GLOBAL PERSONAL DATA PROTECTION POLICY

Global Policy, effective as of May 1st, 2024.

INDEX

1. POLICY STATEMENT

This Policy provides guidance to comply with applicable legal requirements on data protection, and generally accepted principles on protection of Personal Data, designed to create adequate measures and levels of protection prescribed by the applicable General Framework, in particular as it relates to data protection legislation.

This Policy applies to all Cemex Group entities and Employees, as well as to all Personal Data processed by Cemex Group entities 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 Group's websites or applications or any other Data Subject.

In addition, other Cemex Group policies governing the use or protection of data, whether personal or not, may supplement the processes and activities related to Personal Data outlined in this Policy.

2. POLICY INTERPRETATION, ENFORCEMENT AND ADMINISTRATION

This Policy is approved by the Cemex Senior Vice President of Legal and does not require approval from Cemex's Board of Directors. Additionally, this Policy replaces the Cemex Global Data Protection and Privacy Policy dated May 2018.

Compliance with this Policy is mandatory for all Business Units and all Employees. When in doubt as to the content or application of this Policy, all persons subject to the scope of this Policy have an obligation to contact any Local Privacy Officer of the country where they work in. The Chief Privacy Officer has the ultimate responsibility for the interpretation and administration of this Policy, after consulting with the Cemex Corporate Legal Compliance Department and the Regional Privacy Officers and Local Privacy Officers, as applicable, and has the right to implement any measures, guidelines and tools deemed necessary to assist compliance with this Policy. The Cemex Senior Vice President of Legal and the Chief Data Privacy Officer have the discretion to decide if the Policy should be or should not be physically and/or digitally signed by the Employees who are subject to it, including on a Business Unit per Business Unit basis.

This Policy shall be enforced globally by the Chief Privacy Officer with the support of the Regional Privacy Officers and the Local Privacy Officers. Please refer to Annex A within this Policy for more information on the roles and responsibilities derived from this Policy.

When in doubt as to the content or application of this Policy, or where there is conflict between any part of the General Framework and this Policy, Business Units and Employees have the obligation to contact the Chief Privacy Officer for guidance, or if not available, the corresponding Regional Privacy Officers or Local Privacy Officers. This Policy must be observed in strict compliance with any applicable General Framework. If applicable national privacy laws or additional, new, or stricter applicable regulations on processing of Personal Data conflict with any disposition established in this Policy, applicable law will take precedence.

Should there be any inconsistency or conflict between the English version of this Policy and any other version of the Policy in another language, the English version shall prevail.

3. GENERAL PROVISIONS

3.1. DEFINITIONS

- "Affiliate" means, with respect to any corporation, limited liability company, trust, joint venture, association, company, partnership, or other entity, another corporation, limited liability company, trust, joint venture, association, company, partnership, or other entity that directly, or indirectly through one or more intermediaries, controls or is controlled by or is under common control with the corporation, limited liability company, trust, joint venture, association, company, partnership, or other entity specified.

- "Business Unit" means any area within the Cemex Group, with personnel, resources or assets. The term "Business Unit" also includes countries, regions, departments, divisions, functional areas (including global initiatives within the Cemex Group), companies or specific facilities (ready-mix plants, quarries, etc.) and their Presidents, Executive Vice-presidents, Vice-presidents, Directors or Business Unit Leaders.

- "Business Unit Leader" means the head of any Business Unit.

- "Cemex" means Cemex, S.A.B. de C.V.

- "Cemex Corporate Legal Compliance Department" means to the Cemex Corporate Legal Compliance Department of Cemex's Global Legal Department or any other department which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Corporate Legal Data Privacy Department" means the Cemex Corporate Legal Data Privacy Department of Cemex's Global Legal Department or any another department which may in the future exercise similar functions in relation to the matters of Data Protection and Data Privacy covered herein.

- "Cemex Corporate Legal Department" means the Cemex Corporate Legal Compliance Department of Cemex's Global Legal Department, or any other department which may in the future exercise similar functions in relation to the matters covered herein. For purposes of this Policy, the Cemex Corporate Legal Compliance Department will be the legal department that supervises the Business Units that belong to Cemex's corporate headquarters (for example, but not limited to, corporate finance, corporate treasury, corporate social impact, corporate enterprise risk management, corporate procurement, corporate process and information technology, corporate human resources, corporate communications, corporate planning, or any such Business Units which may replace them in the future).

