Directive
General Data Protection

September 13, 2018

Content:

1. Introduction, scope and objective

The Holcim's General Data Protection Directive is an integral part of the Holcim Directive landscape. This directive should be read in close conjunction with the Holcim policies and directives listed in Annex 2.

1.1 APPLICABILITY OF THIS GENERAL DATA PROTECTION DIRECTIVE

1.1 Holcim Ltd and its consolidated affiliated group companies

This General Data Protection Directive applies to all officers, directors and employees of all grade and levels, and other staff, including temporary or contract staff, trainees, secondees and consultants (together "Holcim Staff") of the Holcim Ltd and its consolidated affiliated group companies ("Holcim" or the "Group")

Holcim Staff must make themselves familiar with and fully comply with this Directive when engaging in any data protection activities.

1.2 Associated Companies/ Joint Ventures

In associated companies or joint ventures where Holcim does not exercise equity or management control, the responsible Group Executive Committee Member will establish that the associated company or joint venture is aware of this Directive and will encourage its adoption or at least essentially equivalent standards by such associated company or joint venture.

1.3 Third Parties

This Directive should also me made binding for Holcim's suppliers, service providers, other business partners and third parties to the extent they perform data processing services for Holcim. Appropriate provisions should be incorporated into any service, contractor or other agreements with such third parties.

1.2 CONTENT IN SCOPE

This Directive sets the overarching framework of Holcim's data protection rules and procedures. It should be read in conjunction with Holcim's other relevant policies, guidelines and procedures relating to data protection and data security matters as detailed in Annex 2 to this Directive.

The Directive defines and explains the rules and principles applied by Holcim when processing personal data of our employees, customers and any other individuals who are in contact with us. It describes how we collect and process personal data and which procedures we have in place to protect and safeguard such personal data.

If you have any questions in respect of this Directive, please contact any member of the Data Protection Team as specified below.

2. DIRECTIVE PRINCIPLES

2.1. Fair processing principles

Personal data shall always be

a) processed lawfully, fairly and in a transparent manner in relation to the data subject (lawfulness, fairness and transparency);

b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes (purpose limitation);

c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (data minimisation);

d) accurate and, where necessary, kept up to date; inaccurate data, having regard to the purposes for which they are processed, should be erased or rectified without delay (accuracy);

e) stored only as long as necessary for the purposes for which they are processed or otherwise permitted or required by applicable law (storage limitation); and

f) protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (integrity and confidentiality).

2.2. Legal grounds

Personal data must be processed on the basis of valid legal grounds. Valid legal grounds are given if and to the extent any of the following conditions applies:

a) The consent of the data subject has been obtained.

b) Processing is necessary for Holcim to comply with a legal obligation.

c) Processing is necessary for Holcim to perform a task carried out in the public interest or in exercise of official authority vested in us.

d) Processing is necessary for Holcim to perform or enter into a contract with the data subject.

e) Processing is necessary for Holcim to protect the vital interests of a data subject or another person.

f) Processing is necessary for the purposes of legitimate interests pursued by Holcim or a third party unless there are overriding interests, rights or freedoms of the data subject.

2.3. Accountability

Holcim has established appropriate rules and procedures to demonstrate compliance of its data processing activities with applicable law and this Directive, in particular with the principles of fair data processing. This includes in particular documenting processing activities in the Records of Processing Activities and conducting data privacy assessments where required (please refer to Section 10).

Where no such specific rules apply, Holcim Staff must create and maintain appropriate documentation demonstrating such compliance of their specific data processing activities. This must include at least any information required to demonstrate

(a) the legal grounds and the purposes of processing and

(b) compliance with the fair processing principles set out above in this Section.

Holcim Staff must notify the local data protection responsible of any personal data processing activities and confirm adequateness of their documentation.

3. USER ROLES AND ACCESS RIGHT CONCEPT

Access to any personal data processed by Holcim must be strictly limited on a need-to-know basis. Responsible Holcim Staff must define a user role for each function or group of functions which has a need to access the data. Holcim Staff who do not belong to a user role may not get access to the personal data. The scope of access must be differentiated and limited for each user role to the minimum scope of data required for the purposes for which the data are processed and the tasks and responsibilities of the relevant user role. The access right concept detailing the access rights for each user role must be transparently documented in written form and must be easily available for review and inspection. Access right concepts should be approved by the local data protection responsible.

