Policy Name	PERSONAL DATA TREATMENT POLICY	Code	Version
		GRC-PC-42	4
Person Responsible	VICE PRESIDENT OF CORPORATE AFFAIRS	Effective since	
Type of Document	BUSINESS GENERAL	october/16	

I. MAIN GOAL

Establish guidelines and general criteria for the management of personal data of employees, customers and suppliers of Corona Industrial S.A.S. (From now on simply "Corona Industrial"), its subsidiaries and subordinates companies.

II. SCOPE

This policy applies to Corona Industrial S.A.S. (From now on simply "Corona Industrial"), its subsidiaries and subordinate companies in Colombia. In the sections of this document in which the word Corona is expressed, it should be understood that refers to any of the companies mentioned above.

III. REGULATORY RAMEWORK

Listed below are the regulations related to the protection of personal data:

- Law 1266 of 2008
- Law 1581 of 2012
- Decree 1377 2013
- Decree 1074, May 26, 2015 (Partial Regulation of Law 158).
  - Circular 02 , November the 3 th 2015 (addition to Chapter 2, title V of the Circular Only of the SIC.
- Decree 886 of 2014 - Regulation of the Article 25 of the Law 1581: National Register of Databases.

IV. APPLICATION SCOPE

Personal data recorded in any database, that makes them susceptible to treatment by entities of public or private, carried out in Colombian territory or in countries where applicable the Colombian legislation.

V. DEFINITIONS

Actors of the treatment of personal data: They are companies or persons who carry out the supply, collection and treatment of personal data, these are:

- **"Responsible for Treatment":** public or private, natural or legal person which by itself or in association with others, decides on the database and/or the processing of the data.

- **"Treatment Manager":** public or private, natural or legal person who by itself or in association with others, performs the Personal Data Treatment on behalf of the Responsible of the Personal Data Treatment.

- **"Information Operator":** it is referred as Information Operator to the person, entity or organization that receives from the source of personal data on several holders of information, manages them and brings to the attention of the users. Operator, as soon as this have access to personal information of third parties, must ensure the protection of the rights of data owner. Unless the operator is the same source of information, this has no commercial or service relationship with the owner, therefore it is not responsible for the quality of the data supplied by the source.

- **"Holder of personal data":** natural person whose personal data are the subject of Treatment.

- **"Assignee":** person who other rights have been transferred.

- **"Source of information":** This is the person, entity or organization that receives or meets personal data from the holders of the information, as a result of a business relationship or service and which, by reason of legal authorization, or from the holder, provided those data to an information operator. The information operator, in turn, will provide personal data to the end user. If the source delivers information directly to users and not through an operator, this will have the double condition of source and operator and will assume the duties and responsibilities of both. The source of the information is responsible for the quality of the data supplied to the operator and must ensure the protection of the rights of the data owner.

- **"Data Manager**": The collaborator of Corona that treats personal data.

- **"External Data Manager":** It is the employee of a third party (Manager) who performs the treatment to the databases delivered by Corona for the accomplishment of the treatment.

- **"User":** The natural or legal person who can access to personal information of one or more holders of the information provided by the operator or by the source, or directly by the owner of the information. The user must ensure the protection of the rights of the data owner. In the case in which the user in turn give information directly to an operator, this will have the double condition of user and source, and will assume the duties and responsibilities of both.

"Authorization": Prior, express and informed consent of the holder to carry out the Personal Data Treatment.

"Privacy notice": Verbal or written communication generated by the Responsible, addressed to the Owner for the Treatment of his personal data, which informs him about the existence of the Information Processing policies that will be applicable to him, how to access to them and the purposes of the Treatment intended to be given to personal data.

"**BASC":** (Business Alliance for Secure Commerce) This is an international business alliance that promotes safe trade in cooperation with governments and international agencies.

"Database" Organized set of personal data which is subject to treatment.

"COE": Centre of excellence.

"Substantial Changes to a Database": These are those related to the purpose of the database, the Treatment Manager, the channels of attention to the Holder, the classification or types of personal data stored in each database, the information security measures implemented, the Information Treatment Policy and the international transfer and transmission of personal data.