- "Cemex Enterprise Information Security Management Department" refers to the Cemex Enterprise Information Security Management Department or any other department which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Global Enterprise Services Department (GES)" means the Cemex Global Enterprise Services department or any other department which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Group" means Cemex and its Affiliates.

- "Cemex Human Resources Department" means any Cemex Human Resources Department or any other department within the Cemex Group which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Internal Audit Department" means the Cemex's Corporate Process Assessment Department or any other department which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Local ETHOS Committee" means any Cemex Local ETHOS Committee or any other local committee that supervises a specific country, region or Business Unit which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Local Legal Department" means any Cemex Local Legal Department that supervises a specific country, region or Business Unit or any other local department which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Regional or Local IT Department" means any Cemex Regional or Local Information Technology Department that supervises a specific country or Business Unit or any other regional or local department which may in the future exercise similar functions in relation to the matters covered herein.

- "Cemex Regional Legal Department" means any Cemex Regional Legal Department that supervises a specific region or any other department which may in the future exercise similar functions, including compliance-related functions, in relation to the matters covered herein. For Business Units that do not have a Cemex Local Legal Department, it is the Cemex Regional Legal Department who will perform the functions established in this Policy.

- "Chief Privacy Officer" means to the Cemex Group officer responsible for working towards the compliance with national and international data protection regulations, as well as with all aspects of this Policy, at a global level.

- "Cross Border Data Transfer" means any transfer of Personal Data to a different country from where such Personal Data was collected.

- "Data Protection Officers" means the data protection officers appointed by the Cemex Group in countries where local privacy laws require companies to do so, or Cemex has decided to do so because it is beneficial considering local best practices.

- "Data Subject" means a living, identified or identifiable individual whose Personal Data is processed by the Cemex Group.

- "Employees" means the individuals who occupy a position in or are directly or indirectly employed by any company of the Cemex Group.

- "European Economic Area" means European Union countries and also Iceland, Liechtenstein and Norway, as updated by the corresponding international agreements that may be reached by the corresponding governing bodies/states.

- "General Framework" means (i) the terms and conditions set forth in this Policy, (ii) applicable local laws and regulations to which each Employee is subject to, (iii) charter documents (i.e., by-laws,

articles of incorporation, etc.) of the Cemex Group; and (iv) any applicable Cemex Group internal policies.

- "Local Privacy Officers" means the Cemex Group officer responsible for monitoring the compliance of data processing activities with this Policy and local privacy laws, at a country/local level. This term includes (i) the Data Protection Officers, and/or (ii) Cemex Group's legal directors for each country (or any other person at the Cemex Local Legal Department appointed by the legal director for this purpose), who, if applicable, shall coordinate with the Data Protection Officers to enforce this Policy locally and carry out any activities required by local privacy laws.

- "Personal Data" means 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 that the Cemex Group possesses or can reasonably access. 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 (for example: professional references of a past Employee). Personal Data may also include Sensitive Personal Data (as defined below).

- "Policy" means this Global Personal Data Protection Policy as may from time to time be changed, modified, amended, restated, supplemented, and/or supplemented.

- "Privacy Committee" means the Cemex Group committee tasked with assisting and supporting the Local Privacy Officers in monitoring the compliance of data processing activities related to this Policy and local privacy laws.

- "Processing" whether the term is capitalized or not, refers to any operation or any set of operations performed upon personal data including, but not limited to, the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure, or destruction of data. Processing may be performed through automated means, or manual processing, if the Personal Data is contained or is intended to be contained in a filing system.

- "Regional Privacy Officer" means the Cemex Group officer responsible for coordinating the Local Privacy Officers in its region and for streamlining the data protection approach, guidelines, and teachings, at a regional level. The "Regional Privacy Officer" reports directly to the Chief Privacy Officer. The Cemex Group has appointed Regional Privacy Officers for Europe, South, Central America and the Caribbean region, Asia, Middle East and Africa region, United States and Mexico.

- "Sensitive Personal Data" means any Personal Data which privacy laws in countries where the Cemex Group operates identify as sensitive, such as information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions and/or information of minors, as well as Personal Data requiring additional measures or requirements for processing under applicable privacy laws (for example, personal financial data in Mexico).

