Personal Data Security Policy Enterprises Holcim in Poland

§ 1.
PREAMBLE

1. The Personal Data Security Policy is a document describing the principles of personal data protection applied by the group of companies.Holcimin Poland, in order to meet the requirements of Regulation (EC) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data (hereinafter referred to as GDPR).
2. The policy is one of the organizational measures aimed at demonstrating that the processing of personal data is carried out in accordance withGDPR Regulation (§ 1, p.1).
3. According to the preamble to the GDPR Regulation„*for a group of companies the company controlling the processing of personal data in its affiliated companies should be considered together with these companies"*.
4. The company was recognized as the parent company **Holcim Polska S.A.** ul. Warszawska 110, 28-366 Małogoszcz, NIP 526-10-60-765, where the criterion for recognition as a parent company is control over data processing and not capital or shareholding dominance. The current list of subsidiaries and affiliated companies within Holcim Enterprises in Poland is available at the company's registered office and on the website www.holcim.pl
5. Depending on the specific factual circumstances, each of the companies participating in the group may be a controller of some data and a processor of others.
6. The criterion determining the role of the controller is the decision-making power in determining the purposes and methods of processing personal data.
7. As part of establishing corporate governance, companies assume that the controller of employees' personal data will be their employer, i.e. the entity with which the employees have entered into an employment relationship.
8. Employees' personal data will also be processed by other group companies on the basis of the controllers' legally justified purposes.
9. Mapping of data processing processes was carried out within and between individual companies of the capital group.
10. As a result of the mapping, a model of data flow and processing in the group was created in the form of register of processing activities (RCP).
11. The basis for transferring data within a group of undertakings is recital 48 of the GDPR: "*Controllers that are part of a group of companies may have a legitimate interest in transferring personal data within the group of companies for internal administrative purposes, which also applies to the processing of personal data of customers or employees*.
12. As part of the administration process systems IT, including: HR and payroll, finance, sales and purchasing,personal data are transferred to a third country outside the European Economic Area.
13. The data is transferred in accordance with Article 46 of the GDPR, in particular by concluding EU Standard Contractual Clauses.
14. One of the mechanisms to secure data transfer are binding corporate rules (e.g. the Holcim Data Protection Directive).
15. This document meets the requirements set out in the GDPRand is approved by the relevant supervisory authority.

§ 2.
Legal basis

1. Personal data in**Holcim companies in Poland (Holcim Polska SA and subsidiaries)**are processed in compliance with applicable legal provisions, in particular:
    a. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC,
    b. provisions of the Act of 16 July 2004 – Telecommunications Law (consolidated text: Journal of Laws of 2022, item 1648, as amended),
    c. provisions of the Act of 13 April 1993 on Combating Unfair Competition (Journal of Laws of 2022, item 1233, as amended),
    d. provisions of Article 22 § 1-5 of the Act of 26 June 1974, the Labor Code (consolidated text: Journal of Laws of 2022, item 1510, as amended) and implementing provisions issued under this Act,
    e. other provisions of laws and regulations regulating the processing of specific categories of personal data.
2. Personal data at Holcim Enterprises in Poland are processed for the purpose of fulfilling tasks. In particular, personal data are processed for:
    a. securing the proper course of core business, realization of other justified goals and tasks of Holcim Enterprises in Poland in the scope of:
        1) planning, conducting, managing and administering personal data of data subjects (or a third party with whom data subjects are associated) in contractual business relationships, e.g. by executing transactions and orders for products or services, processing payments, carrying out accounting, auditing, billing and debt collection activities, arranging shipments and deliveries, facilitating repairs and providing support services, and assurance other services or items,which data subjects may request from us;
        2) maintaining the security and protection of our products, services and websites or other systems, preventing and detecting security threats, fraud and other criminal or malicious activities;
        3) to meet legal compliance obligations such as compliance checks or record-keeping obligations (e.g., under antitrust laws, export regulations, trade sanctions and embargo laws, anti-bribery and corruption laws and internal regulations or to prevent official misconduct or money laundering), which may include automated background checks contact details and identifying data subjects on relevant lists of sanctioned parties and contacting data subjects to confirm their identity in the event of a potential match or recording data subject interactions with third parties, which may be relevant for competition protection purposes;
        4) resolving disputes, enforcing the performance of our agreements and demonstrating the validity, filing or defending claims or
        5) ensuring compliance with legal requirements, e.g., regarding maintaining sales records for tax purposes or sending notifications and other information as required by law.
    b. ensuring correct, legal and compliant with the objectives of the Enterprises Holcim in Poland, personnel policy and ongoing management of employment relations and other employment relations established by enterprisesHolcimin Poland.

