HEIDELBERGCEMENT

Group Compliance Incident Reporting & Case Management Guideline

Applicable to:	**all companies of the HeidelbergCement Group**
Created by:	**Group Compliance**
Date of issue:	**April 2020**
Version no.:	**4.1**

Contents

1. Introduction

In its Code of Business Conduct, the HeidelbergCement Group requires all employees to observe high standards of business ethics in their duties and responsibilities. Employees and representatives of the organisation must practice honesty and integrity in fulfilling their responsibilities and must comply with all applicable laws and regulations.

The objective of this Guideline is to provide instructions and principles for

- the submission of compliance-related concerns by employees, directors and officers of HeidelbergCement, on a confidential and, if preferred, anonymous basis,
- the processing and treatment of submitted complaints/incident reports,
- the protection of persons reporting concerns against retaliatory actions.

This Guideline was first issued in February 2012; this version replaces the previous one and takes immediate effect; it applies to all companies of HeidelbergCement Group[1] and is addressed to all employees of HeidelbergCement Group companies.

Special compliance guidelines (e.g. purchasing, tax, treasury, etc.) might specify additional requirements.

2. Why report an incident?

One of the pillars of the HC compliance programme is to ensure rapid alert in any case of actual or potential compliance incidents; the main tool in this respect is to have a reporting system in place which encourages and enables employees to disclose any observations of non-compliant behaviour and address them in the right way to the relevant persons in the organisation.

Furthermore, to best benefit from the implementation of Group-wide proactive measures to avoid non-compliant conduct, it is required that every single incident is recorded and analysed.

It is important to report at an early stage to allow the issue to be addressed quickly before it escalates further.

It is in the interest of every employee to retain a positive public perception of HeidelbergCement.

[1] HeidelbergCement AG and all companies controlled directly or indirectly by HeidelbergCement AG; for joint entities the definition and the rules of the Group Compliance Policy apply as well for this Guideline.

3. Which types of incidents should be reported?

In principle, every kind of infringement of applicable laws and internal policies or reasonable suspicion of such is to be disclosed. In particular this refers to concerns in the fields of:

- **Accounting / audit-related matters** (the purposeful, unethical or questionable recording of accounting or auditing matters. Examples may include: fraud; deliberate errors related to financial statements; non-compliance with accounting controls; misinterpretations or false statements to or by senior officers regarding financial records; or deviation from full and fair reporting of the company's financial condition).
- **Alcohol and drugs** (actual or suspected consumption of drugs and/or alcohol which affects or has the potential to affect an employee's or contractor's health and safety performance at work and/or his/her ability to undertake all aspects of their work; breach of the company Drugs and Alcohol Policy as far as applicable).
- **Antitrust/unfair or illegal competition or marketing** (including for example alleged price fixing, output restriction, customer or territory allocation each if agreed with competitors or alleged abusive behaviour in a dominant market position like inappropriate pricing, price discrimination or abusive loyalty rebates and bundling/tying of product sales).
- **Child or forced labour / child abuse** (abuse of children for child labour or of adults for forced labour/modern slavery; any act or failure to act which results in death, serious physical or emotional harm, sexual abuse or exploitation of a child; or which presents imminent danger or serious harm to a child).
- **Conflict of interest** (a situation where a person in a position of trust has competing professional and/or personal interests which can make it difficult to impartially perform the assigned job duties).
- **Compliance or regulatory violation** (violations of or failure to comply with a rule, regulation, law, operating procedure, past practice or protocol for any aspect of the company, incl. antitrust/competition law violations).
- **Corruption / bribery / kickbacks** (the offering or acceptance of money or other incentives to persuade someone to do or not to do something, especially something illegal, improper or unethical).
- **Cybercrime** (criminal activities carried out by means of computers or the internet; includes data security issues- improper disclosures or theft of the company's confidential or proprietary information/data; data breaches to be reported as separate incident type).
- **Data breach / breach of privacy** (data breach is a security incident in which personal data is copied, transmitted, viewed, stolen or used by an individual unauthorised to do so. Personal data is all kind of data that may serve identifying a human being (e.g. name, photo, religion).
- **Discrimination** (the unlawful discrimination of individuals based on an individual's race, colour, ancestry, ethnicity, gender (sex), age, religion, national origin, level of education, political affiliation, physical appearance or disability, marital status, pregnancy or sexual orientation).
- **Embezzlement** (the wilful and intentional taking of money or property by a person who has been entrusted with the money or other assets for that person's own or a third/related party's use or gain).
- **Employee relations** (any material issues related to the way employees work with each other, their supervisors/managers, and the company. Examples include job related actions like promotions, job or shift changes, terminations, disciplinary actions and performance issues, if carried out improperly or in breach of legal requirements).
- **Environmental issues / sustainability** (the potential for direct or indirect damage to the environment by a wilful or negligent act. Examples include the illegal or unintentional discharge of pollutants, poisons, hazardous wastes, radioactive chemicals, or any other contaminants, that kill or do harm, or have the potential to cause environmental damage).

