CORPORATE POLICIES

PERSONAL DATA PROCESSING AND PROTECTION POLICY

Present Personal Data Processing and Protection Policy (the "Policy") of companies CI PRODECO S.A., CONSORCIO MINERO UNIDO S.A., CARBONES DE LA JAGUA S.A., CARBONES EL TESORO S.A. and SOCIEDAD PORTUARIA PUERTO NUEVO S.A. members of the PRODECO GROUP, as well as the foundations constituted by those (the "Entities"), establishes the criteria that must be applied in the Processing and Protection of Personal Data, in activities such as the collection, storage, use, circulation, and deletion, and in general all those activities implied in the Processing of Personal Data, in compliance of stipulations of Law 1581 of 2012 and the regulations that modify or regulate such law.

Some of the requirements set forth in this Policy may also apply to third-party service providers and other contractual partners and must therefore be considered when drafting and approving contracts with such third parties.

1. Objective

Present Policy establishes the guidelines under which the Entities will carry out the Processing of Personal Data and its protection, as well as the objectives of such Processing, the rights of the Data Subjects of Personal Data, as well as the procedures to answer consultations, complaints and claims presented to such Companies, associated with the mentioned Processing.

As indicated in the Code of Conduct, as a part of Prodeco Group's Corporate Practice, we have made a commitment to only collecting and retaining personal information that is reasonably necessary to meet business requirements and as permitted by the applicable local laws and regulations of Colombia.

2. Definitions

The following definitions are terms that are stipulated in the law and that should be considered when applying present Policy:

a. Authorization: Previous, express and informed approval by the Data Subject in order to carry out the Processing of Personal Data.

b. Chief Data Protection Officer (CDPO): The Chief Data Protection Officer of Prodeco Group – whose contact details are set out in the section 11.1. below.

c. Database: Organized set of Personal Data that will be subject to Processing.

d. Data Controller: Individual or legal entity, public or private, which by itself or in association with others, makes decisions regarding the database and/or Processing of the Data.

e. Data Processor: Individual or legal entity, public or private, that by itself or in association with others, Processes the Personal Data on behalf of the Data Controller.

f. Data Subject: Employees, suppliers, contractors, customers or any individual whose Personal Data will be subject to Processing by the Entities.

g. Data Protection Contact (DPC): natural person(s) who is/are appointed by the Data Controller as a first point of contact in data protection matters and who is/are in charge with the data protection tasks including the implementation and enforcement of the Policy and the supervision of the Processing of the personal data.

h. Habeas Data: The "Habeas Data" right is the right that every person has of knowing, updating and rectifying the information that has been collected about him in files and public or private Information banks.

i. Personal Data: all information directly or indirectly relating to an identified or identifiable person, in particular with reference to names, telephone numbers, e-mail addresses, location data, etc.

j. Policy: means the most recent edition

of this Personal Data Processing and Protection Policy.

k. Privacy notification: Notification through physical, electronic or any other media generated by the Entities and made available to the Data Subject regarding the Processing of his Personal Data, through which that person is advised of the existence of present Personal Data Processing and Protection Policy, the manner in which he can access such information and the reason why his Personal Data will be processed by the Entities.

l. Private information: The information that due to its intimate or reserved nature is only relevant to the Data Subject.

m. Process, Processed or Processing: Any operation or set of operations associated to Personal Data, such as the collection, storage, organization, use, cleaning, analysis, circulation, transmission, transfer, update, amendment or deletion of same.

n. Prodeco Group: Group of Companies comprised by: C.I. Prodeco S.A., Carbones de la Jagua S.A., Consorcio Minero Unido S.A., Carbones El Tesoro S.A. and Sociedad Portuaria Puerto Nuevo S.A.