- "Third Party(ies)" means, but is not limited to, any third parties that will be acting as customers, vendors, contractors, subcontractors, agents, subagents, custom brokers, freight forwarders, logistics providers, distributors, representatives, intermediaries, business partners, joint ventures, or any other person transacting with or acting on the Cemex Group's behalf (such as representatives, agents or intermediaries), as well as their employees or other persons working on their behalf.

3.2. GENERAL DATA PROTECTION AND PRIVACY PROVISIONS

A. PRINCIPLES FOR PERSONAL DATA PROCESSING

To procure compliance with applicable data protection laws and best practices, the Cemex Group must act according to the following principles for Personal Data processing:

LAWFULNESS

Processing of Personal Data must be done lawfully, fairly and in a transparent manner to protect the rights that Data Subjects from whom the Cemex Group entities process Personal Data. Processing of Personal Data must always have a lawful basis. The following list describes common lawful bases for processing Personal Data of customers, suppliers, business partners, candidates, and Employees:

CONSENT	Data can be processed following consent by the Data Subject. Before giving consent, the Data Subject must be informed how their data is being used and for what purpose. If there are multiple purposes for the processing of the Personal Data, the Data Subject's consent should be given for each purpose. Consent must be granted by the Data Subject's clear affirmative action and must be properly documented as per the applicable General Framework. In certain cases, as with Employees in the European Economic Area, lawful basis other than consent must be relied on to process Personal Data (unless otherwise authorized by the Local Privacy Officer). Additionally, for the processing of Sensitive Personal Data, automated decision-making, and Cross Border Data Transfers, explicit consent is usually required. Nevertheless, processing of Sensitive Personal Data should be kept to a minimum and its processing should always be tied to a lawful basis. When collecting or otherwise processing Sensitive Personal Data, the Local Privacy Officer must be consulted.
CONTRACTUAL NECESSITY	Personal Data of customers, suppliers, business partners and Employees, as well as pensioners, may be processed on the basis that such processing is necessary for a Cemex Group entity 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 or services. Regarding Personal Data of Employees, a Cemex Group entity will often be in a position where Personal Data must be processed to comply with several obligations under individual and collective employment contracts, such as paying salaries and benefits to its Employees.
LEGITIMATE INTERESTS	When a Data Subject contacts a Cemex Group entity to ask about its products or services, or to receive more information about specific offerings, the Cemex

	Group entity may process their Personal Data to be able to provide the requested information about the services or product offerings. Subject to Subsection C of this Section 3.2., the Cemex Group entity may also process Personal Data for market research purposes if such Cemex Group entity is expecting to deliver services or products and if the activity will not negatively affect the Data Subjects. However, Data Subjects can always object or withhold consent to the processing of their Personal Data and the Cemex Group should honor such request immediately. In the case of employee candidates who apply for a job with a Cemex Group entity, 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.
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 a Cemex Group entity may have to process Personal Data on this basis.
COMPLIANCE WITH LEGAL OBLIGATIONS	In certain circumstances, a Cemex Group entity may need to process Personal Data to comply with legal obligations, such as tax requirements, criminal investigations, or to answer and comply with a court order.

FAIRNESS AND TRANSPARENCY

When first collecting Personal Data from Data Subjects, including when collecting Personal Data for human resources or employment reasons, Data Subjects must be informed, through a privacy notice (sometimes called a privacy policy), on the Cemex Group entity processing the Personal Data, as well as on how and why the Cemex Group entity will use, disclose, protect, retain, or otherwise process such Personal Data.

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 Subjects have been informed of the new purposes and have consented to such new purpose.

ACCURACY

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

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, as per the General Framework, in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which the Cemex Group 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 Cemex Global Data Retention Policy (as such policy may from time to time be changed, modified, amended, restated, supplemented and/or replaced) may mention legal obligations in relation to the retention of specific data which must be considered when determining the retention period for Personal Data.

SECURITY, INTEGRITY, AND CONFIDENTIALITY

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

PROTECTING PERSONAL DATA	The Cemex Group must implement and maintain safeguards appropriate to its size, scope and business, available resources, and the amount of Personal Data that it owns or maintains on behalf of others and identified risks. Before the introduction of new methods of data processing, such as new information technology systems, the Cemex Business Unit that will be processing Personal Data must consult with the relevant Local Privacy Officer and Cemex's Enterprise Information Security Management Department to determine whether the new information technology systems offer adequate means for protecting Personal Data and if the new method is admissible under the applicable General Framework. 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, in relation to such Personal Data, the (i) confidentiality: only people who have a need to know and are authorized to use the Personal Data can access it; (ii) integrity: Personal Data must be accurate and suitable for the purpose for which it is processed; and, (iii) availability: authorized users are able to access the Personal Data when they need it for authorized purposes. All Business Units and Employees that manage and store Personal Data have the obligation to ensure that such Personal Data is stored in devices, platforms,

databases, folders that have the required safeguards to not be accessed by persons not authorized to have access to such Personal Data.

