Compliance
Internal Policy

CEMEX Global Data Protection and Privacy Policy

Prepared by	**Raúl Salinas** **Chief Privacy Officer/Compliance Director**
Authorized by	**Roger Saladaña** **Senior VP of Legal**

INDEX

I. Introduction.

CEMEX, S.A.B. de C.V. and its affiliates (hereinafter, "CEMEX" or "we") has grown to become one of the largest companies in the building materials industry. We are present in many markets where we constantly seek to deliver better building solutions to our customers. Our research & development strategy has produced innovative building solutions that are leveraged on technology that has enabled us to satisfy our customer's constant-changing needs. In addition, as a company that embraces innovation, we have changed the way we work by adopting new technologies to help us achieve greater efficiencies, which in turn has enabled us to become more connected not only to our customers, but also to our employees and business partners. Within the organization, information exchange for corporate cooperation, integration and growth has been crucial in pursuing CEMEX's business goals. These connections require personal data to be collected and processed at different levels and for different purposes.

As part of its social responsibility, CEMEX is fully committed to international compliance with data protection laws for protecting personal data of customers, suppliers, business partners and employees. When it comes to accessing, storing and transmitting personal data of our customers, suppliers, business partners and employees, we must ensure that adequate levels of protection and security are in place across CEMEX's worldwide operations. We recognize that the correct and lawful treatment of personal data will maintain confidence in the organization and will provide for successful business operations. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times and is also a key component of CEMEX's overall business strategy, as it lays the foundation for trustworthy business relationships.

II. Purpose.

This CEMEX Global Data Protection and Privacy Policy (this "Policy") lays out what we as CEMEX should do to comply with legal requirements on data protection, as it is based on generally accepted principles on protection of personal data and ensures adequate measures and levels of protection prescribed by the data protection legislation, including the recently enacted European Economic Area's applicable laws.

III. Scope.

This Policy applies to all CEMEX companies worldwide. This Policy applies to all personal data processed by CEMEX regardless of the media on which data is stored or whether it relates to past or present employees, customers, business partners, shareholders, users of CEMEX's websites or any other data subject. All individual CEMEX companies and their employees must ensure compliance with this Policy through appropriate practices, processes, controls and training. Individual companies of the CEMEX Group are not entitled to adopt policies or guidelines that deviate from this Policy.

Although this Policy is based on generally acceptable privacy protection measures prescribed by the laws in the countries where CEMEX operates, national privacy laws may sometimes contain additional/new requirements on activities performed with personal data. In such circumstances, national privacy laws will take precedence in the event that this Policy conflicts with those or when those laws have stricter

requirements than this Policy. In addition, other CEMEX policies governing the use of data, whether personal or not (such as CEMEX's Information Retention Policy and CEMEX's Global Information Security Policy), may supplement the processes and activities related to personal data outlined in this Policy.

This Policy applies to all activities performed for the purpose of processing, accessing or storing personal data. Throughout this Policy, the term **"personal data"** is used to refer to any information identifying a data subject or information relating to a data subject that may be identified (directly or indirectly) from that data alone or in combination with other identifiers CEMEX possess or can reasonably access. Personal data includes **"sensitive personal data"** such as information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions and other information which privacy laws in the countries where CEMEX operate consistently identify as sensitive. Personal data can be factual (for example: a name, email address, location or date of birth) or an opinion about that person's actions or behavior. In addition, the term **"data subject"** in this Policy refers to a living, identified or identifiable individual about whom CEMEX holds personal data.

IV. Personal Data Protection Principles.

We adhere to the following principles relating to processing of personal data:

a. LAWFULNESS.

