



# Group Compliance Incident Reporting & Case Management Policy

Scope: Heidelberg Materials AG and all companies directly or indirectly controlled by it  
Owner: Group Legal & Compliance  
Approver: Dr. Dominik von Achten, CEO

# **Table of contents**

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>Why report an incident?</b>	<b>3</b>
<b>3</b>	<b>Who can report and which types of incidents should be reported?</b>	<b>4</b>
<b>4</b>	<b>How to report an incident</b>	<b>6</b>
4.1	General reporting instructions	6
4.2	Compliance reporting line “SpeakUp”	7
4.3	Alternative telephone reporting options	7
4.4	Reporting in physical meeting	8
4.5	External reporting channels	8
<b>5</b>	<b>General principles when processing reports</b>	<b>8</b>
<b>6</b>	<b>Confidentiality</b>	<b>9</b>
<b>7</b>	<b>Measures following reports</b>	<b>9</b>
7.1	Process steps	9
7.2	Documentation and reporting	12
<b>8</b>	<b>Non-retaliation of reporting persons</b>	<b>12</b>
<b>9</b>	<b>Misuse of compliance incident reporting</b>	<b>12</b>
<b>10</b>	<b>Data protection</b>	<b>13</b>
<b>11</b>	<b>Contact and further information</b>	<b>13</b>

## **1 Introduction**

Heidelberg Materials<sup>1</sup> takes seriously any suspicion or concrete indication of a human rights or environment-related violation in its own business area or along the supply chain. In its Code of Business Conduct and in its Policy Statement on Human Rights, Heidelberg Materials requires all employees to observe high standards of business ethics in their duties and responsibilities. Along the supply chain, Heidelberg Materials suppliers must meet human rights-related and environmental expectations, which are set out in the Heidelberg Materials Supplier Code of Conduct.

This Group Compliance Incident Reporting & Case Management Policy (“Policy”) applies to all submissions made by employees, directors, and officers of Heidelberg Materials or any (external) third party, e.g., direct and indirect suppliers and their employees, residents around local sites of Heidelberg Materials and other parties directly or indirectly involved in the supply chain of Heidelberg Materials as well as customers.

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

- the submission of compliance-related concerns by employees, directors and officers of Heidelberg Materials as well as external third parties, on a confidential and, if preferred, anonymous basis;
- the processing and treatment of submitted complaints/incident reports;
- the protection of persons reporting concerns against retaliation.

This Policy was first issued in February 2012; this version replaces the previous one and takes immediate effect; it applies to all companies of Heidelberg Materials and is addressed to all its employees as well as third parties as outlined above.

## **2 Why report an incident?**

Heidelberg Materials recognizes the immense value of reporting incidents, violations, and suspicions of non-compliant behaviour in its own business area or along the supply chain, as it serves as a catalyst for improvement and the elimination of any misconduct. Heidelberg Materials highly appreciates the proactive efforts of its employees and any third party in reporting such incidents, as it reflects their genuine interest in driving positive change and continuous improvement within the company. By fostering a culture of reporting without the fear of retaliation, Heidelberg Materials aims to create an environment that encourages transparency and accountability, maintaining the highest standards of integrity and ensuring the long-term success of the company.

Timely reporting is of major importance to ensure swift resolution of issues and minimize any potential harm to both those affected and Heidelberg Materials. It is in the interest of every employee and stakeholder to retain a positive public perception of Heidelberg Materials. Hence, as a major pillar of the compliance program, the systematic incident reporting and case management involves promptly notifying the relevant individuals within the organization to facilitate prompt action and resolution. To fully leverage the benefits of implementing group-wide measures to prevent non-compliant conduct, it is essential that every incident is diligently recorded and analysed. This comprehensive approach allows us to identify patterns, address root causes, and continually improve our compliance efforts.

---

<sup>1</sup> Heidelberg Materials AG and all companies controlled directly or indirectly by it; for joint entities the definition and the rules of the Group Compliance Policy apply as well for this Policy.

### **3 Who can report and which types of incidents should be reported?**

Heidelberg Materials encourages its employees and third parties, such as suppliers, contractors, customers, NGOs, communities, and other stakeholders, to disclose **every and any kind** of risks of infringement, infringement of applicable laws, human rights or environment-related obligations, and policies or reasonable suspicion of such.