"Channels to exercise rights":_ These are the means of receiving and attending to requests, consultations and claims that the Treatment Responsible and the Treatment Manager must make available to the Information Holders, with the respective contact data, through of which the Holder can exercise his rights to know, update, rectify and delete his personal data contained in databases, as well as revoke the authorization that he has granted for the treatment thereof, when this is possible. These channels must provide at least the possibility for the Holder to exercise his rights through the same medium by which his information was collected, recording the receipt and processing of the respective application.

"Unequivocal conduct": Behavior that allows the reasonable conclusion that the Owner of Personal Data granted the authorization for the treatment of his data.

"Consultation": A process by which the Personal Data Holder may request from Corona Industrial, its subsidiaries and subordinates companies his personal information that is stored in the databases.

"Corona" or "Responsible": Corona Industrial S.A.S., its subsidiaries and subordinates companies that are identified in numeral 8 of Chapter V of this Policy.

"Personal Data": Any information linked or that it can be associated with one or more natural persons determined or determinable.

"Public Data": It is the data that is not semi-private, private or sensitive. They are considered Public Data, inter alia, the data relating to the marital status of people, their profession or trade and their status as a trader or public servant. By its nature, the public data can be contained, among others, in public records, public documents, gazettes and official bulletin and properly ordered judicial rulings which are not subject to reservation.

"Sensitive Data": Sensitive data means those that affect the privacy of the Holder or whose abuse may lead to discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, membership of labor unions, social organizations, human rights organizations or any that promote the interests of any political party or guarantee the rights and guarantees of opposition political parties, as well as health, sexual life and biometric data.

"Security Incident": Refers to the breach of security codes or the loss, or theft and/or unauthorized access of information from a database managed by the Treatment Responsible or by its Manager.

"Claim": Process by which the **O**wners of Personal Data or their assignees may request from Corona Industrial, its affiliated companies and subsidiaries and the updating, rectification, partial or total suppression of information, the proof of authorization or revocation of the same.

"National Register Database (RNBD, in its Spanish acronym)": Public directory of personal databases subject to treatment which operate in the country, managed by the Superintendency of Industry and Commerce (Colombia) and with free consultation for citizens.

"SIC": Superintendency of industry and Commerce.

"Transfer": Data transfer takes place when the Responsible or Manager of the Personal Data Treatment, located in Colombia, sends the information or personal data to a receiver, which in turn is a Treatment Responsible and is located inside or outside the country.

"Transmission": Treatment of personal data that involves the communication of the same inside or outside of Colombia when it is intended to carry out a Treatment by the Manager or the Responsible.

"Personal Data Treatment": Any operation or set of operations on Personal Data, such as collection, storage, consultation, exchange, transfer, use, circulation or deletion.

"USC": Shared Services Unit (in its Spanish acronym).

VI. STANDARDS AND CRITERIA FOR IMPLEMENTATION

The Privacy Committee will define the guidelines for the development and implementation of the Personal Data Protection in Corona.

1. GENERAL PRINCIPLES FOR THE PERSONAL DATA TREATMENT

In the Personal Data Treatment the following principles will be complied:

a) **Principle of Purporse:** The Personal Data Treatment must obey a legitimate purpose that will be informed to the Holder.

b) **Principle of freedom:** The Personal Data Treatment can only be exercised with the prior, express and informed consent of the Holder. Personal Data may not be obtained or disclosed without prior authorization or legal or judicial mandate that relieves the consent of the Holder.

c) **Principle of truth or quality:** The information subject to treatment must be truthful, complete, accurate, updated, verifiable and understandable. Treatment of partial, incomplete, fractional or error-inducing data is prohibited.

d) **Transparency Principle**: The Treatment must guarantee the right of the Holder to obtain from Corona, at any time and without restrictions, information about the existence of data that concern him.

e) **Principle of access and restricted circulation:** Personal Data, except public information, may not be available on the Internet or other means of mass communication, unless access is technically controllable to provide restricted knowledge only to the Holders or third parties authorized by them.

f) **Security Principle**: The information subject to Treatment must be handled with the technical, human and administrative measures necessary to provide security for the records, avoiding their adulteration, loss, consultation, unauthorized or fraudulent access or use.

g) **Confidentiality Principle:** All persons involved in the Data Personal Treatment are obliged to guarantee the reservation of the information, even after the end of their relationship with any of the tasks involved in the treatment.