§ 3.
Basic Definitions

The terms used in the document have the following meanings:

a. **Holcim companies in Poland or Holcim in Poland** - Holcim PolandS.A. with its registered office in Małogoszcz, ul. Warszawska 110, 28-366 Małogoszcz (Controller) and its subsidiaries. The current list of subsidiaries and affiliated companies is available at the company's registered office and on the website www.holcim.pl
b. **Administrator (of data)**- means a natural or legal person, public authority, agency or other entity that, alone or jointly with others, determines the purposes and means of processing personal data.
c. **SHOWS**- Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46 of 27 April 2016 (OJ EU L 119 of 04/05/2016).
d. **Personal data**- any information relating to an identified or identifiable natural person. An individual is considered to be directly or indirectly identifiable by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.
e. **Processing of personal data**- any automated or non-automated operation or set of operations performed on personal data or on sets of personal data and includes collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of personal data.
f. **Restriction of processing**- involves marking the personal data being processed in order to limit their future processing.
g. **Anonymization**- change of personal data as a result of which these data lose their personal nature.
h. **Consent of the data subject**- means any freely specified, specific, informed, and unambiguous indication of a data subject's consent to the processing of personal data related to them, by means of a statement or clear affirmative action. Consent must be documented in an appropriate manner to prove it.
i. **Data Protection Impact Assessment**- is a process carried out by the Controller, if required by applicable law and, if necessary, with the involvement of the Data Protection Officer, prior to processing, where there is a likelihood of a high risk to the rights and freedoms of natural persons due to the type of personal data processing and the use of new technologies, taking into account the nature, scope, context, and purposes of the processing. This process must assess the impact of the planned processing operations on personal data protection.
j. **Data subject** is any natural person who is the subject of data processing.
k. **Recipient**- means a natural or legal person, public authority, agency or other body to which personal data are disclosed, whether a third party or not.
l. **Processor (Processor)**is a natural or legal person, public authority, agency or any other body that processes personal data on behalf of the controller.
m. **Data Protection Officer (DPO)**- is a person formally appointed by the Controller to inform and advise the Controller/Processor/employees on applicable data protection law and this Policy and to monitor compliance therewith and to act as a contact point for Data Subjects and the supervisory authority.
n. **Pseudonymization**- means the processing of personal data in such a way (e.g. by replacing names with numbers) that the personal data can no longer be assigned to a

specific data subject without the use of additional information (e.g. a reference list of names and numbers), provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not assigned to an identified or identifiable natural person.

o. **Special categories of personal data**- reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and include the processing of genetic data, biometric data for the unique identification of a natural person, health data, data concerning a person's natural sexual life, or sexual orientation. Depending on applicable law, special categories of personal data may also include information on social security measures or administrative and criminal proceedings and sanctions.
p. **Profiling**- is arbitrary form automated processing of personal data, which involves the use of personal data to evaluate certain personal factors relating to a natural person, in particular to analyse or forecast aspects relating to the performance of that natural person at work, his or her economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
q. **Personal data breach**- it is an accidental or unlawful incident leading to the destruction, loss, modification, unauthorized disclosure of or unauthorized access to personal data.
r. **WITH data collection**- means a structured set of personal data accessible according to specific criteria, regardless of whether that set is centralised, decentralised or functionally or geographically dispersed;
s. **Employee -** employees and all other persons acting on behalf of the EnterprisesHolcimin Poland, regardless of the legal form of their relationship withHolcimin Poland.
t. **IT system**- a set of cooperating devices, programs, information processing procedures and programming tools used to process data.
u. **Protection of personal data**- implementation and operation of appropriate technical and organizational measures to ensure data protection against unauthorized processing.
v. **Bsafety**- a factual situation that prevents accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data transmitted, stored or otherwise processed.
w. **Information System Administrator (ASI)**- a team of persons authorized by the Controller, responsible for the security of personal data processed in IT systems, including in particular for preventing third-party access to the systems and taking appropriate actions in the event of detection of violations in these systems.
x. **BuildingsHolcim**- buildings located independently or within the offices or plants of Holcim Enterprises in Poland, the current list of addresses of Holcim facilities in Poland is available on the websitewww.holcim.pl/lokalizacje