4. SENSITIVE DATA AND CHILDREN'S DATA

4.1. Processing conditions

Notwithstanding Section 2.2 above, valid legal grounds for processing of personal data of children under the age of 16 (or other age limit defined under applicable law) or Sensitive Data (as defined below) are given only if and to the extent any of the processing conditions under applicable law applies, in particular if

a) The data subject has given its explicit consent, unless we are prohibited by the applicable law to rely on such consent.

b) The relevant personal data have been manifestly made public by the data subject.

c) The Processing is necessary for Holcim to carry out obligations under employment, social security or social protection law, or a collective agreement.

d) The Processing is necessary for Holcim to establish, exercise or defend against legal claims or where courts are acting in their judicial capacity.

Holcim Staff must contact the Data Protection Team and obtain approval prior to commencing any processing of Children's' Data or Sensitive Data. Any such processing activities must be documented in the Record of Processing Activities.

4.2. Definition

"Sensitive Data" for purposes of this Directive are personal data concerning racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sex life or sexual orientations, criminal record, health data, genetic data and biometric data.

5. AUTOMATED DECISION MAKING / PROFILING

5.1. Our legal obligations

Holcim must protect the rights of individuals in relation to any automated decision making, including profiling. This applies to the following situations:

a) Holcim takes decisions which produce legal effects or similarly significantly affect individuals are taken based solely on automated processing, i.e. without any human intervention (automated decision making) or

b) Holcim uses personal data to evaluate, analyse or predict certain aspects concerning an individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour or location and movement by automated processing.

Automated decisions are only admissible if they are:

a) necessary to enter into, or to perform, a contract with the individual,

b) authorised by the applicable law; or

c) based on the individual's explicit consent.

5.2. How we comply

Before any personal data are processed in any of the above situations, Holcim must take suitable safeguards to protect the rights of individuals concerned. Holcim Staff must notify the Data Protection Team of any business activities which may involve automated decision making or profiling.

The Data Protection Team approves the processing activity only if the following processes are implemented and documented:

a) Individuals are specifically informed about the automated decision making and the logic behind it.

b) Individuals have the right to obtain human intervention, express their point of view and request that the decision taken is explained to them.

c) Individuals have the right to challenge the decision.

6. INFORMATION OF DATA SUBJECTS

6.1. Our legal obligations

Where personal data relating to an individual data subject are collected from the data subject or a third party, Holcim must provide the data subject with certain information as defined by applicable law in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for information addressed specifically to a child.

A data subject means an identified or identifiable natural person whose personal data is subject to processing.

6.2. How we comply

Holcim has established procedures to ensure that all individuals concerned are informed timely, comprehensively and transparently in accordance with applicable law. Information is provided to data subjects through Holcim's general Data Privacy Notice which is available on the Holcim Data Privacy website (Holcim Data Privacy Webpage) and through additional information given in specific circumstances as required and appropriate.

The details and procedures are set out in the relevant Holcim guidelines which must be observed by all Holcim Staff. Any information to data subjects must be approved by the Data Protection Team. Holcim Staff must promptly notify the Data Protection Team if they are in doubt whether individuals concerned are properly informed about any of their data processing activities.

7. DATA SUBJECT RIGHTS

7.1. Our legal obligations

Under certain circumstances and subject to certain exemptions, individuals whose personal data are being processed by Holcim (e.g. employees, customers or other business partners) may have the following rights in relation to their personal data under applicable law:

d) Rectification of inaccurate or incomplete personal data.

e) Restriction (pausing or stopping) processing of their personal data.

f) Erasure (deletion) of their personal data.

g) Objection against the processing of their personal data.

h) Data Portability: Request that their personal data are delivered in a structured, commonly used and machine readable format either to themselves or directly to a third party if technically feasible.

7.2. How we comply

Holcim has established procedures to ensure that Holcim complies with data subject rights and timely, comprehensively and transparently responds to any data subject requests.

The details and procedures are set out in the relevant Holcim guidelines which must be observed by all Holcim Staff. The Data Protection Team is responsible for dealing with and responding to any data subject requests. Holcim Staff must promptly notify the Data Protection Team of any data subject requests and cooperate with the Data Protection Team in accordance with the relevant guidelines. Data protection requests are properly documented and recorded by the Data Protection Team.

7.3. Dealing with data subjects and other data protection matters

The Data Protection Team is exclusively responsible for any data subject requests, complaints, claims, questions, requests and any other communication or dealings with data subjects or other third parties (e.g. the media) in relation to data protection matters.

Any such matters must be immediately reported to the Data Protection Team.

8. DIRECT MARKETING

8.1. Express consent must be obtained from the individuals concerned prior to sending any marketing communication to an individual (including contact persons working for a customer organization), unless

a) we have obtained such individual's contact details during a previous order and the marketing relates to similar products and services as previously ordered and

b) the individual has not expressly objected to receiving marketing communication and

c) the individual is clearly and distinctly given the opportunity to object to any marketing communication, free of charge and in an easy manner.

