# Policy / Политика

## General Data Protection / Общие правила защиты персональных данных

February 28 2020 / 28 февраля 2020 г.

## 1. Introduction, scope and objective

The LafargeHolcim's General Data Protection Policy is an integral part of the LafargeHolcim Directive landscape. This policy should be read in close conjunction with the LafargeHolcim policies and directives.

### 1.1. Applicability of this General Data Protection Policy

1.1. LafargeHolcim Ltd and its consolidated affiliated group companies

This General Data Protection Policy 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 "LafargeHolcim Staff) of the LafargeHolcim Ltd and its consolidated affiliated group companies ("LafargeHolcim" or the "Group")

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

## 1. Введение, область действия и цель

Политика «Общие правила защиты данных» LafargeHolcim является неотъемлемой частью комплекса директив LafargeHolcim. Эту директиву следует рассматривать в тесной связи с политиками и директивами LafargeHolcim.

### 1.1. Применимость настоящей Политики «Общие правила защиты данных»

1.1. LafargeHolcim Ltd и консолидированные аффилированные компании группы

Настоящая Политика «Общие правила защиты данных» применима ко всем должностным лицам, директорам и сотрудникам всех разрядов и уровней, а также к другому персоналу, включая временный или внештатный персонал, учеников, командируемых сотрудников и консультантов (далее — «Персонал LafargeHolcim») и консолидированных аффилированных компаний группы (далее — LafargeHolcim или «Группа»).

Персонал LafargeHolcim должен ознакомиться с настоящей Политикой и полностью ее соблюдать при выполнении любых действий по защите данных.

1.2. Associated Companies/ Joint Ventures

In associated companies or joint ventures where LafargeHolcim 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 Policy and will encourage its adoption or at least essentially equivalent standards by such associated company or joint venture.

1.2. Ассоциированные компании/ совместные предприятия

В ассоциированных компаниях или совместных предприятиях, в отношении которых LafargeHolcim не осуществляет контроль в качестве собственника или руководителя, ответственный член Исполнительного комитета Группы устанавливает, что ассоциированная компания или совместное предприятие осведомлены о настоящей Политике, и способствует принятию настоящей Политике или как минимум в существенной степени равноценных стандартов соответствующей ассоциированной компанией или совместным предприятием.

1.3. Third Parties

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

1.3. Третьи лица

Настоящая Политика также должна быть обязательна для исполнения поставщиками товаров, поставщиками услуг, другими деловыми партнерами LafargeHolcim и третьими лицами, если они оказывают LafargeHolcim услуги по обработке данных. В соглашения об оказании услуг, договоры подряда и иные соглашения с такими третьими лицами должны быть включены надлежащие положения.

**1.2. Content in scope**

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

**1.2. Содержание Политики**

Настоящая Политика устанавливает всеобъемлющую структуру правил и процедур LafargeHolcim по защите данных. Настоящую Директиву следует рассматривать совместно с другими соответствующими политиками, руководствами и процедурами LafargeHolcim, связанными с защитой и обеспечением безопасности данных, указанными в Приложении 2 к настоящей Политике.

The Policy defines and explains the rules and principles applied by LafargeHolcim 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.

Политика определяет и разъясняет правила и принципы, применяемые LafargeHolcim при обработке персональных данных ее сотрудников, заказчиков и любых других физических лиц, которые контактируют с нами. Политика описывает, как мы собираем и обрабатываем персональные данные, и какие процедуры у нас имеются для защиты таких персональных данных.

## 2. Policy 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 minimization);

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

## 2. Принципы Политики

### 2.1. Принципы справедливой обработки

Персональные данные должны всегда:

a) обрабатываться на законных основаниях, справедливо и прозрачно по отношению к субъекту данных (законность, справедливость и прозрачность);

b) собираться в указанных явных и законных целях и обрабатываться исключительно способом, соответствующим этим целям (целевое ограничение);

c) быть достаточными, релевантными и ограничиваться объемом, необходимым с учетом целей их обработки (минимизация объема данных);

d) быть точными и при необходимости обновляться; неточные данные необходимо незамедлительно безвозвратно удалять или исправлять с учетом целей их обработки (точность);

e) храниться только в течение срока, необходимого с учетом целей их обработки или иным образом разрешенного или требуемого в соответствии с применимым законодательством (ограничение срока хранения).

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

f) быть защищены с использованием надлежащих технических или организационных мер от несанкционированной или незаконной обработки и случайной утраты, уничтожения или повреждения (целостность и конфиденциальность).

### 2.2. Legal grounds

Personal data must be processed on the basis of the 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 LafargeHolcim to comply with a legal obligation.

c) Processing is necessary for LafargeHolcim to perform a task carried out in accordance with the legislative requirements or in exercise of official authority vested in us.