§ 4.
The purpose of introducing the Personal Data Security Policy document

1. The purpose of the Personal Data Security Policy is:
    a. achieving and maintaining an acceptable level of security of information assets of Holcim Enterprises in Poland by implementing an appropriate system to protect these assets against internal and external threats;
    b. ensuring the security of personal data at Holcim Enterprises in Poland, with particular emphasis on compliance with the law;
    c. raising the level of awareness of Holcim Enterprise Staff in Poland regarding the essence of the personal data security problem.

2. The Management Board of Holcim Enterprises in Poland declares its commitment to the proper management of personal data security and declares that it will make every effort to ensure the security of personal data protection.

§ 5.
Scope of application of the Personal Data Security Policy document

1. The Personal Data Security Policy applies to all forms of information containing personal data: paper documents, electronic records and other documents owned by Holcim Enterprises in Poland or administered by Holcim Enterprises in Poland and processed in the IT, traditional (paper) and communication systems of Holcim in Poland.
2. The Personal Data Security Policy applies to all Holcim Personnel in Poland, i.e. to allemployeesHolcim Enterprises in Poland, as well as third parties who have access to personal data in Holcim Enterprises in Poland.
3. Personal data protection, as set out in the Personal Data Security Policy, is implemented at every stage of information processing.

§ 6.
Rules for the processing of personal data

Personal data must be:

a. processed lawfully, fairly and transparently for the data subject***("legality, fairness and transparency")***;
b. collected for specific, explicit and legitimate purposes andunprocessedfurther processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is not considered incompatible with the original purposes under Article 89(1) GDPR***("purpose limitation")***;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed***("data minimization")***;
d. accurate and, where necessary, kept up to date; all reasonable steps must be taken to ensure that personal data that are inaccurate in relation to the purposes for which they are processed are immediately erased or rectified***("regularity")***;
e. kept in a form which permits identification of a data subject for no longer than is necessary for the purposes for which the data are processed; personal data may be kept for a longer period provided they are processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes under Article 89(1) of the GDPR, provided that appropriate technical and organisational measures required by the GDPR to protect the rights and freedoms of data subjects are implemented***("storage limitation")***;
f. processed in a way that ensures appropriate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage, using appropriate technical or organisational measures***("integrity and confidentiality")***.

§ 7.
Personal Data Protection Officer

1. **The Management Board of Holcim Enterprises in Poland has appointed a Data Protection Officer - Krzysztof Radtke.** It reports directly to the Management Board of Holcim Enterprises in Poland and performs its tasks in accordance with the GDPR regulation.
2. The most important duties of the Data Protection Officer include:
    a. informing the Controller, the processor and employees who process personal data about their obligations under data protection law and advising them on this matter;
    b. monitoring compliance with data protection regulations by the Controller, the processor and employees who process personal data;

c. ensuring the processing of personal data in accordance with the provisions of the Personal Data Security Policy, including the segregation of duties, awareness-raising activities, training of staff involved in processing operations and related audits;
d. issuing and canceling, in parallel withAdministrator, authorizations to process personal data;
e. running, in parallel withAdministrator, records persons authorized to process personal data;
f. providing recommendations on data protection impact assessments upon request and monitoring their implementation;
g. acting as the contact point for the supervisory authority on issues relating to processing, including prior consultation, and, where appropriate, conducting consultations on any other matter;
h. conducting explanatory proceedings in the event of a breach of personal data protection,
i. control of the activities of organizational units in terms of compliance of data processing with personal data protection regulations;
j. initiating and undertaking projects to improve personal data protection,
k. cooperation with the supervisory authority.