o. Public information: The information qualified as such as per stipulations of the law or of the Political Constitution, which is not semi-private, private or sensible. It is considered that public information is information associated to the marital status of the persons, their profession or position, their quality of merchants or public officials, to name a few, and those that can be obtained without any reservation, due to their nature the public information may be contained in, among others, public records, public documents, gazettes, official bulletins and judicial sentences duly executed and not subject to reserve.

p. Semiprivate information: The one that does not have an intimate, reserved or public nature and whose knowledge or dissemination could be of interest not only for the Data Subject but for certain sector of people, or of the society in general, such as financial or credit information.

q. Sensible information: It is understood that sensible information is the one that affects the intimacy of the Data Subject or whose undue use could generate discrimination and/or affect that person's integrity, such as those that reveal the racial or ethnic origin, the political orientation, religious or philosophical convictions, social security measures and information, administrative or criminal proceedings and sanctions, the membership to unions or social and human rights organizations that promote the interests of any political party or which guarantee the rights and guarantees of political parties, as well as information regarding the health, the sexual behavior, the source of their resources or assets, biometric information, profiling data, in particular resulting from the automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to a natural person, and others. This information will not be processed by the Entities, unless its Processing is authorized by law and the Authorization for its use has been obtained, by informing the Data Subject that he is not under the obligation of authorizing its Processing and which part of the information is sensible, as well as the objective of the Processing.

3. Data Processing Principles

In compliance of stipulations in the Law, the Entities carry out the Processing of Personal Data, respecting the following general principles:

a. Lawfully Processed: Personal Data Processing is a regulated activity that must be subject to stipulations of Law 1581 of 2012 and all other stipulations that develop it or regulate it, including this Policy. In the case of Sensitive Data, a higher standard of diligence is required to Process such data. Data Controllers shall be sole responsible for complying with and enforcing the applicable data protection legislations.

b. Objectivity: The Processing of Personal Data collected must obey a legitimate objective, in accordance to the Constitution and the Law, and must be informed to the Data Subject.

c. Freedom: The Processing can only be carried out with the previous, expressed and informed consent by the Data Subject. The Personal Data cannot be obtai-

ned or disseminated without previous authorization or if there is lack of legal or judicial mandate that replaces the consent.

d. Accurate and kept up to date: The information subject to Processing must be truthful, complete, exact, verifiable and comprehensible. The Processing of partial, incomplete, fractioned or misleading information will not be carried out.

e. Transparency: The Processing must guarantee the right of the Data Subject to obtain from the Entities, at any moment and without restriction, information regarding the existence of the information that concerns him. The Data Controller shall provide the Data Subject with all information about the processing of his or her Personal Data no later than at the time of collection of such Personal Data. The Data Subject shall be informed of the (i) Processed or the categories of the Processed Personal Data and the (ii) purpose(s) for which the Personal Data is intended to be Processed (unless such is apparent based on the circumstances or the Data Subject already disposes of such information). Further, the Data Subject must be informed about the identity of the Data Controller and its contact details, third parties or categories of third parties to whom the Personal Data may be transmitted to and whether these third parties area located abroad.

f. Access and restricted circulation: Information Processing is subject to the limits that are derived from the nature of the Personal Data, as well as the stipulations of the Law. In this sense, the Personal Data, except the public information and the stipulations of the authorization granted by the information Data Subject, cannot be made available in Internet or other dissemination or massive communication media, except if the access is technically controllable to provide restricted knowledge only to the Data Subjects or third authorized parties.

g. Security: The information subject to Processing by the Entities must be processed under the technical, human and administrative means, which are necessary to grant security to the records, avoiding their alteration, loss, consultation, use or non-authorized or fraudulent access.

h. Confidentiality: All the persons that intervene in the Processing of Personal Data that does not have the classification of public nature are under the obligation of guaranteeing the secrecy and confidentiality of the information, even after concluding their association with some of the work comprised by the Processing, and they can only supply or communicate the Personal Data when it entails the development of activities authorized by Law, and in accordance with the stipulations of the Information Security Policy implemented by the Entities.