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

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

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

### 2.2. Правовые основания

Персональные данные должны обрабатываться на действительных правовых основаниях. Действительные правовые основания имеются в тех случаях и в той мере, в которых применимы какие-либо из нижеуказанных условий:

a) было получено согласие субъекта данных;

b) обработка необходима LafargeHolcim для соблюдения правового обязательства;

c) обработка необходима LafargeHolcim для выполнения задачи, обусловленной требованиями действующего законодательства, или в рамках реализации предоставленных нам официальных полномочий;

d) обработка необходима LafargeHolcim для исполнения или заключения договора с субъектом данных;

e) обработка необходима LafargeHolcim для защиты жизненно важных интересов субъекта данных или иного лица;

f) обработка необходима для соблюдения законных интересов LafargeHolcim или третьего лица (в отсутствие преимущественных прав или свобод субъекта данных).

### 2.3. Accountability

LafargeHolcim 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, LafargeHolcim 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.

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

### 2.3. Отчетность

LafargeHolcim разработала надлежащие правила и процедуры, чтобы иметь возможность продемонстрировать соответствие своих действий по обработке данных применимому законодательству и настоящей Директиве, в частности принципам справедливой обработки данных. Это включает, в частности, документирование действий по обработке данных в Записях о действиях по обработке данных и при необходимости проведение оценки защиты персональных данных (см. раздел 10).

Если не применяются специальные правила, Персонал LafargeHolcim должен создать и вести надлежащую документацию, демонстрирующую соответствие ее конкретных действий по обработке данных применимому законодательству и настоящей Директиве. Такая документация должна включать, как минимум, любую информацию, которая необходима, чтобы продемонстрировать:

(a) правовые основания для обработки и цели обработки;

(b) соответствие принципам справедливой обработки данных, приведенным выше в настоящем разделе.

Персонал LafargeHolcim должен уведомлять местное ответственное лицо по защите данных о любых действиях по обработке персональных данных и подтверждать их надлежащее документирование.

## 3. User Roles and Access Right Concept

Access to any personal data processed by LafargeHolcim must be strictly limited on a need-to- know basis. Responsible LafargeHolcim manager must define a user role for each function or group of functions which has a need to access the data. LafargeHolcim 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.

## 3. Роли пользователей и концепция прав доступа

Доступ к любым персональным данным, которые обрабатывает LafargeHolcim, должен быть строго ограничен по принципу служебной необходимости. Ответственный за обработку персональных данных LafargeHolcim должен определить роль пользователя для каждой функции или группы функций, в рамках которых необходимо иметь доступ к данным. Персонал LafargeHolcim, к которому неприменима определенная роль пользователя, не может получить доступ к соответствующим персональным данным. Объем доступа для каждой роли пользователя должен быть дифференцирован и ограничен минимальным объемом данных, необходимым в целях обработки данных, и минимальным объемом задач и обязанностей, предусмотренных для соответствующей роли пользователя. Концепция права доступа, определяющая права доступа для каждой роли пользователя, должна быть четко зафиксирована в письменной форме и должна быть доступна для ознакомления и проверки. Концепции права доступа должны быть утверждены местным ответственным лицом по защите данных.

## 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.

## 4. Конфиденциальные данные и данные детей

### 4.1. Условия обработки

Невзирая на раздел 2.2 выше, действительные правовые основания для обработки персональных данных детей в возрасте до 16 лет (или в другом возрасте, определенном в соответствии с применимым законодательством) или Конфиденциальных данных (в соответствии с приведенным ниже определением) имеются в тех случаях и в той мере, в которых применимы какие-либо из условий обработки данных в соответствии с применимым законодательством, в частности если:

a) субъект данных дал свое явное согласие, если применимое законодательство не запрещает нам полагаться на такое согласие;

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

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

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

LafargeHolcim 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 Policy 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**

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

b) субъект данных явно сделал соответствующие персональные данные общедоступными;

c) обработка необходима LafargeHolcim для выполнения обязательства, предусмотренного трудовым законодательством, законодательством о социальном страховании или социальной защите или коллективным договором;

d) обработка необходима LafargeHolcim для подачи, обоснования иска или защиты по иску или для исполнения законных требований суда.

До начала любой обработки данных детей или Конфиденциальных данных работник LafargeHolcim должен получить согласие по защите данных на их обработку. Любые такие действия по обработке данных должны быть зафиксированы в Записях о действиях по обработке данных.

**4.2. Определение**

Термин «Специальная категория персональных данных» для целей настоящей Политики означает персональные данные, касающиеся расовой или этнической принадлежности, политических мнений, религиозных и философских убеждений, членства в профсоюзной организации, сексуальной жизни или сексуальной ориентации, сведений о судимости, сведений о состоянии здоровья, генетических сведений и биометрических данных.