3. The Data Protection Officer has the right to:
   a. Recommended and enforcing the performance of tasks related to the protection of personal data in Holcim Enterprises in Poland;
   b. access to the premises where data files are located and carry out the necessary tests or other control activities in order to assess the compliance of data processing with the law;
   c. request written or oral explanations to the extent necessary to establish the factual circumstances;
   d. demand the presentation of documents and any data directly related to the issue of the inspection;
   e. request access to devices, media and IT systems used for data processing for inspection.
4. Data subjects may contact the Data Protection Supervisor on all matters relating to the processing of their personal data and the exercise of their rights under the GDPR at the following e-mail address:

pl-m-inspektor-ochrony-danych@holcim.com

§ 8.
Impact Assessment - Risk Analysis

1. Impact assessment is a formal procedure for conducting a risk analysis, specified in Article 35 of the GDPR, for which the Controller is responsible.
2. The impact assessment must be carried out in cooperation with the Data Protection Officer.
3. ININ order to perform a risk analysis, it is necessary to identify the personal data that should be secured, and these data in the form of sets (categories of persons) are listed in the Register of Processing Activities (RCP), whereby the list processing operations (asset inventory) include: the description of the data sets (categories of persons), name of the data set (description of the category of persons), description of the purposes of processing, nature, scope, context of personal data, recipients of data, functional description of the processing operation, assets used for personal data processing (Information, Programs, Operating Systems, IT Infrastructure, Infrastructure, Employees and collaborators, Outsourcing).
4. Necessity Assessmentandproportionality (compliance with GDPR provisions) includes - as part of the impact assessment (risk analysis) - confirmation that the Controller (or Processor) meets legal obligations towards data in the files (for categories of persons) by ensuring that:

a. these data are legally processed (pursuant to Art. 6, 9),
b. these data are adequate in relation to the purposes of processing,
c. these data are processed for a specified period of time (data retention),
d. towards these people the so-called information obligation (Articles 12, 13 and 14) has been fulfilled, together with an indication of their rights (e.g. the right to access data, transfer, rectification, deletion, restriction of processing, objection, withdrawal of consent),
e. information clauses have been developed for categories of people,
f. there are entrustment agreements with processors (art. 28),which are recorded using methods implemented at Holcim in Poland,
g. Confirmation of compliance with the above legal requirements of the GDPR can be found inRegister of Processing Activities (§ 9. p. 7 letter f. below).

5. Risk analysis includes a structured set of rules for conducting a risk analysis to secure personal data adequately to the identified threats resulting from accidental or unlawful destruction, loss, modification, unauthorized disclosure or unauthorized access to personal data.
6. It is assumed that risk analysis is carried out for a set or group of sets (categories of persons) or for processing processes (e.g. for a set of employees, a set of customers, for the process of sending commercial information from a marketing database).
7. As part of the risk analysis, additional definitions as below:
   a. **Assets**- tangible and intangible measures affecting the processing of personal data,
   b. **Personal data protection breach (incident)**- is a breach of security leading to the accidental or unlawful destruction, loss, modification, unauthorized disclosure of, or unauthorized access to, personal data transmitted, stored or otherwise processed,
   c. **Danger**- potential breach (potential incident),
   d. **Consequences**- results of an undesirable incident (losses in the event of a threat),
   e. **Risk**- the probability that a specific threat will occur and cause loss or destruction of resources.
8. At the determining threats:
   a. The Controller is responsible for determining the list of threats to confidentiality, availability and integrity that may occur in the processing of data in a collection, for a category of persons or in the processing process,
   b. Threats should be identified in relation to previously identified assets.
9. Risk calculation for threats includes:
   a. The administrator determines the Probability (P) of occurrence of individual threats in a set (for a category of persons) or in the processing process, where the established probability scale is presented in Table A,
   b. The Administrator determines the Consequences (S) of incidents (materialization of threats), taking into account financial losses, loss of reputation, sanctions/criminal consequences, where the established scale of Consequences is presented in Table B,
   c. The Administrator calculates Risk (R) for all threats and their effects according to the formula:

R = P x S

Table A Probability of threat occurrence (P)	Scale (Weight)
low risk	1
medium threat	2
high risk	3

Table B Consequences of the threat	Scale (Weight)
small (up to PLN 10,000, local press incident)	1
medium (PLN 10,000 - 100,000, nationwide press incident)	2
large (from PLN 100,000, violation of the law)	3

10. Comparing the calculated risks to the scale and determining further risk management includes:
    a. The administrator compares the calculated risks with the scale and makes decisions regarding further risk management,
    b. The established Risk scale is presented in Table C.