i. Adequate, relevant and not excessive: Relevant Personal Data shall be processed in an adequate and non-excessive manner. This also implies that it is not acceptable to hold Personal Data on the basis that it might possibly be useful in the future. Personal Data should also be disposed of or deleted once the purpose for which it has been held is completed, unless applicable mandatory laws foresee a longer period of retention.

j. Data Protection by design and by default: The Data Controller must conduct a data protection assessment if the Processing is expected to lead to an increased risk for the Data Subject's privacy and other rights. Appropriate measures in order to mitigate the risk of data protection breaches must be taken from the time the Processing is planned (data protection by design); furthermore, it must be ensured that only personal data which is necessary for specific purposes of the Processing is Processed (data protection by default).

4. Data Subject Rights

The Entities, during the Processing of Personal Data will ensure compliance of the following Data Subjects' rights:

a. Knowledge, update and rectification of their Personal Data within the Entities as Data Controller and the Data Processors. This right can be exercised with regards to, among others, partial, inexact, incomplete, fractioned, or misleading information, or information whose Processing is expressly prohibited or that has not been authorized by the Data Subject.

b. Request proof of the Authorization granted to the Entities, except when expressly excluded in the law as a requirement for the Processing, in accordance to stipulations of Article 10 of Law 1581 of 2012 or of the regulations that modify, update, add, regulate or repeal this law,

or whenever there is continuity of the Processing in accordance with Article 10, numeral 4th of Decree 1377 of 2013.

c. Be informed by the Entities as Data Controller or by the Data Processor, upon request, regarding the use given to its Personal Data.

d. Present to the Industry and Commerce Superintendence complaints due to violations of stipulations of Law 1581 of 2012 and all the other regulations that modify, add or complement it, in accordance with section 7.4 of present Policy.

a. Annul the Authorization and/or request the removal of the Personal Data when the Processing does not respect the principles, the rights and constitutional and legal guarantees. The repeal and/or removal will proceed whenever the Industry and Commerce Superintendence has established that within the Process the Data Controller or Data Processor has incurred in conducts contrary to the law and the constitution.

The request for removal of the information and annulment of Authorization will not proceed when the Data Subject has a legal or contractual duty of remaining in the Database and/or the Data Controller has the legal or contractual duty of continuing with the Processing.

e. Access, without any charge, his Personal Data that has been the object of Processing.

f. Request information about his or her Personal Data processed by the Data Controller, and in particular about the envisaged period of storage of the Personal Data or the relevant criteria used to determine such period.

All right of access request by Data Subjects must be communicated to the CDPO.

All complaints related to this Policy received from employees, governments, regulatory bodies or business partners must be communicated to the CDPO.

5. Duties of the Data Controller and Data Processor of Personal Data

5.1. Duties of the Entities as Data Controller for Processing Personal Data:

The Entities, as Data Controller for the Processing, must comply the following duties, without prejudice of all the other stipulations included in the law and in other stipulations that govern its activity:

a. Guarantee to the Data Subject, at all times, the full and effective exercise of his habeas data rights.

b. Request and keep, under the conditions stipulated in the law, the corresponding Authorization granted by the Data Subject.

c. Report on the objective of the collection and the rights to which he is entitled by virtue of the Authorization granted.

d. Preserve the information under the security conditions necessary to prevent its falsification, loss, consultation, or non-authorized or fraudulent use or access.

e. Guarantee that the information provided to the Data Processor is truthful, complete, exact, updated, verifiable and comprehensible.

f. Update the information, timely advising the Data Processor, of all the changes with respect to the information that has been previously supplied and adopt the measures necessary so that all the information supplied is kept updated.

g. Amend the information when it is incorrect and communicate the corresponding matter to the Data Processor.

h. Supply the Data Processor, whichever is the case, only Data whose Processing is previously authorized in accordance with stipulations of the law.