8.2. Holcim Staff must therefore comply with the following rules prior to sending any advertising or marketing material to specified individuals:

a) You should not send marketing material by email unless the recipient has expressly consented in advance or Holcim has obtained their email address in the course of providing similar products or services to them (or in the course of negotiating to do so).

b) Individual's consent (marketing permission) must be obtained for any relevant communication channel you intend to use (e.g. email, telephone calls and SMS) and must be clearly and properly documented to demonstrate compliance and handle objections. Consent forms and mechanisms to store and document consent must be approved by the Legal and the Data Protection Team.

c) You must ensure that individuals who have notified us that they do not want to receive marketing material or who have withdrawn their consent are not contacted. Appropriate registers must be maintained for reference to ensure that Holcim complies with this obligation.

d) Any direct marketing message must clearly and distinctly give the individual the opportunity to object to any marketing communication, free of charge and in an easy manner. Relevant wording must be approved by the Legal and the Data Protection Team.

9. TRANSFER OF PERSONAL DATA

Personal data may be transferred to recipients within Holcim Group or to third parties only to the extent such transfer is permitted under applicable law, required and appropriate.

Holcim has established a Data Transfer Guideline which describes legal requirements for data transfers and procedures to be observed by Holcim Staff in detail.

In particular, the following rules apply to personal data transfers:

9.1. Third Party Transfers

Holcim has established procedures to ensure that any transfer of personal data to a third party recipient, whether acting as processor on behalf of Holcim or as controller, complies with applicable law. In particular, any such data transfer must be based on an appropriate data processing agreement which complies with the requirements under applicable law. These requirements apply in particular when we engage third party vendors and service providers (such as IT service providers, payroll providers, IT freelancers or data destruction companies) who process personal data on our behalf.

Holcim has established guidelines on engaging vendors and entering into data processing contracts with recipients of personal data which explain how to identify data transfers and the legal requirements for the required processing agreements. They also set out the applicable Holcim procedures which must be observed by all Holcim Staff.

The Data Protection Team and the Holcim legal functions are responsible for supporting Holcim Staff in identifying data transfer situations, assessing if a data transfer is permitted and concluding the appropriate contractual agreements. Such agreements should oblige third party vendors who process personal data on our behalf to comply with this Directive accordingly.

Holcim Staff must promptly notify the Data Protection Team of any data transfer situations and of any data transfer agreements concluded. Data transfer agreements must be properly documented and recorded.

9.2. Cross-border Transfers

A transfer of personal data to a recipient located in a country outside of the EU/EEA that does not provide adequate data protection safeguards, is only admissible if additional safeguards accepted under applicable law are taken. Such safeguards include in particular agreeing with the recipient the standard contractual clauses adopted by the European Commission or similar legal instruments approved by a supervisory authority.

Holcim Staff must comply with the specific procedures for cross-border data transfers as set out in the Holcim Data Transfer Guidelines.

9.3. Intra-Group Transfers

The above principles apply to personal data transfers between Holcim Group affiliates ("Intra-Group Transfers") accordingly, as there is no legal privilege for such transfers.

In order to avoid a multitude of bilateral agreements, Holcim has established a Intra Group Data Transfer Agreement which covers the key intra-group data streams and serves to meet the accountability and documentation requirements under applicable data protection law.

Prior to starting any business activity that may result in an Intra-Group Transfer, Holcim Staff should notify the Data Protection Team. The Data Protection Team will confirm whether the data transfer is permitted by applicable law, covered by the Intra Group Data Transfer Agreement and make any amendments to the Intra Group Data Transfer Agreement which may be required.

10. RECORDS OF PROCESSING ACTIVITIES

10.1. Maintaining the Holcim Records

Holcim maintains records of personal data processing activities to the extent required by the applicable law and in accordance with applicable law for each legal entity within Holcim Group.

The Data Protection Team is responsible for maintaining and updating the records.

10.2. Notification of processing activities

Holcim Staff members and organizational functions (e.g. HR, Sales, IT, IT Security, Accounting) who use, sponsor, monitor, manage or are otherwise involved in a processing activity must notify the Data Protection Team of the processing activity as early as possible (e.g. already in the planning phase of a project). In case of doubt, Holcim Staff must contact the Data Protection Team to obtain guidance whether a processing activity must be included in the Records.

A processing activity is any business activity, technology, product, service, IT system or application and any other activity which involves processing of personal data.