2. SPECIAL CATEGORIES OF DATA

2.1 Sensitive Data:

The processing of sensitive data is forbidden except when:

a) The Holder has given the explicit authorization to such Treatment, except in cases in which the granting of such authorization is not required by law.

b) The Treatment is necessary to safeguard the Vital interest of the Holder and the Holder is physically or legally incapacitated. In these events, legal representatives must give their authorization.

c) The Treatment is carried out in the course of legitimate activities and with the due guarantees of a foundation, NGO, association or any other non-profit organization whose purpose is political, philosophical, religious or labor union. Provided that it refers to its members or persons who maintain regular contacts for their purpose. In these events, the data cannot be supplied to third parties without the authorization of the Holder.

d) The Treatment refers to data that are necessary for the recognition, exercise or defense of a right in a judicial process.

e) The Treatment has a historical, statistical or scientific purpose. In this event, measures must be taken to eliminate the identity of the Holders.

2.2 Rights of Children and Adolescents:

The Personal Data Treatment of children and adolescents is prohibited, except in the case of data of a public nature. Areas that by the nature of their management must perform this type of personal data should apply the principles for the protection of the fundamental rights of this type of Personal Data Holders.

3. TREATMENT TO WHAT THE DATA WILL BE SUBJECTED AND THE PURPOSE OF THE SAME

The data will be used by Corona for the development of its corporate purpose and the contractual relationship that links it with the Owner of Personal Data, if any, and in particular for:

a) Develop commercial relationships with third parties. b) Inform about new products or services.
c) Perform statistical treatments of the data.
d) Evaluate the quality of products or services.
e) Develop marketing and promotional activities.
f) Transmit, by means of publication on Corona's website, mail, e-mail, cellular or mobile devices, - via messages (SMS or MMS) -, commercial or promotional information about the products and/or services, events and/or advertisings, in order to promote, invite, manage, execute, inform and, in general, carry out campaigns, promotions or contests.
g) Conduct internal studies on the fulfillment of commercial relationships and market studies.
h) Attend services through Call Center
i) Comply obligations contracted with the Holder.
j) Respond to legal requirements of administrative and judicial entities. k) Execute the employment contract.
l) Guarantee the safety of Corona.
m) Develop training activities.
n) Share, including the transfer and transmission of his personal data to third countries for the purposes related to the operation of Corona, according to the provisions of law and always guaranteeing compliance with the minimum established in the Colombian regulations.

The Responsible person and/or the Treatment Manager will use the data only and exclusively for the purpose that has been informed to the Personal Data Holder. For any reason, misleading or fraudulent means may be used in the Data Treatment, and in cases where the use has been defined as temporary, information may only be used as long as is necessary for the purpose for which it was requested.

4. AUTHORIZATION

The Personal Data Treatment by Corona requires the free, prior, express and informed consent of the Holder. Corona, in its capacity as Manager of the Personal Data Treatment, has had the necessary mechanisms to obtain the authorization of the Holder, his assignee or legitimate representatives.

The authorization may be given by means of a physical or electronic document or any other format that allows to guarantee its subsequent consultation, and that, in addition, can be demonstrated, unequivocally, that the Personal Data Holder: a) has authorized the treatment, b) knows and accepts that Corona will collect and use the information for the purposes that have been informed.

In view of the above, the authorization requested should include:

a) The Responsible for Treatment and what data is collected;
b) The purpose of Data Treatment;
c) The rights of access, correction, updating or suppression of the personal data supplied by

the Holder and,

d) If Sensitive Data is collected.

e) The identification, physical or electronic address and telephone number of the Treatment Responsible.

