXHIBIT 1.

Company: Any CBMM Entity referred to individually.

Confidentiality: ensure that the access to Information is obtained solely by authorized personnel and when it is indeed required.

Controller: Individual responsible for making decisions on the Processing of Personal Data.

Data Protection Authority: an independent public authority which is established by a State as the competent authority to issues regarding Data Protection.

Data Subject: Individual who the Personal Data refers to.

DPIA: Data Protection Impact Assessment.

DPO: Person responsible for the Protection of Personal Data in the Company and for communication with the ANPD and the Data Subjects.

Information: data, whether or not processed, that could be used for production and transmission of knowledge, contained in any means, support, or format.

Information Security: protection of Information in all forms (electronic, physical, verbal, digital media) against several types of Threats to ensure continuity of the business, aiming to preserve the Confidentiality, Integrity, and Availability of the Company Information.

Information Security Incident: event that causes or may cause interruption, reduction and/or adverse effects to the Confidentiality, Integrity, and Availability of the systems, services, Personal Data, and IT assets of CBMM**.**

Integrity: ensure the accuracy and completeness of the Information and the Processing methods, as well as the transparency while dealing with the appropriate audience.

Personal Data: Any Information related to a Data Subject. Identifiable means an individual that may be identified, directly or indirectly, specially through and identifier such as name, id number, location data, electronic means identifier or one or more specific elements of physical, physiological, genetic, mental, economic, cultural, or social identity of this person.

Processor: Individual who performs the Processing of Personal Data on behalf of Controller.

Privacy: Protection and Privacy of Personal Data.

Privacy Commission: Collegiate body composed of members of different departments of the company and in charge of discussions regarding Privacy issues and Processing activities.

Privacy Incident: Any adverse event, confirmed, or suspected, potential or effective, related to violation of security of Personal Data that imply or may imply in loss of Confidentiality, Availability or Integrity of Personal Data such as, but not limited to, non-authorized, accidental or illegal access that cause destruction, loss, change, disclosure or else any improper or illicit processing of personal data that may give rise to risks for rights and freedom of the Data Subject.

Privacy Office: Multidisciplinary body focused on support the DPO performing his attributions.

Privacy Portal: Privacy management tool.

Processing: Any operation carried out with Personal Data, by automate means or otherwise, such as the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation, or Information control, modification, communication, transfer, diffusion, or extraction.

Sensitive Personal Data: According to the scope of each legislation, several categories of data may be considered as Sensitive Personal Data. The following categories could be deemed as Sensitive Personal Data in some of CBMM's applicable jurisdictions:

- Racial or ethnic origin;
- Political opinions;
- Religious or philosophical beliefs;
- Membership in unions, commercial or professional association;
- Genetic data;
- Biometric data for purposes of identifying a specific individual or biometric models;
- Health data/medical Information;
- Financial Information;
- Gender identity or sexual orientation of an individual
- Government id card or id number;
- Passwords
- Criminal conviction or registry of an individual
- Information on social security measures

Users: registered (user) in the CBMM computer network to access the Information system and computing resources of CBMM