Processing of personal data must be done lawfully, fairly and in a transparent manner in order to protect the rights of data subjects from whom CEMEX processes personal data. Collection, processing and sharing of personal data should always be based on lawful purposes. This restriction is not intended to prevent processing, but to ensure that we process personal data without adversely affecting the individual data subjects of whom we process personal data. The following list describes common scenarios for processing personal data of customers, suppliers, business partners and employees under lawful bases:

i. Consent. Data can be processed following consent by the data subject. Before giving consent, the data subject must be informed how his/her data is being used and for what purpose. Please keep in mind that if relying on consent alone to process personal data of a data subject in the European Economic Area, rather than assuming that consent was granted implicitly, consent must be granted by the data subject's clear affirmative action and must be properly documented. Where explicit consent is required, the relevant Data Protection Officer (as defined in Section IX.c of this Policy) must advise on the legal requirements for capturing explicit consent. In the case of employees, given the dependency that results from the employer/employee relationship, lawful bases other than consent—such as the necessity to process the data for their legitimate interest or due to a contractual necessity—must be relied on to process personal data.

Unless we can rely on another legal basis of processing, explicit consent is usually required for processing sensitive personal data, for automated decision-making and for cross border data transfers. Nevertheless, processing of sensitive personal data should be kept

to a minimum and its processing should always be tied to a lawful basis. When in doubt about whether collecting or processing sensitive personal data, a CEMEX employee or department must consult with the local Data Protection Officer.

ii. Contractual necessity. Personal data of customers, suppliers, business partners and employees may be processed on the basis that such processing is necessary in order for CEMEX to enter into or perform a contract with them. Before the negotiation phase of a contract, we may face the need to process personal data to evaluate bids or service proposals from business partners or suppliers. In the case of customers, we may need to process personal data to fulfill orders for delivery of our products. Regarding personal data of employees, a CEMEX company will often be in a position where personal data must be processed in order to comply with several obligations under individual and collective employment contracts, such as paying salaries and benefits to its employees. This same lawful basis applies for pensioners.

iii. Legitimate interests. When a data subject contacts us to ask about our products or services, or to receive more information about specific offerings, we may process his/her personal data to be able to provide the requested information about our services or product offerings.

We may also process personal data for market research purposes if we are expecting to deliver services or products and as long as the activity will not affect negatively the data subjects. Please note, however, that data subjects can always object to processing of their personal data and we should honor such request immediately. Please see Section VI for more information on direct marketing activities.

In the case of employee candidates who apply for a job with CEMEX, a legitimate interest for processing personal data may be a reliable lawful basis for processing personal data, when, for instance, checking a business profile of a candidate on social networks that show employment history, education and professional skills in order to be able to assess specific risks regarding such candidate for a specific function. The employee candidate, should, however, be informed about this in the job advert or in person.

iv. Vital interests. While this basis is very limited in its scope, and generally only applies to matters of life and death of data subjects, there may be circumstances where we may have to process personal information on this basis. For example, we may have to process personal data related to medical records of employee candidates to determine if they are fit for performing hard physical/manual labor.

v. Compliance with a legal obligation. There may also be circumstances where we may have to process personal data to comply with the law, such as in tax requirements, criminal investigations or to answer and comply with a court order.

The above are the most common legal bases for processing personal data. If a CEMEX employee comes across a situation where he/she may have to process personal data from data subjects but is unsure on whether such processing is permissible under this Policy, he/she must consult with the Data Protection Officer of the country where he/she works in.

b. FAIRNESS AND TRANSPARENCY.

Information on the identity of the CEMEX company collecting the personal data, as well as on how and why CEMEX will use, process, disclose, protect and retain that personal data must be provided to data subjects when first collecting personal data from them, including for human resources or employment purposes. In general, personal data must be collected directly from the individual concerned rather than from other sources.

c. PURPOSE LIMITATION.

Personal data must only be processed for the purpose that was defined before the data was collected. Collection must be limited to what is strictly necessary for each purpose. Once collected, personal data must not be used for new, different or incompatible purposes from that disclosed when it was first obtained, unless the data subject has been informed of the new purposes and he/she has consented to such new purpose.

d. ACCURACY.