5. PRIVACY NOTICE

Corona count on the Privacy Notice, which contains the information required by Decree 1377 of 2013, which will be communicated to the Personal Data Holder through the company's communications media. To facilitate disclosure, its content may be included within the authorization.

5.1 Privacy Notice:

In compliance with Law 1581 of 2012 and Decree 1377 of 2013, Corona Industrial S.A.S, its affiliated companies and subsidiaries inform the Personal Data Holder that the data that have been collected or that will be collected in the future will be used only for the purposes that have been communicated to him. Also will be informed that he may exercise his right to submit requests for consultation or claim, request correction, update or suppression, in accordance with the law and the guidelines set in the Data Protection Policy published on the website www.corona.co.

6. RIGHTS AND DUTIES OF HOLDERS

The Personal Data Holder shall have the following rights:

a) Know, update, and correct personal data.
b) Request proof of authorization granted to Corona.
c) To be informed by Corona, upon request, regarding the use given to his Personal Data

d) To present consultations before the Treatment Manager, as established in number 9 of the present policy.
e) Submit to the Superintendency of Industry and Commerce complaints for violations of the provisions of this law and other regulations that modify, add or complement, once exhausted the process of consultation or complaint before the Responsible or the Treatment Manager, according to Article 16 of Decree 1377.
f) Access for free to the Personal Data that is subject to Treatment.

The Personal Data Holder must keep his information updated and guarantee, at all times, the truthfulness of the same. Corona will not be responsible, in any case, for any type of responsibility derived from the inaccuracy of the information provided by the Holder.

7. SAFETY MEASURES

Corona will adopt the technical, human and administrative measures that are necessary to grant security to the registries, avoiding its adulteration, loss, consultation, use or access unauthorized or fraudulent. These measures will respond to the minimum requirements made by current legislation and their effectiveness will be periodically evaluated.

8. TREATMENT RESPONSIBLE

Depending on each particular case, the following companies may be Responsible or Manager of the Personal Data Treatment that they collect through the development of their commercial activity and the following Policy is applicable to them:

Name	Address
Almacenes Corona S.A.S.	AV Cll 26 No 86-85, Bogotá DC.
Compañía Colombiana de Cerámica S.A.S.	Calle 100 No 8ª-55 torre C piso 9, Bogotá DC.
Corlanc S.A.S.	CR 48 No. 72 Sur-01, Sabaneta Antioquia
Corona Industrial S.A.S.	Calle 100 No 8ª-55 torre C piso 9, Bogotá DC.
Despachadora Internacional de Colombia S.A.S.	Carretera Briceño – Sopó, Km 2
Electroporcelana Gamma S.A.S.	CR 49 No. 67 Sur-680, Sabaneta Antioquia
Empresa de Refractarios Colombianos - Erecos S.A.S	Cra 49 No. 67Sur – 680 Sabaneta
Locería Colombiana S.A.S.	CR 54 No. 129 Sur-51, Sabaneta Antioquia
Materiales Industriales SAS	Cra 49 No. 67Sur – 680 Sabaneta
Minerales Industriales S.A.	CR 48 No. 72 Sur-01, Sabaneta Antioquia
Nexentia S.A.S.	CR 48 No. 72 Sur-01, Sabaneta Antioquia
Suministros de Colombia S.A.S.	Cra 48 No. 72 Sur 01, Avenida Las Vegas
Insumos y Agregados de Colombia SAS	CR 49 No. 67 SUR 520
Empresa Colombiana de Cementos SAS	Cr 48 No. 72 Sur 01

Each company may be Responsible and/or Administrator of the collection and/or the Personal Data Treatment, and will keep the Authorization and other records stored, preventing them from deteriorating, losing, altering or being used without authorization.