Table C Risk level	Value [R = P x S]
negligible and acceptable risk (we accept)	1 - 2
risk is optional (we accept or reduce)	3 - 6
the risk is unacceptable (we need to lower)	9

11. The risk value response includes:
    a. Risk acceptance - security measures are appropriate - no need for additional security measures;
    b. Risk reduction measures that the Administrator may take:
        1) **Transfer**- risk transfer (outsourcing, insurance),
        2) **Avoidance**- elimination of activities causing risk (e.g. prohibition of taking portable computers outside the organization),
        3) **Reduction**- applying security measures to reduce risk (e.g. encryption flash drives with data transferred outside the company),
    c. Risk analysis is carried out in an established template (internal documents of the Organization).
12. Risk reanalysis is carried out cyclically or after significant changes in data processing (e.g. processing of new sets/categories of persons, implementation of new processing processes, legal changes).
13. Risk management also includesRisk management plan by:
    a. InWherever the Administrator decides to reduce the risk, he or she sets a list of safeguards to be implemented, the implementation deadline and the persons responsible,defining the Risk Treatment Plan (internal documents of the Organization),
    b. The administrator is obliged to monitor the implementation of security measures**.**

§ 9.

Technical and organizational measures necessary to implement the principles of personal data processing

1. Personal Data Administrator within the framework of**Holcim companies in Poland**manages the security of personal data through a continuous process, carried out in cooperation with users, the Data Protection Officer and the IT Systems Administrator.
2. Holcim Enterprises in Poland uses technical and organizational measures to ensure data protection when processing data, as specified in Articles 32-36 of the GDPR, in particular to ensure the integrity and confidentiality of personal data.
3. Holcim Enterprises in Poland, implementing the security policy in the field of personal data protection, have designated buildings, rooms and parts of rooms that constitute the areas of Holcim Enterprises in Poland where personal data are processed.
4. Access to places where personal data is processed is secured by a system of physical and electronic security measures and supervised by Holcim Enterprises in Poland.

5. The facilities and premises of Holcim Companies are protected by professional entities and/or authorized personnel, physically and/or electronically, including by video surveillance. Information about the use of video surveillance is available at points of entry to the premises/plants of Holcim Enterprises in Poland and on physical access barriers (e.g. fences), as well as in publicly accessible places visible to all persons entering the video surveillance area.
6. Holcim companies in Poland are part of the HOLCIM Capital Group, based in Switzerland, under which an Internal Corporate Data Processing Agreement is concluded by Holcim companies in Poland and other entities associated with Holcim. The list of entities of the Holcim Capital Group is available at **line.**
7. Holcim companies in Poland also use the following solutions to ensure data security:
    a. **Authorizations to process data**- where the following rules apply:
        1) The Administrator is responsible for granting/cancelling authorizations to process data in files (for categories of persons) in paper form and in IT systems.
        2) Each authorized person must process data only on the instructions of the controller or pursuant to legal provisions.
        3) Authorizations are granted at the request of the person's superiors.
        4) Authorizations are granted in the form of a documented scope of duties.
        5) Authorizations may be granted in the form of orders, e.g. authorization to carry out inspections, audits, perform official duties, documented instructions from the administrator in the form of an entrustment agreement.
        6) The Administrator keeps records of authorized persons in order to control the correct access to the data of authorized persons, but the records are of auxiliary nature and are not required for the purpose of zepisami RODO.
    b. **Formalized rules for the use of organizational and technical measures to protect personal data**- where the following rules apply:
        1) The Administrator is obliged to apply technical and organisational measures (security measures) adequate to the threats of violation of the rights and freedoms of persons.
        2) The administrator has developed internal data security management proceduresand infrastructure, in which security measures are described in terms of implementation, application, maintenance and continuous improvement.
        3) Proceduressąupdated as necessary after a risk analysis/impact assessment.
    c. **ProcedurePersonal Data Protection**- where the following rules apply:
        1) Procedure(understood as security) is intended to provide knowledge to persons processing personal data regarding safe processing principles here.
        2) After becoming familiar with the principles of personal data protection, individuals are obliged to confirm their knowledge of these principles and declare their compliance.
    d. **Data protection training**- for which the following rules apply:
        1) KBefore being allowed to work with personal data, each person must undergo training or be familiarized with the provisions of the GDPR.
        2) The IOD is responsible for conducting the training.
        3) In the event of internal training on personal data protection principles it is documented by the methods implemented in the Organization.
        4) After training in the principles of personal data protection, participantsk confirms knowledge of these rules and undertakes to apply them.
    e. Structured **rules incident handling**:
        1) INexternal document(procedure):

a) defines a catalogue of vulnerabilities and incidents that threaten the security of personal data and describes how to respond to them,
b) aims to minimize the effects of security incidents and reduce the risk of threats and incidents in the future.