Personal data on file must be correct, complete, and – if necessary – kept up to date. Inaccurate or incomplete data must be deleted, corrected, supplemented or updated. Accuracy of any personal data collected should be reviewed at regular intervals after initial collection.

e. STORAGE LIMITATION.

Personal data must not be retained longer than necessary for the purpose(s) for which it was obtained. In addition, personal data must not be kept in a form which permits the identification of the data subject for longer than needed for the legitimate business purpose or purposes for which CEMEX originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements. Data may be stored for the duration of any kind of liability arising from legal relations or obligations or the execution of a contract or the application of precontractual measures requested by the data subject. The procedures for data retention are defined in the CEMEX Information Retention Policy. [1]

[1] Please note that local/country laws may have different data retention obligations which CEMEX companies are expected to comply with. For a detailed explanation of storage/retention limitations that must be observed related to the different categories of personal data that CEMEX processes, please refer to CEMEX's Information Retention Policy available at: https://www.cemex.com/documents/20143/160082/information-retention-policy.pdf/4338647a-be82-21b8-4043-d60c81f2567b

f. SECURITY, INTEGRITY AND CONFIDENTIALITY.

Appropriate steps must be taken to process personal data in a manner that ensures its security using appropriate technical and organizational measures to protect against unauthorized or unlawful processing and against accidental loss, destruction or damage.

i. Protecting Personal Data.

Personal Data must be secured by appropriate technical and organizational measures against unauthorized or unlawful processing, and against accidental loss, destruction or damage.

Implementing and maintaining safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymization where applicable) is critical for protecting personal data. Before the introduction of new methods of data processing, particularly new information technology (IT) systems, the CEMEX department that will be processing personal data must consult with the relevant Data Protection Officer and CEMEX's Information Security department in order to determine whether the new IT systems offer adequate means for protecting personal data.

Particular care must be exercised in protecting sensitive personal data from loss and unauthorized access, use or disclosure. All procedures put in place to maintain the security of all personal data from the point of collection to the point of destruction must be followed.

Security of personal data must be maintained at all times by protecting the **Confidentiality**, **Integrity** and **Availability** of such personal data. **Confidentiality** means that only people who have a need to know and are authorized to use the personal data can access it. Any unauthorized collection, processing, or use of such data by CEMEX employees is prohibited. CEMEX employees may have access to personal data only as is appropriate for the type and scope of the task in question. Any data processing undertaken by an employee who has not been authorized to carry out such data processing as part of his/her job duties is unauthorized and must be avoided.

Integrity means that personal data is accurate and suitable for the purpose for which it is processed. **Availability** means that authorized users are able to access the personal data when they need it for authorized purposes.

g. TRANSFER LIMITATION.

Personal data collected by a CEMEX company must not be transferred to a different CEMEX company without appropriate protective measures and safeguards being in place.[2]

h. COMPLY WITH DATA SUBJECT'S RIGHTS AND REQUESTS.

Data subjects have several rights that may be exercised to request that CEMEX provide information on how CEMEX collects and processes their personal data. Requests from data subjects must be answered promptly.

Please see Section V for more details on data subjects' rights related to their personal data.

i. ACCOUNTABILITY.

We are responsible for and must be able to demonstrate compliance with the data protection principles listed above.

V. Rights of Data Subjects.

Data subjects are entitled to a reasonable expectation of privacy in the processing of their personal data. Although privacy laws in the countries where we operate grant data subjects different rights when it comes to how we handle their personal data, most laws grant data subjects the right to request access to their personal data, the right to request that their personal data be corrected, the right to request that the processing of their personal data is stopped or cancelled and the right to object to the processing of their personal data. For data subjects in the European Economic Area[3] from whom we process personal data from within or outside the European Economic Area, the following additional rights apply:

a. right to withdraw consent to processing at any time;

b. right to receive certain information about the CEMEX company's processing activities;

c. right to prevent our use of their personal data for direct marketing purposes;

[2] Please see Section VII for an explanation of the measures and/or safeguards that CEMEX companies must have in place before transmitting personal data of data subjects from the European Economic Area to CEMEX companies located outside of the European Economic Area.