i. Demand the Data Processor, to respect the conditions of security and privacy of Data Subject's information.

j. Process the requests and claims presented under the terms stipulated by law, with regards to the Processing of Personal Data.

k. Inform the Data Processor whenever certain information is under discussion by the Data Subject, once the claim has been presented and if the corresponding procedure is not finished.

l. Inform the Data Subject, at his request, regarding the use given to his Personal Data.

m. Inform the Information protection authorities whenever there are infringements of the security codes and whenever there are risks in managing Data Subjects' Information, with regards to Processing of Personal Data.

n. Comply the instructions and requirements issued by the Industry and Commerce Superintendence or by any other authorities legally empowered in this respect, regarding the Processing of Personal Data.

5.2. Duties of Data Processor of Personal Data:

Data Processor of Personal Data must comply the following duties, without prejudice of all other stipulations established in the law and in any other regulation that governs such activity:

a. Guarantee to the Data Subjects, at all times, the full and effective exercise of their habeas data rights.

b. Preserve the information under the necessary security conditions to prevent its adulteration, loss, consultation, non-authorized or fraudulent use or access.

c. Timely carry out the update, rectification or deletion of the Information under the terms of the law.

d. Update the information reported by the Data Controller, within five (5) business days as of the date of receipt.

e. Process the consultations, complaints and claims presented by the Data Subjects under the terms stipulated by law.

f. Record in the database the legend "information in judicial discussion" once he receives notification by the competent authority regarding judicial processes associated with Personal Data.

g. Abstain from disseminating information that is being controverted by the Data Subject and whose blockage has been ordered by the Industry and Commerce Superintendence.

h. Allow access to the information only to the persons that are authorized to have access to such information, in accordance to present Policy and the law.

i. Inform the Industry and Commerce Superintendence whenever there are violations to the security codes and whenever there are risk in the administration of Data Subjects' information.

j. Comply the instructions and requirements issued by the Industry and Commerce Superintendence associated with the Processing of Personal Data.

5.3. Duties of the Entities associated with the Processing of Personal Data of children and adolescents:

The Entities will abstain from Processing Children's and Adolescent's Personal Data, except for the information that is of public nature, and in this respect, in any case, will request the children's or adolescents' legal representative their authorization to Process the Information and such Process will comply with the following parameters and requirements:

1. Will respond and respect children and adolescents' superior interest.

2. Will make sure to respect their fundamental rights.

6. General purposes of Personal Data Processing

The Processing of Data Subjects' Personal Data has the following purposes:

a. Generate and maintain an efficient and adequate communication of the information that is of use in the contracting relationships in which the information Data Subject is a party;

b. Perform the existing contractual relationship with his customers, suppliers, contractors and employees, including compliance of contractual obligations, such as payment;

c. Provide the products required by its customers;

d. Obtain the products and services that the Data Subjects require, as well as to inform himself about new products or services and/or changes on same;

e. Develop the process of labor selection, evaluation, contract and termination;

f. Generate and keep supports required by the internal and external audit processes;

g. Record employees and/or retired employees (active and inactive) information in Company's databases;

h. Develop investment projects or community support projects, in a direct manner or in alliance with third parties and/or government institutions and/or regarding the compliance of the legal requirements resulting from mining, transportation or port activities, associated to Company's social objective.

i. Supply, share, send or deliver Data Subject's Personal Data to Prodeco Group's affiliated, related or subordinated companies or of the same corporate group, located in Colombia or in any other country in case such companies require the information for the objectives herein indicated. In this respect will comply with all the legal stipulations in matters of transfer of Personal Data;

j. Manage all the information necessary to comply Tax obligations and Company's commercial, corporate and accounting records;

k. Comply with Companies' internal processes in matters of managing customers, employees, suppliers and/or contractors;

l. For the file and update of Company internal information databases processes;

m. Disseminate internal amendments of any type that arise in the development of contractual relations with Information Data Subject;

n. Evaluate and examine the quality of services offered by the Information Data Subject;

o. Send through a safe media the information that in association with contingency topics must be sent for information system's back-up in Colombia or other countries;

p. Transmit the Information that the national government and/or authorities require in the compliance of legal stipulations;

q. Send whatever amendment is implemented in the Processing and Processing of Personal Data Policy adopted by the Entities;

r. Any other administrative, commercial, and advertisement transactions and any other objectives indicated in the authorization granted by the Information Data Subject or described in the corresponding privacy notification, whichever is the case.