Examples: New products which process personal data (e.g. a smart meter), a camera surveillance system, an access control system, a new customer data base, a new employee performance review system, GPS location of company vehicles, a cashless pay system for the cafeteria, outsourcing of activities or functions to a third party.

11. PREVENTION OF "SHADOW IT"

Holcim Staff are not permitted to engage in any processing of personal data which has not been reviewed for compliance with data protection law and approved by the Data Protection Team (also known as "Shadow IT").

Shadow IT may expose Holcim to significant legal, reputational and financial risks for the following reasons:

a) Shadow IT is not included in record of processing activities and, thus, cannot be included in responses to data subject requests.

b) Compliance with data protection law requirements is not monitored and ensured.

c) Data breaches in Shadow IT are not monitored and, thus, cannot be reported timely to the authorities or data subjects.

d) Data security standards may fall short of Holcim standards.

12. DATA PROTECTION IMPACT ASSESSMENTS

12.1. Our legal obligations

If required by the applicable law Holcim entities shall conduct and document a data protection impact assessment ("DPIA") for certain types of "high risk" data processing activities.

The DPIA is an "assessment of the impact of a planned data processing activity on the protection of personal data". It is only required, if an activity is "likely to result in a high risk for the rights and freedoms of natural persons".

12.2. How we comply

Holcim has developed a DPIA process on the basis of the guidance of the supervisory authorities which is managed by the Data Protection Team and supported by the owners and staff involved in relevant processing activities. The details and the process are defined in the Holcim DPIA Guidelines which must be complied with by Holcim Staff.

Holcim Staff members who own or are involved in a processing activity which may require a DPIA must notify the Data Protection Team as early as possible (e.g. already in the planning phase of a project). The DPIA must be carried out prior to starting the processing activity. It should be started as early as is practicable in the design of the processing operation even if some of the processing operations are still unknown.

No processing activities which may require a DPIA may commence prior to approval by the Data Protection Team and completion of the DPIA (where required).

The Data Protection Team is responsible for appropriately documenting the DPIA and its result, including any information gathered, identified risks, advice of the Data Protection Officer (DPO), decisions and their reasons as well as remedial measures taken.

Holcim Staff remains primarily responsible to monitor the activity and notify the Data Protection Team of any changes which may require a DPIA. The Data Protection Team is responsible for determining adequate audit and updating cycles to confirm continuing compliance of the processing activity.

13. DATA RETENTION AND DELETION DIRECTIVE

Personal data may not be retained and stored for longer than required. This means that Holcim needs to delete personal data when

a) they are no longer needed for the legitimate purposes for which they had been processed,

b) we are no longer required under applicable law or by order of an authority to retain them and

c) no exemption applies which requires or permits that we continue to retain the data.

An exemption will typically apply if we need the data for the establishment, exercise or defence of legal claims.

Holcim Data Retention and Deletion Directive implements these legal requirements which must be complied with by all Holcim Staff. Holcim Data Retention and Deletion Directive is complemented by local policies which define the specific retention periods applicable to the relevant jurisdiction or entity and other local rules and procedures.

14. PRIVACY BY DESIGN & DEFAULT

Privacy by Design & Default applies as a principle for the lawfulness of processing of personal data under applicable law.

Applying Privacy by Design & Default at Holcim means the following:

a) Privacy by Design: From the beginning of any new service or business process that makes use of personal data we must take action (such as pseudonymisation) to minimise personal

data processing and comply with the data protection laws principles (such as data minimisation).

b) Privacy by Default: We must take action to ensure that, by default, in each business activity we only process the personal data that are necessary, to an extent that is necessary, and only store data as long as necessary for the purpose.

Holcim has established a Privacy by Design & Default Guidelines which gives Holcim Staff practical guidance on how to apply Privacy by Design & Default in practice and explains Holcim's relevant procedures which must be observed by all Holcim Staff.

15. DATA SECURITY

15.2. Holcim Data Security Standards

Holcim must implement appropriate state of the art technical and organisational measures to protect the integrity and security of personal data and prevent accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Data security standards applied shall include inter alia the following:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

The Holcim data security standards shall be constantly monitored and regularly audited for continuing adequateness and compliance with applicable law.

The Data Protection Team is responsible for providing appropriate training to Holcim Staff in relation to compliance with the data security policies.

Supervisors, Human Resources and other functions in charge are responsible for enforcing the data security policies and ensuring that any breach results in appropriate disciplinary action and additional training or support, where appropriate.