- **Fraud** (the dishonest practice of obtaining money or property through intentional use of false pretences, false documents, or misrepresentation. An illegal taking of assets or property of value).
- **Harassment** (unwanted, on-going verbal or physical behaviour of an inappropriate nature. The unwarranted threat to cause bodily or emotional harm to another person or harm to another person's property. Examples may include acts of threatening, intimidating, stalking, taunting, gesturing, excessive staring, pestering, hang-up and nuisance telephone calls, obscene telephone calls, abusive postal mail, or improper e-mails).
- **Health & safety** (under-reporting of accidents, any workplace condition that potentially compromises the health, safety, and well-being of employees, customers, vendors, or visitors. Such conditions may include: poor lighting or signage; unstable stacking or storage of materials, products, or equipment; exposure to hazardous materials or contaminants; exposure to excessive noise; lack of protection against weather elements; walkways, floors, or stairways in disrepair; or unnecessary exposure to dangerous machinery. Such workplace conditions may also constitute a breach of relevant legislation).
- **Money laundering** (the process through which proceeds of crime and their true origin and ownership are changed so that the proceeds appear legitimate).
- **Theft** (the illegal taking of any form of property belonging to someone else without consent. The intent is to permanently deprive the owner of property).
- **Unethical or illegal conduct involving customers or vendors** (improper conduct involving customers or vendors such as a sales person taking advantage of a customer or a vendor treating an employee unfairly. If conduct involves Antitrust/Unfair competition, Fraud, Corruption/Bribery, Discrimination, Health & Safety, Harassment, or another category, we use the specific incident type, not unethical or illegal conduct).
- **Other compliance-related issues,** which are not covered by the above-listed types.

Any reasonable suspicions of such infringements should be raised at the **earliest possible stage**. Investigating the matter first by oneself and trying to produce evidence before reporting it might unnecessarily delay the matter and can cause adverse effects (e.g. existing evidence being destroyed). Investigations shall be conducted in-depth by assigned investigators (see section 5).

4. How to report an incident

4.1. *General reporting instructions*

In order to facilitate an efficient and effective investigation, the reporting employee should disclose as much precise information as possible based on the following questions:

- **Who** acted? - full names of suspected individuals and potential witnesses
- **What** happened? - brief but precise overview
- **When** did it happen?
- **Where** did it happen? - name and address of the site/plant where the incident has taken place
- **Why** did it happen? – reasons/factors that led to the incident (background information)
- **How** did it happen? - course of events

4.2. *Reporting Channels*

The **direct superior** should be the first point of contact in case of any suspicions of infringements of applicable laws or internal regulations. This direct way of addressing any issue is in many cases the easiest and most effective way for the company to investigate the alleged infringement and allows for appropriate action in the short term. This may help prevent any major damage.

However, there might be cases where, for whatever reason, employees are not able to confide in their direct superior. In this case one of the following reporting channels should be used:

- the next **superior hierarchy level**,
- the **Legal** or **Compliance department** or other corporate function such as **Human Resources**, **Environment** or **Health & Safety** or
- the **Compliance Reporting Line "SpeakUp"**.

Any recipient of a report on potential compliance violations shall inform the Country Compliance Officer about the complaint.

4.3. *Compliance Reporting Line "SpeakUp"*

The Compliance Reporting Line SpeakUp can be used by both, employees of HeidelbergCement Group companies and third parties. It provides two ways of access:

Internet:
Using a country individual link http://www.speakupfeedback.eu/web/heidelbergcement/XX with for XX using the double-digit ISO country code (e.g. "de" for Germany or "us" for the USA). There the HC company code 18075 must be entered. The reporting party is offered to choose a country specific language of choice (e.g. English and French for Canada or Mandarin, Cantonese and English for China). Further guidance is provided in the selected language. The reporting party is offered a text field to share his/her concerns in any language.

Telephone:
Access by telephone in most countries is toll-free[2]. After dialling, instructions are provided in the languages of the country the reporting party is calling from. The phone intake system works like a voice mailbox. This means there is no operator and the reporting party leaves a message in the language of choice.