**5. Автоматическое принятие решений/формирование профиля**

**5.1. Наши правовые обязательства**

LafargeHolcim должна защищать права физических лиц в отношении любого автоматического принятия решений, включая формирование профиля. Это относится к ситуациям, в которых:

a) LafargeHolcim 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

a) LafargeHolcim принимает решения, которые имеют правовые последствия или подобным образом оказывают существенное влияние на физических лиц, исключительно на основании автоматической обработки данных, т. е. без участия человека (автоматическое принятие решений) или

b) LafargeHolcim 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.

b) LafargeHolcim использует персональные данные для оценки, анализа или прогнозирования с помощью автоматической обработки данных определенных аспектов в отношении эффективности работы, экономической ситуации, состояния здоровья, персональных предпочтений, интересов, надежности, поведения или местонахождения и перемещения физического лица.

Automated decisions are only admissible if they are:

Автоматическое принятие решений допустимо, только если это:

a) authorised by the applicable law; or

a) разрешено применимым законодательством или

b) based on the individual’s explicit consent.

b) делается с явного согласия физического лица.

**5.2. How we comply**

**5.2. Как мы обеспечиваем соблюдение нормативных требований**

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

До обработки любых персональных данных в любой из вышеуказанных ситуаций LafargeHolcim должна принять надлежащие меры для защиты прав соответствующих физических лиц. Работники LafargeHolcim должны уведомить ответственного руководителя по защите данных о любых действиях, связанных с автоматическим принятием решений или формированием профиля.

Resposible manager Data Protection approves the processing activity only if the following processes are implemented and documented:

Ответственный руководитель по защите данных одобряет действия по обработке данных, только если внедрены и документально зафиксированы следующие процессы:

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

a) физические лица информируются об автоматическом принятии решений и логике такого принятия решений;

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.

b) физические лица имеют право на вмешательство человека, выражение своей точки зрения, а также имеют право потребовать, чтобы им объяснили принятое решение;

c) физические лица вправе оспорить решение.

## 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, LafargeHolcim 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. Информация о субъектах данных

### 6.1. Наши правовые обязательства

Если персональные данные, имеющие отношение к субъекту данных — физическому лицу, собираются у субъекта данных или третьего лица, LafargeHolcim должна предоставить субъекту данных информацию, которая определяется применимым законодательством, в сжатой, прозрачной, понятной и легкодоступной форме с использованием понятного и простого языка, в частности информацию, специально адресованную ребенку.

Субъект данных означает идентифицированное или идентифицируемое физическое лицо, чьи персональные данные подвергаются обработке.

## 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 LafargeHolcim (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.

## 7. Права субъекта данных

### 7.1. Наши правовые обязательства

При определенных обстоятельствах и с учетом определенных исключений физические лица, чьи персональные данные обрабатывает LafargeHolcim (например, сотрудники, заказчики или другие деловые партнеры), в соответствии с применимым законодательством могут иметь в отношении их персональных данных право:

d) на устранение неточностей или неполноты персональных данных;

e) ограничение (временное или постоянное) обработки их персональных данных;

f) удаление (безвозвратное удаление) их персональных данных;

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.

i) refuse from transfer of personal data abroad or to any third party.

g) возражение против обработки их персональных данных;

h) переносимость данных: потребовать, чтобы их персональные данные были переданы в структурированном, широко используемом и машиночитаемом формате либо им, либо непосредственно третьему лицу, если это технически осуществимо.

i) отказаться от трансграничной передачи персональных данных и/или от их передачи третьим лицам.

### 7.2. How we comply

LafargeHolcim has established procedures to ensure that LafargeHolcim 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 LafargeHolcim guidelines which must be observed by all LafargeHolcim Staff. Responsible manager of the Data Protection is responsible for dealing with and responding to any data subject requests. LafargeHolcim Staff must promptly notify responsible manager of the Data Protection of any data subject requests and cooperate with him in accordance with the relevant guidelines. Data protection requests are properly documented and recorded by responsible staff.

### 7.2. Как мы обеспечиваем соблюдение нормативных требований

LafargeHolcim разработала процедуры, которые гарантируют соблюдение LafargeHolcim прав субъекта данных и своевременное, всеобъемлющее и прозрачное реагирование на любые запросы субъекта данных.

Подробная информация и процедуры приведены в соответствующем руководстве Группы LafargeHolcim, которое должно соблюдаться всем Персоналом LafargeHolcim. Ответственный руководитель по защите данных отвечает за обработку всех запросов субъектов данных и реагирование на них. Сотрудники LafargeHolcim должены незамедлительно уведомлять Ответственного руководителя по защите данных о любых запросах субъектов данных и вза с имодействовать с ним по вопросам защиты данных в соответствии с применимым руководством. Запросы о защите данных надлежащим образом документируются и регистрируются ответственным сотрудником.