CONTACT DATA FOR APPLICATIONS FILING:

Information Holders may exercise their rights to revoke authorization for the Data Treatment, to know, update, rectify and delete their Personal Data, by sending communications to the Corporate Information Security Area (Area Corporativa de Seguridad de la Información) in Bogotá, DC, to Calle 100 No 8ª-55 tower C floor 9, telephone 6446500, ext. 10910, or at Sabaneta to Cra 48 No. 72 Sur 01, Avenida Las Vegas, telephone 3787800, ext. 60900, in the name of Area Corporativa de Seguridad de la Información.. Equally, the Information Holders can direct their requests to the e-mail misdatos@corona.com.co.

9. REQUESTS BY THE DATA HOLDER

The responsible for ensuring timely response to requests for consultation or complaint is the Corporate Area of Information Security, headed by the Data Protection Officer, through the channels defined in numeral 8 of Chapter VI of this Policy, through the contact data.

9.1 Consultation

The Personal Data Holders or their assignees may, at any time, consult the personal information contained in the databases of Corona Industrial S.A.S, its affiliated companies and subsidiaries. Likewise, they may request the demonstration of the existence of their authorization for the Personal Data Treatment.

- **Term for Consultation Attention**

In accordance with Law 1581 of 2012, the request for consultation must be attended within a maximum term of ten (10) working days from the date of receipt of the same. When it is not possible to attend the consultation within that term, the interested party will be informed, stating the reasons for the delay and indicating the date of the consultation, which in no case may exceed the five (5) working days following the expiration of the first term.

Note: Corona considers important the timely compliance in the response to requests for consultation made by the Personal Data Holder. Therefore, the company defines in the flowchart incorporated in the Personal Data Treatment Manual GRC-MA-42-01, related in the Annex Chapter of this Policy, internal times for the fulfillment of each step, aiming that the response is delivered to the e-mail or to the address indicated by the Data Holder, at least 2 working days prior to the completion of the 10 working days established by Law 1581 of 2012 as the initial date of expiration; Or to be fulfilled the 5 working days after the first expiration in the case in which for some reason it has been necessary to inform the Personal Data Holder a new date for the delivery of the response.

- **Total internal time for response to Consultation filed before the Personal Data Holder:** 8 working days for the first expiration and 13 working days in total, when, after justification, the first term has been requested to be extended, starting from the date on which the consultation is complete, correct, and has been accepted by the Responsible Manager.

9.1 Claims

The Personal Data Holders or their assignees may request the updating, rectification or deletion of all or part of the data. Likewise, they may request the revocation of the authorization.

- **Revocation of authorization:** The Owner of Personal Data or his assignee may revoke the authorization granted, in accordance with the current regulations.

- **Deletion of Personal Data:** The Data Holder may request the Responsible and/or the Treatment Manager to remove all or part of personal data.

The request for deletion of the information and the revocation of the authorization will not proceed when the Holder has a legal, contractual or commercial duty to remain in the database.

In accordance with Article 16 of Decree 1377, the Holder or assignee may only lodge a complaint to the Superintendency of Industry and Commerce once the consultation process or complaint has been exhausted before the Responsible or the Treatment Manager.

When a claim is received by the Personal Data Holder regarding inconsistencies in the information, or that the data is under discussion, the Treatment Responsible, and when on his behalf the Treatment Manager acts, must suspend the

use of the data for a time not less than the date of completion of the procedure. For this, the Data Manager, responsible for the database, must ensure that there is a record where the following notes are entered: **"pending claim"** or **"information in judicial dispute"**, according to the status of the proceeding claim.

- **Term for the attention of Claims related to Personal Data:**

In accordance with Law 1581 of 2012, when a request for complaint is received by the Personal Data Holder, the Data Manager responsible for Treatment will proceed to review if it contains sufficient information to be answered, and, in the case which requires more information, the Holder will be informed within 5 working days of receipt of the claim to remedy the faults. After two (2) months from the date of the request, without the applicant submitting the required information, it will be understood that the claim has been withdrawn.

Likewise, the Law indicates that the maximum term to attend the claim shall be fifteen (15) working days from the day following the date of receipt. When it is not possible to attend to it within that term, the interested party will be informed, before the expiration of the refered term, the reasons for the delay and the date on which his claim will be dealt with, which in no case may exceed the eight (8) working days following the expiration of the first term.