Reporting instructions:
In order to ensure efficient and timely investigations of the reported incident the following details are necessary to be included in the report in addition to the mandatory details:

- name and address of the site/plant where the incident has taken place; this is very important given the big number of locations HC operates at
- precise date on which the incident occurred
- full names of suspected individuals and witnesses

[2] A list of dialling-in numbers to the SpeakUp reporting system for all countries is available on the intranet (Group > Group Functions > Compliance > Reporting System SpeakUp) or at Group Compliance (see section 10 of this document) or with the local/Country Compliance Officer/Legal Counsel.

The description of the incident should be as precise and straightforward as possible. The report can be re-accessed at any time later on with an individual access number. This access number is provided by the system. The reporting party needs to take notice of it and memorise it. The status of the incident report and the messages posted on the system message board should be checked regularly in case there are any further details needed for the investigation of the incident.

Issues can be raised via SpeakUp in the following ways:

- **openly** by providing one's name and contact details when reporting an incident,

- **under complete anonymity** (no personal details are provided). However, this way of reporting bears the risk that full investigation and clarification of facts might not be possible due to lack of information and opportunity to receive further necessary details from the reporting party.

Although personalised reporting is preferred for accelerating and facilitating the investigation process, **full confidentiality is still warranted** to reporting employees and anonymous reporting remains an option in case of sensitivity.

4.4. *Alternative telephone reporting options*

In few countries the telephone access to SpeakUp does not function. For these countries solutions should be investigated such as indirect access to SpeakUp via a local telecommunication provider or an alternative phone line which isn't SpeakUp.

In order to ensure a common minimum standard of alternative phone reporting options the following requirements have to be met:

- The separate telephone line can be organised either internally (e.g. communication of Compliance Officer's telephone number and invitation by appropriate communication to all employees to report any compliance incidents by calling this number, warranting a proper and confidential investigation and keeping the name of the reporter anonymous, should he/she so wish) or externally (e.g. by an external lawyer).
- The person who takes the calls should be independent. In the case of an internal solution, this person should with regard to this task report directly to the Country General Manager or to a manager of the second level or higher. He/she should in addition have everybody's complete confidence in this respect.
- The line must be well communicated. Every employee should know that it exists, how it works, how to access it in a way that ensures confidentiality and anonymity if desired (e.g. by using the draft of the poster which Group Compliance provided when setting up the SpeakUp system as a sample and by printing posters which will be posted at each site).
- Upcoming reports as well as notices of results or interim results following the investigation must be properly documented.
- The reports must be investigated quickly, competently and confidentially.

Please do not hesitate to contact Group Compliance in case of concerns that these requirements are not completely fulfilled.

5. Investigation process

Once a compliance incident has been raised, investigations will be started immediately. The first point of contact will file the issue and inform the following persons/functions:

Category	Persons to be informed
Serious cases as e.g.: ▪ Fraud / Embezzlement ≥ 100,000 EUR (likely damage) per incident ▪ Corruption (active/passive bribery, governmental officials and/or HC management involved) ▪ Child abuse, forced labour	▪ CEO, CFO or relevant Area Vorstand ▪ Group Compliance ▪ Country General Manager ▪ Country Compliance Officer
Other incidents (e.g. fraud/embezzlement < 100,000 EUR likely damage per incident)	▪ Country Compliance Officer ▪ Supervisor of suspected person & head of unit/department ▪ If any other unit/department is affected, head of other unit/department

The appropriate General Manager or Country Compliance Officer, depending on the nature and financial impact of the incident as outlined above, decides who is responsible for investigating the case, considering one or more of the following persons, depending on the nature of the incident:

- Head of the department or business in which the incident has taken place
- Head of the department relevant for the nature of the incident (e.g. HR, H&S, Environment, Legal, IT)
- Head of respective organisational unit (e.g. Country General Manager)
- Internal Audit (Country or Group level)
- Compliance officer responsible for respective organisational unit or Head of Group Compliance
- External parties such as audit firms, police, public prosecution department, etc.

The decision on launching or not launching the investigation must be formally documented. In case the Country Compliance Officer is not involved in the investigation, he/she shall be informed about the investigation throughout the entire process in order to ensure complete reporting to Group Compliance in the context of the quarterly Compliance Incident Report according to the provisions of the Group Compliance Policy.

The timing target for finalisation of investigations and decision on any sanctions or remedial measures to be taken is not later than **60 days after submission of the incident report**.

The investigation process shall be documented in detail including all investigatory steps (e.g. who was interviewed, the documentation that was reviewed, etc.) and any remedial measures to be taken. The key findings and actions shall be summarised in a final report. The applicable regulations on data protection and privacy must, however, be observed at all times.