### 7.3. Dealing with data subjects and other data protection matters

Responsible manager of the Data Protection 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.

### 7.3. Работа с субъектами данных и другими аспектами защиты данных

Ответственный руководитель по защите данных несет исключительную ответственность за обработку любых запросов, жалоб, требований, вопросов и любых других сообщений субъектов данных и за взаимодействие с субъектами данных и другими третьими лицами (например, СМИ) по вопросам защиты данных.

**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

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.** LafargeHolcim 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 LafargeHolcim 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).

**8. Прямой маркетинг**

**8.1.** Перед отправкой каких-либо маркетинговых сообщений физическому лицу (включая контактных лиц организации заказчика) необходимо получить явное согласие соответствующего физического лица на отправку, за исключением случаев, когда

a) мы получили контактные данные такого физического лица в рамках предыдущего заказа и маркетинговое сообщение относится к продуктам и услугам, подобным тем, которые были заказаны ранее, и

c) физическому лицу явным и недвусмысленным образом была дана возможность бесплатно и легко отказаться от получения любых маркетинговых сообщений.

**8.2.** Персонал LafargeHolcim должен соблюдать следующие правила до отправки любых рекламных или маркетинговых материалов указанным физическим лицам.

a) Запрещается отправлять маркетинговые материалы по электронной почте, если получатель предварительно не выразил на это явное согласие или LafargeHolcim не получила его адрес электронной почты при предоставлении ему подобных продуктов или услуг (или в процессе проведения переговоров о предоставлении таких продуктов или услуг).

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.

b) Должно быть получено согласие физического лица (разрешение на получение маркетинговых материалов) для любого соответствующего канала коммуникации, который вы намерены использовать (например, электронная почта, телефонные звонки и SMS-сообщения), при этом такое согласие должно быть четко и надлежащим образом зафиксировано документально, чтобы обеспечить возможность продемонстрировать соблюдение нормативных требований и урегулировать возражения. Бланки и механизмы для хранения и документирования согласия должны быть одобрены Юридическим отделом и Командой по защите данных.

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 LafargeHolcim complies with this obligation.

c) Необходимо убедиться в том, что маркетинговые материалы не направляются физическим лицам, сообщившим нам о своем нежелании их получать или отозвавшим свое согласие. Должны вестись соответствующие реестры в качестве справочной информации, чтобы обеспечить соблюдение этого обязательства со стороны LafargeHolcim.

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.

d) В любом прямом маркетинговом сообщении физическому лицу должна явным и недвусмысленным образом быть дана возможность бесплатно и легко отказаться от получения маркетинговых сообщений. Соответствующий текст должен быть одобрен Юридическим отделом и Командой по защите данных.

## 9. Transfer of Personal Data

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

## 9. Передача персональных данных

Персональные данные могут быть переданы получателям в Группе LafargeHolcim или третьим лицам, только если такая передача данных разрешена в соответствии с применимым законодательством и является необходимой и надлежащей.

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

LafargeHolcim разработала Руководство по передаче данных, в котором подробно описываются правовые требования в отношении передачи данных и процедуры, которые должен соблюдать Персонал LafargeHolcim.

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

В частности, к передаче персональных данных применимы следующие правила.

### 9.1. Third Party Transfers

LafargeHolcim has established procedures to ensure that any transfer of personal data to a third party recipient, whether acting as processor on behalf of LafargeHolcim 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 and if necessary – on the basis of the consent of the data subject for processing. 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.

### 9.1. Передача третьим лицам

LafargeHolcim разработала процедуры, чтобы гарантировать, что любая передача персональных данных получателю — третьему лицу, выступающему в качестве обработчика данных от имени LafargeHolcim или в качестве контролера, осуществляется в соответствии с применимым законодательством. В частности, любая такая передача данных должна осуществляться на основании надлежащего соглашения об обработке данных, соответствующего требованиям применимого законодательства, а при необходимости – на основании согласия субъекта на обработку. В частности, эти требованиям применимы, когда мы задействуем поставщиков товаров или услуг — третьих лиц (таких как поставщики ИТ-услуг, поставщики услуг по расчету заработной платы, фрилансеры в сфере ИТ или компании по уничтожению данных), которые обрабатывают персональные данные от нашего имени.

LafargeHolcim 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 LafargeHolcim procedures which must be observed by all LafargeHolcim Staff.

LafargeHolcim разработала руководство по работе с поставщиками и заключению договоров по обработке данных с получателями персональных данных, в котором разъяснено, как идентифицировать передачу данных, а также приведены требования законодательства к соглашениям об обработке данных. В нем также приведены применимые процедуры LafargeHolcim, которые должны соблюдаться всем Персоналом LafargeHolcim.