[3] Privacy laws in countries outside of the European Economic Area might also grant data subjects the additional rights described in a) through d). If you are located in a country outside of the European Economic Area and receive a request from a data subject based on either (i) any of the rights described in this Policy or (ii) other rights granted by a local law, you must forward such request to the local Data Protection Officer so that he/she may ultimately decide whether such request is based on legal grounds and how the request should be handled.

d. right to ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;

e. right to restrict processing in specific circumstances;

f. right to challenge processing which has been justified on the basis of our legitimate interests or in the public interest;

g. right to request a copy of an agreement under which personal data is transferred outside of the European Economic Area;

h. right to object to decisions based solely on automated processing, including profiling;

i. right to prevent processing that is likely to cause damage or distress to the data subject or anyone else; and

j. right in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine-readable format.

When a data subject asserts any of the rights described in this Section, CEMEX employees must first verify the identity of an individual requesting the data. CEMEX employees shall not allow third parties to persuade them into disclosing personal data without proper authorization. CEMEX has established proper procedures for answering requests from data subjects based on their legal rights, so CEMEX employees must not answer by themselves any such request and must immediately forward any data subject request they receive to the Data Protection Officer of the country where they work in.

VI. Direct Marketing.

We are subject to certain rules and privacy laws when marketing to our customers. In general, prior explicit consent by a data subject is required for direct marketing by any electronic means of communication. The limited exception for existing customers known as “soft opt in” allows organizations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the data subject in an intelligible manner so that it is clearly distinguishable from other information.

A data subject’s objection to direct marketing must be promptly honored. If a customer opts out at any time, his/her details should be permanently deleted as soon as possible.

VII. Transfers of Personal Data.

For some internal business processes, CEMEX companies may often need to share personal data with each other. In addition, a CEMEX company may also often find itself in a position where personal data must be shared with a third party outside of the CEMEX Group for performing contractual obligations or receiving proposals for services. Whichever the case is, all transfers of personal data, without exception, must always comply with the principles described in Section IV of this Policy.

a. Transfers between CEMEX companies.

In addition to being subject to the principles described in Section IV of this Policy, transfers of personal data from one CEMEX company to another, whether in the same country or not, must not take place before ensuring that adequate legal and technical measures of personal data protection are in place. Privacy laws in both the originating country and the destination country have different requirements that must be complied with before transferring personal data. Before transferring/sharing personal data with another CEMEX company, CEMEX employees must ensure that the Data Protection Officers of the countries involved in the transfer are consulted for their advice.

If personal data needs to be transferred from a CEMEX company with its registered office in the European Economic Area to a CEMEX company with its registered office in a country in another region, both the transferring company and the receiving company must observe and comply with privacy laws of the European Union and of the country of residence of the transferring company. This also means that rights from data subjects under the laws of country of residence of the transferring company must also be complied with by the receiving company. Any requests from data subjects regarding their personal data must be reviewed and answered in accordance with Sections V and IX.c of this Policy.

b. Transfers between CEMEX companies and third parties.

A CEMEX company may transfer personal data to a third party, provided that **(1)** data security, backup, disaster recovery and other technical safeguard measures commonly required for third parties accessing or processing personal data of customers, suppliers, business partners and employees have been reviewed and approved by CEMEX's Information Security department and **(2)** processing by such third party shall be regulated in a written agreement reviewed and approved by the legal department of the CEMEX company which will be transferring personal data. Moreover, whenever personal data of a CEMEX company with registered office in the European Economic Area must be processed by a third party from a location outside of the European Economic Area, the CEMEX Legal department involved in the review of the agreement with the third party under which personal data will be transferred and processed must liaise with the Data Protection Officer of the country where personal data will originate from in order to ensure that required legal documents for securing the transfer of personal data to countries outside of the European Economic Area, such as data protection agreements and the European Commission's Standard Contractual Clauses that provide adequate safeguards for transferring personal data to countries outside of the European Economic Area, are drafted and executed.