16. DATA BREACH RESPONSE PROCEDURE

Holcim has established a Data Breach Response Procedure which defines the processes and measures to:

a) respond to a Data Breach, including the immediate steps and measures that must be taken when a Data Breach is identified to mitigate any damage and risk to Holcim or affected individuals, as well the roles and responsibilities for managing a response to a Data Breach; and

b) comply with the Company’s relevant obligations under applicable privacy and data protection legislation, including any obligations to timely notify Data Breaches to supervisory authorities or affected individuals.

A "Data Breach" is any actual or suspected breach of security leading to the accidental or unlawful destruction, loss or loss of access to, alteration, unauthorised disclosure of or access to, or other misuse involving Holcim Data, in particular personal data.

All Holcim Staff and any contractors who process personal data on behalf of Holcim must make themselves familiar and comply with the Data Breach Response Procedure.

17. BREACH OF THIS DIRECTIVE

All Holcim Staff are required to make themselves familiar and comply with this Directive. Breaches of this Directive may give rise to disciplinary procedures and may result in disciplinary sanctions.

18. SUPPORTING DOCUMENTATION

The Group Executive Committee mandates the Holcim Data Protection Committee to adopt any necessary supporting documentation for the implementation of this Directive such as Procedures and Guidelines.

2. Requirements and related MCS

As per the MCSs)Control no. 11 (Personal data protection) applicable versions.

3. Reporting

1. Corporate level

a) Holcim Group Executive Committee

The Group Executive Committee approves creating, changing or suspending this General Data Protection Directive.

b) Group Data Protection Committee responsible for the area covered by the Directive

Group General Counsel and Compliance Officer, Group HR Director, Group Finance Director and Group Chief Information Officer are responsible for the area covered by the General Data Protection Directive, for approving any necessary supporting documentation for the implementation of this Directive such as Procedures and Guidelines, and for submitting the changes to this General Data Protection Directive to the Group Executive Committee approval.

c) Group Data Protection Officer ("DPO") and Group Data Management Office (“DMO”)

Group Data Protection Officer leads the activity of the Group Data Management Office and promotes data protection compliance and best practice in setting and maintaining standards and procedures across the Group. The DPO evaluates the existing data protection framework to identify potential gaps in data protection processes within all Group subsidiaries.

The DPO advises, monitors and reports on the implementation of this Directive, maintains, proposes amendments and revises where necessary the Group General Data Protection Directive and its supporting documentation (Directives, Procedures, Guidelines).

The DPO acts as the independent Responsible Person for Data Protection in accordance with relevant data protection laws including but not limited to Swiss Federal Data Protection Act (DSG) and European General Data Protection Regulation. Locally appointed Data Protection Officers (where required by the applicable law), Data Protection Responsibles are functionally responsible to the DPO in the area of Data Protection.

2. **Country level**

Country CEO

Each country CEO is responsible for the Group Company's compliance with this Directive and shall delegate responsibilities for specific tasks to the local data protection responsible and to different organizational functions and units.

Country CEO checklist – When applicable

The Country CEO needs to:

- Ensure the implementation of the MCSs Control no. 11
- Direct the applicable function managers to implement the technical and organizational measures to protect the personal data processed by the company and to document such measures
- Direct the applicable function managers to ensure that relevant employees under their supervisor receive data protection training relative to their work responsibilities
- Ensure data breaches are reported and required measures are taken in a timely manner as per the local law requirements.

Document Control			
Approved by:	Responsible Group Executive Committee Member: Jan Jenisch, Group Chief Executive Officer, Keith Carr, Group General Counsel Responsible Person: Christopher Wright, Head of Group Compliance; Catalin Olarescu, Head of Data Management Office		
Related Directive, Directives and MCS	Information Systems User Directive		
Version control			
Version Number	Date Issued	Author	Update information
01	13 September 2018	Catalin Olarescu, Head of Data Management Office	
02	28 February 2020	Catalin Olarescu, Head of Data Management Office	Reclassified as Directive. Introduction of section "Requirements and related MCSs"

Definitions and Abbreviations

(Alphabetical order)

Example

BoD	Board of Directors
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CFT	Corporate Financing and Treasury
CH	Corporate Holding Companies, Corporate Holdings
CLCO	Chief Legal and Compliance Officer
DPO	Data Protection Officer
DMO	Data Management Office
DPR	Data Protection Responsible
Group	Holcim Group, referring to the consolidated Group including all Corporate Holding and Operating Companies.
Group affiliated company/subsidiary	Refers to a company where Holcim has control, regardless of whether it is a Corporate Holding company or an Operating Company. When it is referred to as a subsidiary, it comprises all its governing bodies, including its board, board committees and executive management.
HR	Human Resources
IDTA	Intra Group Data Transfer Agreement
MCS	Minimum Control Standards