Responsible manager of the Data Protection and the LafargeHolcim legal functions are responsible for supporting LafargeHolcim 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.

Ответственный руководитель по защите данных и Юридический отдел LafargeHolcim отвечают за предоставление Персоналу LafargeHolcim поддержки в части идентификации ситуаций передачи данных, правовой оценки допустимости передачи данных и заключения соответствующих соглашений. Такие соглашения должны обязывать поставщиков — третьих лиц, обрабатывающих персональные данные от нашего имени, соответствующим образом соблюдать настоящую Директиву.

### 9.2. Cross-border Transfers

A transfer of personal data to a recipient located in a country outside of the RF 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 RF or similar legal instruments approved by a supervisory authority.

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

### 9.2. Трансграничная передача данных

Передача персональных данных получателю, который находится в стране за пределами РФ и не обеспечивает надлежащие меры защиты данных, допускается только при условии принятия дополнительных мер защиты в соответствии с применимым законодательством. Такие меры защиты включают, в частности, согласование с получателем стандартных условий договора, принятых РФ, или подобных документов правового характера, одобренных надзорным органом.

Персонал LafargeHolcim должен соблюдать специальные процедуры трансграничной передачи данных, приведенные в Политике LafargeHolcim по передаче данных.

### 9.3. Intra-Group Transfers

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

In order to avoid a multitude of bilateral agreements, LafargeHolcim has established an 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, LafargeHolcim Staff should notify responsible manager of the Data Protection. The responsible manager 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.

### 9.3. Передача данных внутри Группы

Вышеуказанные принципы применимы к передаче персональных данных между аффилированными лицами Группы LafargeHolcim (далее — «Передача данных внутри Группы»), поскольку на такую передачу данных не распространяются юридические привилегии.

Чтобы избежать использования различных версий двухсторонних соглашений, LafargeHolcim разработала Соглашение о передаче данных внутри Группы, в котором определяются ключевые потоки данных внутри Группы и которое обеспечивает соблюдение требований к отчетности и документальному оформлению, предусмотренным применимым законодательством о защите данных.

Перед началом любых действий, которые могут привести к Передаче данных внутри Группы, Персонал LafargeHolcim должен уведомить о них Ответственного руководителя по защите данных. Ответственный руководитель по защите данных должен подтвердить, разрешена ли передача данных в соответствии с применимым законодательством, распространяется ли на нее Соглашение о передаче данных внутри Группы, и внести любые необходимые поправки в Соглашение о передаче данных внутри Группы.

## 10. Records of Processing Activities

### 10.1. Maintaining the LafargeHolcim Records

LafargeHolcim 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 LafargeHolcim Group.

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

## 10. Записи о действиях по обработке данных

### 10.1. Ведение записей LafargeHolcim

LafargeHolcim ведет записи о действиях по обработке персональных данных в соответствии с применимым законодательством для каждого юридического лица Группы LafargeHolcim.

Команда по защите данных отвечает за ведение и актуализацию записей.

### 10.2. Notification of processing activities

LafargeHolcim 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 responsible manager of the Data Protection of the processing activity as early as possible (e.g. already in the planning phase of a project). In case of doubt, LafargeHolcim Staff must contact the responsible manager of the Data Protection 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"

LafargeHolcim 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 responsible manafer of the Data Protection (also known as "Shadow IT").

### 10.2. Уведомление о действиях по обработке данных

Персонал LafargeHolcim и функциональные подразделения (например, Отдел управления персоналом, Отдел продаж, Отдел информационных технологий, Отдел ИТ-безопасности, Бухгалтерия), которые используют, спонсируют, отслеживают действия, управляют действиями или иным образом задействованы в действиях по обработке данных, должны уведомлять ответственного руководителя по защите данных о деятельности по обработке данных как можно раньше (например, уже на этапе планирования проекта). В случае возникновения сомнений Персонал LafargeHolcim должен уточнить у ответственного руководителя по защите данных, должны ли действия по обработке быть включены в Записи.

Действия по обработке данных — это любые действия, технология, продукт, услуга, ИТ-система или приложение и любое другое действие, которые подразумевает обработку данных.

Примеры: новые продукты, которые обрабатывают персональные данные (например, умный счетчик); система видеонаблюдения; система контроля доступа; новая база данных заказчиков; новая система проверки эффективности работы персонала; GPS-идентификация местоположения транспортных средств компании; система безналичных расчетов для кафетерия; передача действий или функций на аутсорсинг третьему лицу.

### 11. Предотвращение Теневых ИТ

Персоналу LafargeHolcim запрещено участвовать в обработке персональных данных (также известной как Теневые ИТ), которая не была проверена в части соответствия законодательству о защите данных и одобрена ответственным рукововодителем по защите данных.