Any unauthorized collection, processing, or use of such data is prohibited. Employees (and/or Third Parties, if applicable and once any transfer requirements have been complied with) 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 (or Third Party) who does not need to process such data as part of their job duties and/or has not been expressly authorized to carry out such data processing must be avoided.

Furthermore, Business Units and Employees are not authorized to request Personal Data being managed by any persons providing services or goods to any Business Unit, unless such request has been authorized by the Chief Privacy Officer or the corresponding Regional Privacy Officer or Local Privacy Officer.

Storage of Personal Data by Employees outside of Cemex-authorized platforms is prohibited. Furthermore, when storing Personal Data in any type of Cemex Group-authorized storage, such as cloud storage, or other optical and/or magnetic storage, all privacy settings must be carefully reviewed to ensure that all Personal Data can only be accessed by authorized personnel.

TRANSFER LIMITATION

Personal Data collected by a Cemex Group entity must not be transferred to a different Cemex Group entity or any Third Party outside of the Cemex Group without appropriate protective measures and safeguards being in place, and without complying with any other requirements pursuant to applicable law.

COMPLIANCE WITH DATA SUBJECTS' RIGHTS AND REQUESTS

Data Subjects have the right to request that a Cemex Group entity provides information on how such Cemex Group entity collects and processes their Personal Data, in accordance with the applicable General Framework. Requests from Data Subjects must be answered promptly.

ACCOUNTABILITY

The Cemex Group (through its Employees) is responsible for and must be able to demonstrate compliance with the data protection principles listed in this Policy in relation to any Personal Data it processes in accordance with the applicable General Framework.

B. RIGHTS OF DATA SUBJECTS

Subject to the General Framework, Data Subjects are entitled to a reasonable expectation of privacy in the processing of their Personal Data. Although privacy laws in the countries where the Cemex Group operates grant Data Subjects different rights when it comes to how their Personal Data is processed, most laws grant data subjects at least the following rights:

1. Right to withdraw consent to processing at any time;
2. Right to receive certain information about the Cemex Group processing activities;
3. Right to prevent the Cemex Group's use of their Personal Data for direct marketing purposes; and
4. Right to ask the Cemex Group 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.

In addition to the rights mentioned above, Data Subjects in the European Economic Area and certain other countries as defined by the General Framework may also have the following rights:

1. Right to restrict processing in specific circumstances;
2. Right to challenge processing that has been justified on the basis of our legitimate interests or in the public interest;
3. For Data Subjects in the European Economic Area, the right to request a copy of an agreement under which Personal Data is transferred outside of the European Economic Area;
4. Right to object to decisions based solely on automated processing, including profiling;
5. Right to prevent processing that is likely to cause damage or distress to the Data Subject or anyone else; and
6. Under limited circumstances, right to receive or ask for the Data Subjects' 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 3.2., Employees must first verify the identity of an individual requesting the data. Employees shall not allow third parties to persuade them into disclosing Personal Data of anyone without proper authorization.

Regarding Personal Data processed by Cemex Group entities, the Cemex Group has established proper procedures for answering requests from Data Subjects based on their legal rights, so Employees must not answer by themselves any such request and must immediately forward any Data Subject request they receive to the Local Privacy Officer of the country they work in.

C. DIRECT MARKETING

The Cemex Group is subject to certain rules and privacy laws when marketing its products and services to customers. As a rule, prior explicit consent by a Data Subject is required for direct marketing by any electronic means of communication. A limited exception for such rule (known as "soft opt in") is applicable to existing customers of a Cemex Group entity, and allows such Cemex Group entity to send marketing texts or emails if:

1. The Cemex Group entity has obtained contact details in the course of a sale to the Data Subject;

2. The Cemex Group entity is marketing similar products or services; and

3. If the Cemex Group entity gave the person an opportunity to opt out of marketing when first collecting the details of the Personal Data and in every subsequent message.