2) Each person authorized to process personal data is obliged to notify their immediate superior (or the Data Protection Officer) of the discovery of a vulnerability or the occurrence of an incident.
3) Typical personal data security vulnerabilities include:
   a) inadequate physical security of premises, equipment and documents,
   b) inadequate protection of IT equipment and software against leakage, theft and loss of personal data,
   c) failure to comply with the personal data protection rules by employees (e.g. failure to apply the clean desk/screen rule, password protection,not lockingrooms, wardrobes, desks).
4) Typical personal data security incidents include:
   a) external random events (fire in the facility/room, flooding, loss of power, loss of communication),
   b) internal random events (server, computer, hard drive, software failures, IT and user errors, data loss/misplacement),
   c) intentional incidents (breaking into the IT system or premises, theft of data/equipment, information leakage, disclosure of data to unauthorized persons, conscious destruction documents/data, action of viruses or other malicious software).
5) If an incident is detected, the DPO conducts an explanatory proceeding, which:
   a) determines the scope and causes of the incident and its possible consequences,
   b) initiates possible disciplinary actions,
   c) works to restore the organization's operations after an incident occurs,
   d) recommends preventive (preventive) actions aimed at eliminating similar incidents in the future or reducing losses when they occur.
6) The Administrator documents all the above-mentioned personal data protection violations, including the circumstances of the personal data protection violation, its effects and the actions taken/remedial.
7) WITHIt is prohibited to intentionally or unintentionally trigger incidents by persons authorized to process data.
8) In the event of a personal data breach resulting in a risk to the rights or freedoms of natural persons, the Controller shall, without undue delay - if possible, no later than 72 hours after discovering the breach - report it to the supervisory authority.
9) If a personal data breach may result in a high risk to the rights or freedoms of natural persons, the Controller shall, without undue delay, notifies the data subject of such a breach.

f. **Record of processing activities**- where the following rules apply:
   1) The Administrator maintains the register in the form documented,
   2) the processor also keeps a register in documented form.
g. **Audits**- where the following rules apply:
   1) Within accordance with Article 32 of the GDPR, the Controller should regularly test, measure and evaluate the effectiveness of technical and organizational measures to ensure the security of processing,
   2) for this purpose the Administrator uses formalized rules regarding audits,

3) InIn order to document the audit, the Administrator uses internally defined rules.

h. **Rules prestoring the availability of personal data and access to them** in the event of a physical or technical incident (BCP):
   1) Within accordance with Article 32 of the GDPR, the Controller should ensure the ability to quickly restore the availability of personal data and access to them in the event of a physical or technical incident,
   2) The administrator has developed recovery procedures,which are internal documents of the Organization.

§ 10.
The rights of persons whose data are processed by Holcim in Poland

1. Holcim companies in Poland guarantee that individuals whose personal data are processed in connection with their current activities will be able to exercise the rights granted to them by applicable law.
2. In particular, every natural person whose personal data is processed in connection with the activities of Holcim Enterprises in Poland has the right to request from the Controller access to his or her personal data, to rectify, erase or limit the processing, or the right to object to the processing, as well as the right to transfer data.

§ 11.
Consequences of violating the Personal Data Security Policy

Persons violating the Personal Data Security Policy will be held accountable (disciplinary or official) or criminally.

§ 12.
Final provisions

1. Detailed rules regarding the processing of personal data are regulated in internal procedures and instructions.
2. This Policy replaces the edition of June 1, 2023 in its entirety and is subject to publication in the internal and external communication channels of Holcim Companies in Poland, including on the website www.holcim.pl .

Xavier Guesnu
President of the Management Board
Holcim companies in Poland

(document signed electronically)

Disclaimer
This document is a translation. In case of doubt, the original Polish text shall prevail.