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

Теневые ИТ могут привести к возникновению у LafargeHolcim существенных юридических, репутационных и финансовых рисков по следующим причинам.

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

a) Теневые ИТ не включаются в запись действий по обработке данных и, соответственно, не могут быть включены в ответы на запросы субъектов данных.

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

b) Не отслеживается и не обеспечивается соблюдение требований законодательства по защите данных.

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

c) При Теневых ИТ не отслеживаются утечки данных и, соответственно, невозможно своевременно сообщить о таких утечках данных уполномоченным органам или субъектам данных.

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

d) Стандарты обеспечения безопасности данных могут быть ниже, чем соответствующие стандарты LafargeHolcim.

## 12. Data Protection Impact Assessments

## 12. Оценка влияния защиты данных

### 12.1. Our legal obligations

### 12.1. Наши правовые обязательства

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

Если это требуется в соответствии с применимым законодательством, компании LafargeHolcim должны выполнять оценку влияния защиты данных (DPIA) для определенных типов действий по обработке данных, которые относятся к высокому риску, и документально оформлять ее результаты.

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".

Оценка влияния защиты данных является «оценкой влияния запланированных действий по обработке данных на защиту персональных данных». Проведение такой оценки необходимо, только если «существует вероятность, что действие повлечет за собой высокий риск для прав и свобод физических лиц».

**12.2. How we comply**

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

LafargeHolcim 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.

**12.2. Как мы обеспечиваем соблюдение нормативных требований**

LafargeHolcim разработала на основе руководства надзорных органов процесс оценки влияния защиты данных, который осуществляется под управлением ответственного руководителя по защите данных и поддерживается лицами, ответственными за соответствующие действия по обработке данных и вовлеченным в них персоналом. Подробная информация и процесс приведены в Руководстве LafargeHolcim по оценке влияния защиты данных, которое должен соблюдать Персонал LafargeHolcim.

Персонал LafargeHolcim, который выступает в роли лица, ответственного за соответствующее действие по обработке данных, для которого может потребоваться оценка влияния защиты данных, или принимает в нем участие, должен уведомить об этом Команду по защите данных как можно раньше (например, уже на этапе планирования проекта). Оценка влияния защиты данных должна быть выполнена до начала действия по обработке данных. Она должна быть начата как можно раньше на этапе разработки операции по обработке данных, даже если некоторые из операций по обработке данных еще не известны.

К выполнению действий по обработке данных, для которых может потребоваться оценка влияния защиты данных, можно приступить только после их одобрения Командой по защите данных и завершения оценки влияния защиты данных (если ее выполнение необходимо).

Команда по защите данных отвечает за надлежащее документальное оформление оценки влияния защиты данных и ее результатов, включая всю собранную информацию, идентифицированные риски, консультации руководителя Отдела по защите данных (DPO), решения и их обоснования, а также предпринятые корректирующие действия.

LafargeHolcim 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.

Персонал LafargeHolcim продолжает нести основную ответственность за отслеживание действий и уведомление Команды по защите данных о любых изменениях, которые могут потребовать выполнения оценки влияния защиты данных. Команда по защите данных отвечает за определение надлежащих циклов аудита и актуализации для подтверждения постоянного соответствия действий по обработке данных установленным требованиям.

## 13. Data Retention and Deletion Directive

Personal data may not be retained and stored for longer than required. This means that LafargeHolcim 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.

LafargeHolcim Data Retention and Deletion Directive implements these legal requirements which must be complied with by all LafargeHolcim Staff. LafargeHolcim 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.

## 13. Директива о хранении и удалении данных

Запрещается хранить и удерживать персональные данные дольше, чем это необходимо. Это значит, что LafargeHolcim должна удалить персональные данные, когда:

a) они больше не требуются в законных целях, в которых они обрабатывались,

b) они больше не требуются в соответствии с применимым законодательством или указанием уполномоченного органа о необходимости их хранения и

c) не применимы никакие исключения, согласно которым мы должны или нам разрешено продолжать хранить эти данные.

Исключение обычно применимо, если нам необходимы данные, чтобы подать, обосновать иск или обеспечить защиту по иску.

Директива LafargeHolcim о хранении и удалении данных внедряет эти требования законодательства, которые должен соблюдать весь Персонал LafargeHolcim. Директиву LafargeHolcim о хранении и удалении данных дополняют местные политики, в которых определяются конкретные периоды хранения данных, применимые в соответствующей юрисдикции или для соответствующей организации, а также местные правила и процедуры.

## 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 LafargeHolcim 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.

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

## 14. Проектируемая защита персональных данных и защита персональных данных по умолчанию

Проектируемая защита персональных данных и защита персональных данных по умолчанию применима как принцип обеспечения законности обработки персональных данных в соответствии с применимым законодательством.