Unless stated otherwise in applicable law, 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. Additionally, a Data Subject's objection to direct marketing must be promptly honored. If a customer opts out at any time, their details should be permanently deleted as soon as possible.

D. TRANSFERS OF PERSONAL DATA

For some business processes, the Cemex Group entities may often need to share Personal Data with each other. In addition, a Cemex Group entity 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 this Policy such as the Transfer Limitation Principle established in Subsection A of this Section 3.2.

TRANSFERS BETWEEN CEMEX GROUP ENTITIES

Transfers of Personal Data from one Cemex Group entity 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. Furthermore, privacy laws in both the originating country and the destination country of the Personal Data may have different requirements that must be complied with. Before transferring Personal Data from one Cemex Group entity to another, whether in the same country or not, Employees must ensure that the Local Privacy Officers of the countries involved in the transfer are consulted for their advice.

Additionally, rights from Data Subjects under the laws of the transferring company's country of residence must also be complied with by the receiving Cemex Group entity. Any requests from Data Subjects regarding their Personal Data must be reviewed and answered in accordance with this Policy.

TRANSFERS BETWEEN CEMEX GROUP ENTITIES AND THIRD PARTIES

A Cemex Group entity may transfer Personal Data to a Third Party, provided that:

- 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 the Cemex Enterprise Information Security Management Department; and

- Processing by such Third Party is regulated in a written agreement reviewed and approved by the Cemex Local Legal Department of the Cemex Group Entity which will be transferring Personal Data.

Whenever Personal Data of a Cemex Group entity 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 Local 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 Local Privacy Officer of the country where Personal Data will originate. The foregoing is necessary to ensure that required legal documentation for securing the transfer of Personal Data to countries outside of the European Economic Area, where needed, is drafted and executed.

3.3. AMENDMENTS AND WAIVERS

The Chief Privacy Officer (or any person with the equivalent title) reserves the right to change and/or amend this Policy at any time without prior notice. Changes to this Policy shall be notified through the Cemex Group's internal communications channels.

This Policy must be analyzed and reviewed at least every two years, or before in accordance with any applicable General Framework, to determine if any updates or amendments are necessary, with the ultimate decision being of the Cemex Corporate Legal Department.

All changes or amendments to this Policy must be informed to the Cemex Internal Control Department. All waivers and exceptions to this Policy, the processes contained herein, and any rules and/or guidelines set forth in this Policy, must be expressly approved in writing by the Cemex Senior Vice President of Legal (or any person with the equivalent title) after consulting with the Chief Privacy Officer and the Cemex Legal Corporate Compliance Department before granting any waiver or exception.

3.4. NON-COMPLIANCE PROCESS AND REPORTING

Strict compliance of this Policy is expected and required from all Employees and Cemex representatives. Any violation of this Policy may result in disciplinary action including but not limited to, employment suspension or termination, as well as any other sanctions set forth and applicable pursuant to applicable laws.

The Cemex Group encourages reporting, in good faith, any violation regarding this Policy or any applicable laws. The official channels for reporting any actual or suspected breaches to this Policy are the following:

- ETHOSline, via online, phone, or e-mail;
- Cemex Internal Audit Department;
- Any Cemex Local ETHOS Committee, via phone, e-mail or in person;
- The corresponding Cemex Regional Legal Department or Cemex Local Legal Department;
- Cemex Corporate Legal Compliance Department; or
- Cemex Corporate Legal Data Privacy Department.

Privacy laws in the jurisdictions where the Cemex Group operates may require us to notify incidents of Personal Data breaches to local authorities, and in certain instances, to the Data Subject(s) whose Personal Data is involved in the incident. If an Employee becomes aware of an unauthorized access, processing, disclosure or loss of Personal Data, such Employee must not attempt to investigate the

matter themselves and must instead immediately contact the Local Privacy Officer of the country where they work in for advice.

3.5. NO RETALIATION

The Cemex Group strictly prohibits retaliation or any form of discrimination against any individual who reports in good faith any possible non-compliance with this Policy or applicable laws. Such retaliation would be grounds for discipline, including potential termination of employment. No Employee shall be directly or indirectly terminated, demoted, suspended, threatened, blacklisted, harassed, or in any other manner discriminated in the terms and conditions of employment or post-employment solely because they reported in good faith an actual or suspected violation of this Policy or applicable laws.