VIII. Incidents on Unauthorized Access, Processing, Disclosure or Loss of Personal Data.

In general, privacy laws in the jurisdictions where we operate require us to notify, in some circumstances, incidents of personal data breaches to local authorities, and in certain instances, to the data subject whose personal data is involved in the incident. If a CEMEX employee becomes aware of an unauthorized access, processing, disclosure or loss of personal data, such employee must not attempt to investigate the matter him/herself and must instead contact the Data Protection Officer of the country where he/she works in for advice.

CEMEX has put in place procedures to deal with any suspected unauthorized access, processing, disclosure or loss of personal data and will notify data subjects or any applicable regulator where the company is legally required to do so. Decisions made by the Data Protection Officers and Privacy Managers/Compliance Officers (as defined in Sections IX.b and c) of this Policy) to remedy and/or follow up on incidents of unauthorized access, processing, disclosure or loss of personal data must be upheld by the management of the CEMEX company in question.

IX. Governance.

a. Global Level

At a global level, CEMEX's **Chief Privacy Officer**[4] is responsible for overseeing all privacy and data protection matters, including ensuring compliance with all aspects of this Policy. The Chief Privacy Officer works towards the compliance with national and international data protection regulations, reports to the General Counsel of the CEMEX Group and is supported by regional Privacy Managers/Compliance Officers.

b. Regional Level

At the regional level, CEMEX has appointed **Regional Compliance Officers** for the South, Central America and the Caribbean region, Asia, Middle East and Africa region, United States and Mexico, who also serve as Regional Privacy Officers. For the European region, CEMEX appointed a **Regional Privacy Manager**. The Regional Privacy Manager and Regional Compliance Officers report to the Chief Privacy Officer on all matters related to protection of personal data.

The Regional Privacy Manager and Regional Compliance Officers shall perform the following tasks:

[4] The Compliance Director of the CEMEX Group is the Chief Privacy Officer.

i. Coordinate the local Data Protection Officers and streamline the data protection approach and guidelines in their region.

ii. Coordinate the local Data Protection Officers and streamline the data protection teachings in their region.

iii. Support the Information Security Department on the Protection Impact Assessment when implementing a new software in their region.

iv. Support the local Data Protection Officers and legal departments on resolution of concerns or implementing actions that should, by their nature, be consistent in their region.

v. Oversee coordination efforts to execute remedial actions for cases of breaches of personal data and follow up on the implementation of such actions.

vi. Address any incident related to personal data which, under his/her opinion, has the potential to cause a material impact to the operations of the country where the incident arose or to the CEMEX Group in general.

vii. Follow up on cases related to breaches of personal data and assertions of privacy rights by data subjects for each country to ensure that each case has been properly closed.

viii. Escalate to the Chief Compliance Officer cases where new or amended laws require additional requirements on handling/processing of personal data or changes to this Policy.

ix. Report to the Chief Compliance Officer, on a quarterly basis, if there has been a case of personal data breach in his/her region.

x. Coordinate the implementation, on an annual basis, of a training course on handling/processing personal data for CEMEX employees.

c. Local/Country Level

At the local/country level, CEMEX has appointed **Data Protection Officers** where local privacy laws require companies to do so.[5] Data Protection Officers are tasked with monitoring the compliance of data processing activities with this Policy and local privacy laws. As part of these duties to