Применение в LafargeHolcim проектируемой защиты персональных данных и защиты персональных данных по умолчанию означает нижеследующее.

a) Проектируемая защита персональных данных. Инициируя какой-либо сервис или бизнес-процесс, который использует персональные данные, мы должны предпринять действия (такие как псевдоминимизация), чтобы минимизировать обработку персональных данных и обеспечить соблюдение принципов законодательства о защите данных (например, принципа минимизации данных).

b) Защита персональных данных по умолчанию. Мы должны предпринять действия, чтобы обеспечить в рамках каждого действия обработку только необходимых персональных данных и хранение данных только в течение срока, необходимого с учетом цели.

LafargeHolcim разработала Руководство по проектируемой защите персональных данных и защите персональных данных по умолчанию, которое является практическим руководством для Персонала LafargeHolcim в отношении того, как мы применяем на практике принципы проектируемой защиты персональных данных и защиты персональных данных по умолчанию, и в котором разъясняются соответствующие процедуры LafargeHolcim, которые должны соблюдаться всем Персоналом LafargeHolcim.

**15. Data Security**

**15.2. LafargeHolcim Data Security Standards**

LafargeHolcim 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 LafargeHolcim 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 LafargeHolcim Staff in relation to compliance with the data security policies.

**15. Обеспечение безопасности данных**

**15.2. Стандарты обеспечения безопасности данных LafargeHolcim**

LafargeHolcim должна внедрить надлежащие передовые технические и организационные меры по защите целостности и обеспечению безопасности персональных данных и предотвращению случайного или незаконного уничтожения, утраты, изменения, несанкционированного раскрытия персональных данных или доступа к передаваемым или иным образом обрабатываемым персональным данным.

Применимые стандарты обеспечения безопасности данных должны включать среди прочего:

(a) псевдоминимизацию и шифрование персональных данных;

(b) способность обеспечить постоянную конфиденциальность, целостность, доступность и работоспособность систем и сервисов по обработке данных;

(c) способность своевременно восстанавливать доступность персональных данных и доступ к ним в случае физических или технических инцидентов;

(d) процесс для регулярного тестирования и оценки эффективности технических и организационных мер обеспечения безопасности обработки данных.

Стандарты обеспечения безопасности данных LafargeHolcim должны постоянно отслеживаться и проверяться в части их соответствия применимому законодательству.

Команда по защите данных отвечает за надлежащее обучение Персонала LafargeHolcim по вопросам соблюдения политик обеспечения безопасности данных.

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.

Руководители, Отдел управления персоналом и другие ответственные функциональные подразделения отвечают за применение политик обеспечения безопасности данных, за применение надлежащих дисциплинарных мер в случае нарушений, за дополнительное обучение и за предоставление поддержки.

## 16. Data Breach Response Procedure

## 16. Процедура реагирования на утечку данных

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

Группа LafargeHolcim разработала Процедуру реагирования на утечку данных, в которой определены процессы и меры:

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 LafargeHolcim or affected individuals, as well the roles and responsibilities for managing a response to a Data Breach; and

a) реагирования на Утечку данных, включая немедленные шаги и меры в случае выявления Утечки данных, направленные на минимизацию ущерба и рисков для LafargeHolcim или задействованных физических лиц, а также роли и ответственность по управлению реагированием на Утечку данных;

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.

b) соблюдения соответствующих обязательств Компании, предусмотренных применимым законодательством о защите персональных данных, включая любые обязательства по своевременному уведомлению надзорных органов или задействованных физических лиц об Утечке данных.

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 LafargeHolcim Data, in particular personal data.

Утечка данных — это любое фактическое или предполагаемое нарушение безопасности, приведшее к случайному или неправомерному уничтожению, утрате Данных LafargeHolcim или потере доступа к ним, их изменению, несанкционированному раскрытию или получению доступа к ним либо к иному неправомерному использованию Данных LafargeHolcim, в частности персональных данных.

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

Весь Персонал LafargeHolcim и любые подрядчики, которые обрабатывают персональные данные от имени LafargeHolcim, должны ознакомиться с Процедурой реагирования на утечку данных и соблюдать ее.

**17. Breach of this Directive**

All LafargeHolcim 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 LafargeHolcim 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 Minimum Control Standard 11 (Personal data protection) applicable version.

## 3. Reporting

**1. Corporate level**

**a) LafargeHolcim Group Executive Committee**

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

**17. Нарушение настоящей Директивы**

Весь Персонал LafargeHolcim должен ознакомиться с настоящей Директивой и соблюдать ее. В случае нарушения настоящей Директивы могут применяться дисциплинарные процедуры и дисциплинарные меры.