Additionally, regarding the Processing of Personal Data of Company employees and ex-employees, besides the objectives previously mentioned and, if necessary, the Processing will have the objective required in the labor field and eventually the information will be shared with other institutions, whenever this is necessary to comply with the corresponding legal stipulations.

With respect to the Information (i) collected directly in the security points; (ii) taken from the documents that are supplied by the security personnel; and (iii) obtained from video recordings that are carried out inside or outside Company facilities, they will be used for the security of people and Company assets and facilities and can be used as an evidence of any type of process.

The information regarding Personal Data provided to the Entities will be used only for the purposes therein indicated and therefore the Entities will not sell, license, transmit or disseminate such information, except if: (i) there is an express authorization to do so: (ii) it is necessary to allow contractors, suppliers or agents to provide the entrusted services; (iii) is necessary in order to supply our products; (iv) the information is associated with Company's merger, consolidation, acquisition, divestment, or any other restructuring process; (v) that is required or permitted by the corresponding legal stipulations.

7. Procedures

Below we establish the general guidelines of the Authorization, Consultation and Claims and Deletion of Information processes, as well as Annulment of Authorization and Complaints with the Industry and Commerce Superintendence.

7.1. Authorization

The Processing of Personal Data by the Entities will require the previous and express authorization from the Data Subject and the same must be obtained

from such Data Subject before collecting the Personal Data, in the following manners: (i) oral; (ii) written; (iii) through clear behavior of the information Data Subject that will reasonably allow reaching the conclusion that he granted the authorization. In spite of the above, the mere silence of the Information Data Subject with regards to the Authorization cannot be assimilated as a clear conduct of having granted the corresponding Authorization.

When requesting the Authorization, the following points must be informed to the Information Data Subject:

a. The Process to which his Personal Data will be submitted to and the objective of same if they are different to the ones established in present policy.

b. Data Subject's option to provide a response to the questions presented, when they refer to Sensible Information whose Processing is allowed by law or when dealing with children's or adolescents' Public Information.

c. The rights that he has as Data Subject.

d. The identification, physical or electronic address and telephone number of the Data Controller.

Data Subject's authorization will not be necessary when dealing with:

a. Information required by a public or administrative institution exercising its legal duties or under a judicial order.

b. Information of public nature.

c. Medical or sanitary emergency situations.

d. Processing of information authorized by law for historical, statistical or scientific objectives.

e. Information associated with People's Civil Registry.

7.2. Consultations and Claims

The Data Subjects can present petitions, consultations or claims and become familiar with, update, rectify or delete information and annul the Authorization granted or request proof of same and in general exercise their rights. In this respect the Entities have provided the contact details of the Chief Data Protection Officer in the section 11.1. below, in order to address such petitions, consultations or claims.

7.2.1. Consultations

The Data Subjects or their heirs can consult Data Subject's Personal Data that is filed in any Information base whenever its Processing is Companies' responsibility, through the channels established in section 11.

7.2.2. Claims

The Data Subjects or their heirs that consider that the information contained in a database should be corrected, updated or deleted, or whenever they realize that there is an alleged non-compliance of the duties stipulated in the law, can present a claim to the Entities through the channels established in section 11.