In order to ensure transparency and traceability of the investigation process, all documentation (both electronic and hardcopy) which is relevant to the investigation and ultimate outcome and resolution of the incident shall be retained in accordance with local legal requirements so that it can be produced in a timely manner if necessary.

Communication with the reporting party is an important element in the whole investigation process. In any case, the reporting party will be informed once the investigations are finalised (provided that the reporting channel used allows this feedback).

The investigation process is described in detail in the SpeakUp *Investigation Guide* which is available to all persons assigned as investigators to any compliance incidents.

6. Securing data if severe compliance violations are suspected

If severe compliance violations are suspected and securing of electronic data is deemed prerequisite for investigation, the process described below, if necessary adapted to local law (e.g. with respect to data protection/privacy), is to be followed at the earliest possible stage of an investigation in order to ensure that electronic data is properly secured and its integrity protected. Make sure to involve your data protection officer or coordinator before taking actions with personal data.

1. The management responsible for investigating the case will provide the appropriate local senior IT manager with the identity of the suspected individual and request that the individual's hard drive/PC/mobile device/any other electronic data or archival system be secured until advised otherwise. If appropriate, the individual's network access will be restricted or denied. Once the hard drive/PC/mobile device has been obtained from the individual, a "chain of custody" record will be kept to accurately document who was in possession of the electronic device(s) at any time during the investigation process. The investigators will ensure that searches of the hard drive/PC/mobile device will preferably be executed on a forensic image copy, are made only by qualified experts and that all data are analysed in a way which is accepted by the courts to serve as evidence. If necessary, external consultants will be retained to carry out these searches in the manner described. The hard drive/ PC/mobile device itself can only be analysed provided that investigation will not change the metadata stored (e.g. time stamps etc.).
2. If appropriate, the IT manager will disable the individual's ability to log on to the network and secure his/her hard drive/PC/mobile device.
3. The IT manager will ensure that an up-to-date back-up of the suspect's network data-store is performed and protected.
4. At the end of the investigative process the management responsible for investigating the case will decide whether access will be returned to the user, permanently disabled and or the suspect's network access will ultimately be removed.

In some instances there may be a suspicion surrounding an employee, but insufficient evidence to take the steps described. If this is the case it shall be ensured that a back-up according to step 3 will be taken to ensure that data cannot be deleted while further investigations occur.

7. Remedial actions

In case the investigation of an incident report produces evidence of non-compliant behaviour, various types of remedial actions have to be taken into consideration for which different functions are responsible:

Type of action	Responsible functions
Disciplinary measures	▪ Responsible: Line management according to grandfather principle[3] ▪ Involvement: HR, Country Compliance Officer
Civil claims	▪ Responsible: Line management according to grandfather principle[4] ▪ Involvement: Legal, Country Compliance Officer
Criminal prosecution	▪ Responsible: Country General Manager, Country Compliance Officer ▪ Involvement: Legal, Country Compliance Officer (if applicable)
Detected shortcomings	▪ Responsible: Appropriate department ▪ Involvement: Internal Audit (if necessary), Country Compliance Officer

8. Investigation principles

- **No retaliation:** All submitted incident reports, irrespective of the reporting channel, are to be handled in a way which avoids any retaliation towards the reporting employee.
- **Confidentiality:** All persons to whom incidents are reported are obliged to handle the cases confidentially.
- **Anonymity:** In case an incident was reported anonymously the investigator may offer through the available communication channels a personal talk or telephone call, however, if the reporting party prefers not to disclose his/her own identity this wish has to be respected.
- **Protection of the investigated persons' rights:** The investigated persons' rights of defence and protection of personal data shall be ensured.

9. Misuse of compliance incident reporting

Raising untrue allegations in bad faith is a misuse of the compliance incident reporting system and may in itself be regarded as a compliance incident resulting in sanctions for the reporting party.

In this respect it should be remembered that certain reports or complaints may be groundless and/or abusive and be intended to create problems for peers or superiors. Despite verifying such claims, it may sometimes be appropriate to avoid a costly and time-consuming, disproportionate investigation in such circumstances.

[3] ***„Grandfather prinicple"***: involving both, the employee's direct supervisor and the supervisor's supervisor.

10. Contact persons

For more information please contact:

Roland Sterr
Director Group Legal & Compliance
Phone: +49 6221 481-13663
Fax: +49 6221 481 13705
Email: roland.sterr@heidelbergcement.com

or your local/Country Compliance Officer/Legal Counsel