**18. Сопутствующая документация**

Исполнительный комитет Группы приказывает Комитету LafargeHolcim по защите данных утвердить всю необходимую сопутствующую документацию для реализации настоящей Директивы, такую как Процедуры и Руководства.

## 2. Требования и соответствующий стандарт минимального контроля (MCS)

В соответствии с действующей версией Стандарта минимального контроля 11 (Защита персональных данных).

## 3. Сферы ответственности

**1. Корпоративный уровень**

**a) Исполнительный комитет Группы LafargeHolcim**

Исполнительный комитет Группы утверждает создание, изменение или приостановку действия настоящей Директивы «Общие правила защиты данных».

**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.

**b) Комитет по защите данных Группы, ответственный за сферу действия Директивы**

Генеральный юрисконсульт и должностное лицо по вопросам нормативного регулирования Группы, директор Группы по управлению персоналом, финансовый директор Группы и главный информационный директор Группы отвечают за сферу действия Директивы «Общие правила защиты данных», за одобрение любой сопутствующей документации, необходимой для реализации настоящей Директивы, такой как Процедуры и Руководства, а также за представление изменений к настоящей Директиве «Общие правила защиты данных» для их одобрения Исполнительным комитетом Группы.

**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).

**c) Руководитель Отдела по защите данных Группы (DPO) и Отдел по управлению данными Группы (DMO)**

Руководитель Отдела по защите данных Группы руководит деятельностью Отдела по управлению данными Группы и способствует соблюдению нормативных требований по защите данных и реализации передовых методик по созданию и актуализации стандартов и процедур в Группе. Руководитель Отдела по защите данных Группы оценивает существующую нормативную базу по защите данных, чтобы выявить потенциальные пробелы в процессах защиты данных во всех дочерних предприятиях Группы.

Руководитель Отдела по защите данных Группы предоставляет консультации по вопросам внедрения настоящей Директивы, отслеживает ее внедрение, предоставляет соответствующую отчетность, при необходимости актуализирует и пересматривает Директиву «Общие правила защиты данных» Группы и сопутствующую документацию (Директивы, Процедуры, Руководства).

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.

Руководитель Отдела по защите данных Группы действует в качестве независимого ответственного лица по защите данных согласно соответствующему законодательству о защите данных, включая среди прочего Федеральный закон Швейцарии о защите персональных данных (DSG) и Генеральный регламент ЕС о защите персональных данных. При назначении руководителя Отдела по защите данных на локальном уровне (если это необходимо в соответствии с применимым законодательством) ответственные лица по защите данных подотчетны руководителю Отдела по защите данных Группы в сфере Защиты данных.

## 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.

## 2. Уровень страны

### Генеральный директор на уровне страны

Каждый генеральный директор на уровне страны отвечает за соответствие Компании Группы настоящей Директиве и должен передать обязанности по выполнению определенных задач местному ответственному лицу по защите данных и различным функциональным подразделениям и отделам организации.

## Definitions and Abbreviations / Определения и сокращения

*(Alphabetical order) / (в алфавитном порядке)*

*Example / Пример*

| | |
|---|---|
| *BoD / СД* | Board of Directors /<br>Совет директоров |
| *CEO / ГД* | Chief Executive Officer /<br>Генеральный директор |
| *CFO / ФД* | Chief Financial Officer /<br>Финансовый директор |
| *CFT / КФиК* | Corporate Financing and Treasury /<br>Корпоративные финансы и казначейство |
| *CH / ХК* | Corporate Holding Companies, Corporate Holdings /<br>Корпоративные холдинговые компании, корпоративные холдинги |
| *CLCO* | Chief Legal and Compliance Officer /<br>Директор по правовому обеспечению и надзору |
| *DPO* | Data Protection Officer /<br>Руководитель Отдела по защите данных |
| *DMO* | Data Management Office /<br>Отдел по управлению данными |
| *DPR* | Data Protection Responsible / Ответственное лицо по защите данных |
| *Group / Группа* | LafargeHolcim Group, referring to the consolidated Group including all Corporate Holding and Operating Companies. /<br>Группа LafargeHolcim, что означает консолидированную Группу, включая все входящие в нее холдинговые и операционные компании |
| *Group affiliated company/ subsidiary / Аффилированная компания/дочерняя компания Группы* | Refers to a company where LafargeHolcim 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. /<br>Компания, контролируемая LafargeHolcim, независимо от того, является она холдинговой или операционной компанией Группы. Если речь идет о дочерней компании, в это понятие включаются все ее руководящие органы, в том числе совет директоров, комитеты совета директоров и исполнительное руководство |
| *HR / ОУП* | Human Resources / Отдел управления персоналом |
| *IDTA* | Intra Group Data Transfer Agreement /<br>Соглашение о передаче данных внутри Группы |
| *MCS* | Minimum Control Standards /<br>Стандарты минимального контроля |