7.2.2.1. Requirements to present claims

a. Must prepare the claim addressed to the Data Controller or Data Processor of Personal Data.

b. It must indicate Data Subject's identification document number.

c. Include the description of the facts that resulted in the claim.

d. Indicate the physical address or electronic mail where he can be contacted.

e. Attach the documents required to support the claim.

7.2.2.2. If the claim is incomplete

Will contact the interested party within five (5) business days following receipt of the claim, asking him to solve the failures or complete the information required to process the claim. If after two (2) months as of the date of sending the communication asking for clarification or completion of the claim, the interested party does not present the required information, it will be understood that he has abandoned the claim.

7.2.2.3. If the claim is complete

Once the claim is received and at the latest two (2) business days after having received it, it will be included in the database with a legend that should say "claim being processed" and the reason. Such legend must remain valid until the claim is resolved.

7.2.2.4. Term

The maximum term to respond to the claim will be fifteen (15) business days as of the date following its receipt, except in cases foreseen in section 7.2.2.2, in which such term will start as of the date following the date of receipt of the information required. When it is not possible to solve the claim within such term, will inform the interested party the reasons for the delay and the date in which the claim will be resolved, but under no circumstance can this term be more than eight (8) business day following the expiration of the first term.

7.3. Deletion of Information and/or annulment of authorization

When the Data Subject requests deletion of the information and/or annuls the Authorization, this request cannot be processed when:

a. It is a legal or contractual obligation or right of the Entities to process and/or preserve such Information.
b. To maintain the Information is essential to safeguard Data Subject's interest or the public interest.

c. To maintain the Information is essential to carry out the contractual or labor relationship with the Data Subject, as long as the information is necessary for such execution and the information is not Sensible Information.

d. The deletion impedes or hinders the exercise of the duties of the administrative or judicial authorities.

In case the authorization annulment request is applicable, it is necessary that the interested party reports precisely whether the annulment is total or partial. The authorization annulment is partial when the interested party advised that he wishes to annul the Processing of his Personal Data for certain specific objectives, such as advertisement, competitions, consumer surveys, etc. The annulment of the authorization will be total when the Data Subject requests to stop the Processing of his Personal Data for all the objectives authorized.

7.4. Complaints presented to the Industry and Commerce Superintendence

Once the consultation or claim process has been concluded with the Prodeco Group Companies according to stipulations in section 7.2, the Data Subject or successor can present a claim with the Industry and Commerce Superintendence if he does not agree with the results of the process carried out with the Entities.

7.5. Requirements from the authorities

The Entities, its authorized, assigned, licensed, affiliated and/or subordinate companies will cooperate with the competent authorities to guarantee compliance of the laws in matters of protection of the industrial property, copyrights, fraud prevention and other matters.

With the granting of the Authorization, it is understood that the Data Subjects expressly authorize the Entities to supply any Personal Data about them to the competent authorities, in order to comply any requirement of such authorities and in order to cooperate with them as they discretionally understand that it is necessary and adequate in regards to any investigation of an illicit fact, or infringement of the regulations of Consumer Statute, infringement of copyright or industrial property rights, or any other activity that is illegal or that could expose the Entities or its authorized, assigned, licensed, affiliated and/or subordinate companies, to any legal responsibility. Besides, it will be understood that the Data Subjects authorize the Entities to communicate their Personal Data to competent authorities with regards to this or other investigations that they carry out.

8. Security of the information

In developing the principle of security established in Law 1581 of 2012, the Prodeco Group will adopt the technical, human and administrative measures that are necessary to grant security to the records, avoiding their alteration, loss, consultation, non-authorized or fraudulent use or access. The personnel that carries out the Processing of Personal Data will carry out the protocols established in order to guarantee security of the information.

9. Privacy notification

Whenever it is not possible to provide the Personal Data Processing and Protection Policy to the Data Subject, the Entities will inform the Data Subject of the existence of this policy and the manner of having access to same through a Privacy Notification, through the mechanisms allowed by law in this respect, in a timely manner and in any case at the latest at the

moment of collecting the Personal Data. The text of the Privacy Notification must include the contents required by Article 15 of Decree 1377 of 2013 and copy of such notification must be kept for later consultation by the Data Subject and/or the Industry and Commerce Superintendence, if needed.