3.6. TRAININGS AND AUDITS

If and when required by the Chief Privacy Officer, or the corresponding Regional Privacy Officer or Local Privacy Officer, Employees could be required to attend necessary trainings. Employees that receive training on this Policy can be asked to provide written confirmation that they have received the corresponding training. The Employees that require any training shall be identified by the Chief Privacy Officer, or the corresponding Regional Privacy Officer or Local Privacy Officer, at its discretion.

Additionally, the Cemex Corporate Legal Compliance Department, the Chief Privacy Officer, the corresponding Cemex Regional Legal Department and Cemex Local Legal Department have the authority to carry out audits to evaluate Employees' compliance with this Policy.

ANNEX A

ADMINISTRATION TASKS

A. CHIEF PRIVACY OFFICER

The Chief Privacy Officer shall work towards compliance with national and international data protection regulations, as well as with all aspects of this Policy.

B. REGIONAL PRIVACY OFFICERS

The Regional Privacy Officers shall enforce this Policy regionally, and perform the following tasks:

- Support the Cemex Enterprise Information Security Management Department on the data protection impact assessment when implementing a new software in their region.
- Support the Local Privacy Officers and Cemex Regional Legal Department and/or Cemex Local Legal Department on resolution of concerns or implementing actions that should, by their nature, be consistent in their region.
- Oversee coordination efforts to execute remedial actions for cases of breaches of Personal Data and follow up on the implementation of such actions.
- Address any incident related to Personal Data which, under their 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.
- 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.
- Escalate to the Chief Privacy Officer cases where new or amended laws require additional requirements on handling/processing of Personal Data or changes to this Policy.
- Report to the Chief Privacy Officer in case there is a case of Personal Data breach in their region.
- Coordinate the implementation, on an annual basis, of a training course on handling/processing Personal Data for Employees.

C. LOCAL PRIVACY OFFICERS

The Local Privacy Officers shall enforce this Policy locally, and, among other activities required by local privacy laws:

- Interpret privacy laws, rules, and regulations, as well as flag regulatory changes and report them to the Regional Privacy Officer.
- Ensure that regular training on data privacy matters is provided to all Employees processing Personal Data.

- Report Personal Data breach cases to the Regional Privacy Officer, as well as advise on and lead the response/notification strategy and execution of remedial actions.
- Lead the response process for inquiries from Data Subjects.
- Inform, advise and issue recommendations on privacy matters to the Business Unit Leader and the corresponding local departments within a Business Unit.
- Approve and keep forms of privacy notices updated.
- Advise whether or not to carry out a data protection impact assessment and which methodology must be followed when carrying out such assessment.

D. PRIVACY COMMITTEES

The Privacy Committees shall support and assist Local Privacy Officers in their functions related to this Policy. These Privacy Committees shall be composed by the Local Privacy Officer, and the leads of the departments overseeing the Information Technology, Global Enterprise Services, Human Resources, Legal and Security functions at the local level (or any other area which in the future carries out the activities performed by the abovementioned departments as of the effective date of this Policy).

The Privacy Committees shall meet with the periodicity that the Local Privacy Officer determines, or as often as the Local Privacy Officer requests it, and shall keep minutes of each meeting.

Among the tasks that each Privacy Committee shall perform are:

- Design training on the Cemex Group's processes for safeguarding and processing Personal Data according to this Policy and local privacy laws.
- Identify, document, and remediate deficiencies in processes for processing Personal Data.
- Ensure that records of processing operations are being kept.
- Ensure that before any Third Party processes Personal Data as a result of services that the country requires, 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 the Cemex Group's headquarters in Monterrey, the Privacy Committee must consult with the Cemex Enterprise Information Security Management Department in Monterrey in order to verify that the Third Party's security offering was reviewed and approved.

THE CEMEX CORPORATE LEGAL COMPLIANCE DEPARTMENT AND/OR THE CEMEX CORPORATE LEGAL DATA PRIVACY DEPARTMENT MAY UPDATE THIS ANNEX ON A REGULAR BASIS. IF YOU HAVE ANY QUESTIONS ABOUT THIS ANNEX, PLEASE CONTACT THE CEMEX CORPORATE LEGAL COMPLIANCE DEPARTMENT TO ENSURE THAT YOU HAVE THE MOST UP-TO-DATE VERSION.