Note: Corona considers important the compliance in the response to requests for complaint made by the Personal Data Holder. Therefore, the company defines in the flowchart incorporated in the Personal Data Treatment Manual GRC-MA-42-01, related in the Annex Chapter of this Policy, internal times for the fulfillment of each step, aiming that the response is delivered to the e-mail or to the address indicated by the Data Holder, at least 2 working days prior to the completion of the 10 working days established by Law 1581 of 2012 as the initial date of expiration; Or to be fulfilled the 5 working days after the first expiration in the case in which for some reason it has been necessary to inform the Personal Data Holder a new date for the delivery of the response.

- Total internal time for response to **Claims,** filed with the Personal Data Holder: 13 working days for the first expiration and 21 working days in total, when, after justification, it was requested to extend the first term, starting from the date in which the claim is complete, correct, and has been accepted by the Treatment Responsible.

10. ENTRY INTO FORCE, MODIFICATION AND DURATION OF THE DATABASES

This policy applies from the July 27, 2013 and the information provided by the interest groups will remain stored for a period of ten (10) years from the date of the last Treatment, in order to allow Corona to comply with the legal and/or contractual obligations in its care, especially in accounting, fiscal and tax matters.

This policy may be modified at any time and unilaterally by Corona.

11. DATA PROTECTION OFFICER:

The Data Protection Officer is the Policy and Compliance Leader - Information Security.

12. NATIONAL REGISTER OF DATABASES (RNBD, in its Spanish acronym)

The registration process of the databases must be carried out before the Superintendency of Industry and Commerce, according to the definitions of the tool made available by this authority and in compliance with the provisions of Decree 886 of 2014, taking into account, among others, the following aspects:

a) **Registration of existing databases:** This registration should be done within the year following the implementation in operation of the RNBD from the SIC.
b) **Creation of databases:** must be registered within two (2) calendar months, subsequent to its creation.
c) **Update of the information contained in the National Registry of Databases.**
In accordance with External Circular No. 002 of November 3, 2015, the information contained in the RNBD should be updated as follows:

- Within ten (10) business days of each month, upon registration of the database. This in case that substantial changes are made to the recorded information.
- Annually, between January 2 and March 31, starting in 2018.

d) **Security Incidents: Security incidents should be reported to the SIC** through the RNBD within fifteen (15) working days of the time they are detected and brought to the attention of the person or area responsible for servicing them.

VII. ANNEXES

Through the following links you can access related documents: LEG-PC-42-01

Personal Data Processing Manual
GRC-PC-23 Information Security Policy
GRC-PC-29 Information Security Policy - Document Management GRC-PC-68 Information Security Policy for Comprehensive Management GRC-PC-69 Information Security Policy for Third Parties
GRC-PC-70 Physical Information Security and Equipment Policy
GRC-PC-71 Security Policy for the Information Technology Area

General consideration:

The areas or managements that own each process are responsible for ensuring the implementation of the respective corporate policies. Audilimited, in its internal audit role, is responsible for verifying compliance with these policies, in accordance with its annual audit plan and, as well as report the results of its evaluations in its audit reports to both management and the corresponding audit committee.

Prepared	Reviewed	Approved	Version
Sandra Rocío Restrepo Coordinadora de Control Interno	Francisco A. Murcia Abogado Corporativo Senior	Ana María Delgado VP Asuntos Corporativos	V4 Oct 2016
Sandra Rocío Restrepo Coordinadora de Control Interno	Francisco A. Murcia Abogado Corporativo Senior	Ana María Delgado VP Asuntos Corporativos	V3 Abril 2016
Sandra Rocío Restrepo Coordinadora de Control Interno	Francisco A. Murcia Abogado Corporativo Senior	Ana María Delgado VP Asuntos Corporativos	V2 Julio 2015
Andrés Echeverri Abogado Corporativo	Sara Ulloa Contralora Corporativa	Ana María Delgado VP Asuntos Corporativos	V1 Julio 2013