10. Data Controller of the Processing of Personal Data

The Data Controller for each specific case will be any one of the Entities that Process the information of the Data Subject. Below we present the information of each one of the Entities:

Company Name	Address	Email	Telephone
C.I. Prodeco S.A. Carbones de la Jagua S.A. Consorcio Minero Unido S.A. Sociedad Portuaria Puerto Nuevo S.A. Fundación Calenturitas Fundación La Jagua Fundación Prodeco	Calle 77 B No. 59 – 61 Piso 4 Centro Empresarial Las Américas II	protecciondedatos@grupoprodeco.com.co	+57 (5) 3695500 Ext. 5449.

11. Chief Data Protection Officer

11.1. Contact Details of Chief Data Protection Officer of Prodeco Group

Chief Data Protection Officer (CDPO)
Prodeco Group
Calle 77 B No. 59 – 61, Piso 4
Centro Empresarial Las Américas II
Barranquilla, Atlántico
E-Mail: protecciondedatos@grupoprodeco.com.co
Phone: +57 5 3695449

11.2. Appointment of Internal Data Protection Contacts

Each Data Controller shall designate a DPC. Several Data Controllers may appoint a single DPC provided that he or she is easily accessible from each establishment.

The DPC shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the data protection task. The contact details of the DPC shall be communicated to the employees and, if required by local law, to the relevant supervisory authorities.

The DPC shall be involved, properly and in a timely manner, in all issues which relate to the protection of Personal Data. He or she shall independently monitor internal compliance with data protection regulations and this Policy, and in particular (i) audit the Processing of Personal Data and recommend corrective measure if infringement have been ascertained and (ii) maintain a list of the data files.

The DPC shall carry out his or her duties independently and without instructions from the Data Controller. The Data Controller shall ensure that the DPC has the resources necessary to carry out his or her tasks, has access to all data files and data Processing operations and to all information necessary to fulfil his or her duties and maintain his or her expert knowledge.

The DPC regularly reports to the CDPO.

12. Update and Validity

The Entities reserve the faculty of reviewing this Policy at any moment. In such case will publish any change to this Policy in the site or web pages that are provided in this respect. Whenever substantial changes are made to this Policy, this fact will be communicated to the Data Subjects by sending a notification to the electronic mail that they have registered, before or at the latest at the moment of implementing them, advising them that they will be able to consult the new policy at the site where they are available. Such notification will indicate the date in which the new policy will be valid. When the change refers to the objectives of the Processing, will request a new Authorization from the Data Subjects. Present Policy will become valid as of

April 09th 2018 and the database will be valid for the reasonable and necessary time, in accordance with the objectives of data Processing. In spite of the above, the Personal Data must be kept whenever it is necessary to comply the stipulated legal and contractual compliance.

RECORD OF CHANGE

Code	Version	Modification date	Description
GPR-PGP-POL-0001	02	2018-04-09	Translation fixes Alignment with the Glencore's Data Protection policy: ▪ Include the DPC definition. ▪ Include the "social security measures and information", and the "profiling data" as a Sensitive Personal Data. ▪ Add to the existing Lawfully Processed principle information about the higher standard of diligences to process such data. ▪ Add to the existing Transparency principle details about the information that the Data Controller shall prove to the Data Subject. ▪ Include the "Adequate, relevant and not excessive" principle. ▪ Include the "Data Protection by design and by default" principle. ▪ Include to the "Right of Access Request and Complaints" the following subjects: o The envisaged period of storage of the Personal Data or the relevant criteria used to determine such period. o All right access requests by Data Subjects must be communicated to the CDPO.

Mark McManus
CEO