[5] For the European region, Data Protection Officers have been appointed for Spain, Czech Republic, Germany, Poland, Croatia, France, Poland and UK. Some of those Data Protection Officers also attend to privacy matters for other countries in the European region where CEMEX has a small presence (e.g. Italy, Sweden, Norway, Switzerland, the Netherlands, etc.). For the rest of the regions where CEMEX operates, there are countries where local laws do not require companies to appoint Data Protection Officers. For such countries, the legal director shall, for purposes of this Policy, perform the duties assigned to Data Protection Officers and attend to any matters related to privacy laws.

monitor compliance, Data Protection Officers shall, among other activities required by local privacy laws:

i. Identify processing activities on personal data.

ii. Analyze and check the compliance of processing activities with this Policy and local privacy laws.

iii. Interpret privacy laws, rules and regulations, as well as flag regulatory changes and report them to the regional Privacy Manager or Compliance Officer.

iv. Ensure that regular training on data privacy matters is provided to all CEMEX employees processing personal data.

v. Report personal data breach cases to the regional Privacy Manager or Compliance Officer, as well as advise on and lead the response/notification strategy and execution of remedial actions.

vi. Lead the response process for inquiries from data subjects.

vii. Inform, advise and issue recommendations on privacy matters to the country manager.

viii. Approve and keep forms of privacy notices updated.

ix. Advise whether or not to carry out a data protection impact assessment (DPIA) and which methodology must be followed when carrying out a DPIA.[6]

For CEMEX's operations in Europe, Data Protection Officers shall be assisted and supported by local **Privacy Committees** on monitoring the compliance of data processing activities with this Policy and local privacy laws. The local Data Protection Officer, as well as the leads of the Information Technology (IT), Business Service Organization (BSO), Human Resources(HR), Legal and Corporate Security local departments of each EU country shall participate as members of each local Privacy Committee. Privacy Committees shall meet twice a year, or as often as the local Data Protection Officer requests it and keep minutes of each meeting.

Among the tasks that each Privacy Committee shall perform are:

i. Coordinate any remediation activities for cases of breaches of personal data and assist the Data Protection Officer with any task required for properly handling/responding to data subjects' requests.

[6] This task applies exclusively for Data Protection Officers in countries where local privacy laws require DPIAs, such as countries in the European Economic Area.

ii. Design training on CEMEX's processes for safeguarding and processing personal data according to this Policy and local privacy laws.

iii. Identify, document and remediate deficiencies in processes for processing personal data.

iv. Ensure that records of processing operations are being kept.

v. Ensure that before any third party processes personal data as a result of services that the country requires (cloud services or some other type of Service that requires processing of personal data), such third party's technical organizational measures for safeguarding personal data, data backup policy, disaster recovery plan and any other technical measures commonly required are reviewed and approved by the country's IT department. For services that must be implemented at a local/country level, but which were procured by CEMEX's headquarters in Monterrey, the Privacy Committee must consult with CEMEX's Information Security in Monterrey in order to verify that the third party's security offering was reviewed and approved.

X. Contacting Key Privacy Personnel.

Any CEMEX employee may approach the relevant Data Protection Officer (or Regional Compliance Officer if the country where he/she works in has neither a local Data Protection Officer nor a legal department) at any time to raise concerns, ask questions, request information or make complaints relating to personal data protection or security issues. If requested, concerns and complaints will be handled confidential and, if found to be systematic within CEMEX, shall be escalated to the Chief Privacy Officer. For contact details of the Data Protection Officer of each country, please contact each country's legal department.

If, however, a CEMEX employee would rather contact CEMEX's Chief Privacy Officer directly due to the urgency of the matter, he/she may do so by sending an e-mail to: derechosarco@cemex.com.

XI. Changes to this Policy.

CEMEX reserves the right to change this Policy at any time without prior notice. Changes to this Policy shall be notified through CEMEX's internal communications channels, as well as by the publication of a notice on CEMEX's main website for each country.

This Policy does not override any applicable national data privacy laws and regulations in countries where CEMEX operates. Please contact the Data Protection Officer of your country for a translated version of this Policy into the local language of your country.