The scope of application includes in particular risks of violations and violations of the human rights-related or environment-related prohibitions of the German Supply Chain Act ("LkSG")<sup>2</sup>. Of course, this also includes topics for which Heidelberg Materials is obliged by law to provide a reporting channel and other compliance concerns (as a whole: the "scope of application"), which we do not refer to in our list of important incident types here:

- **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 regarding financial records; or deviation from full and fair reporting of the company's financial condition).
- **Adequate living wage** (withholding an adequate living wage which amounts to at least the minimum wage as laid down by the applicable law and apart from that, is determined in accordance with the regulations of the place of employment).
- **Alcohol and drugs** (actual or suspected consumption of drugs and/or alcohol which affects or has the potential to affect anyone'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).
- **Chemicals / Waste** (prohibitions according to the Minamata Convention on Mercury of the manufacture of mercury-added products or the use of mercury and mercury compounds in manufacturing processes or the treatment of mercury waste; prohibitions of the production and use of chemicals or the handling, collection, storage and disposal of waste in a manner that is not environmentally sound according to the Stockholm Convention on Persistent Organic Pollutants; the import or export of hazardous wastes and other wastes as defined by the Basel Convention on the Control of Transboundary Movements of Hazardous Waste and their Disposal).
- **Child or forced labour / slavery / child abuse** (abuse of children for child labour or of adults for forced labour/modern and all other forms of 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 the health, safety or morals of a child, in particular slavery, child prostitution, illicit activities).
- **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 perform the assigned job duties impartially).
- **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).

---

<sup>2</sup> Secs. 2 para. 2, 3, 4 LkSG.

- **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, accessed, destroyed, 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, voice recording).
- **Discrimination** (the discrimination or unlawful unequal treatment in employment of individuals based on an individual's race, colour, ancestry, ethnicity, gender (sex), age, religion or belief, national origin, social origin, level of education, political affiliation or opinion, physical appearance, health status, 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 (risk for) 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; in particular any harmful soil change, water pollution, air pollution, harmful noise emission or excessive water consumption that significantly impairs the natural bases for the preservation and production of food, denies a person access to safe and clean drinking water, makes it difficult for a person to access sanitary facilities or destroys them or harms the health of a person).
- **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).
- **Freedom of Association and the Right to Collective Bargaining** (right of employees to form, join and organize workers' organizations including unions or comparable organizations of their own choice without unjustified discrimination and retaliation; right to strike in accordance with applicable national law and the right to bargain collectively on their behalf with the company).
- **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 or work-related condition that potentially compromises the health, safety, and well-being of employees, customers, vendors, or visitors. Such conditions may include: insufficient safety standards in the provision and maintenance of the workplace, workstation and work equipment, in particular poor lighting or signage; unstable stacking or storage of materials, products, or equipment; exposure to hazardous materials or contaminants, resp. absence of appropriate protective measures to avoid exposure to chemical, physical or biological substances; exposure to excessive noise; lack of protection against weather elements; walkways, floors, or stairways in disrepair; or unnecessary exposure to dangerous machinery; lack of measures to prevent excessive physical and mental fatigue, in particular through inappropriate work organisation in terms of working hours and rest breaks; inadequate training and instruction of employees. Such workplace conditions may also constitute a breach of relevant legislation).
- **Land Grabbing** (unlawful eviction and the prohibition of unlawful taking of land, forests and waters in the acquisition, development or other use of land, forests and waters, the use of which secures the livelihood of a person).

- **Money laundering** (the process through which proceeds of crime and their true origin and ownership are changed so that the proceeds appear legitimate).
- **Public procurement** (rules and regulations that public bodies must observe when purchasing goods and services from private companies).
- **Product safety and compliance** (capacity of a product to be considered safe for its intended use and compliance with all applicable regulations).
- **Security Forces** (hiring or use of private or public security forces for the protection of the enterprise's project if, due to a lack of instruction or control on the part of the enterprise, the use of security forces is in violation of the prohibition of torture and cruel, inhumane or degrading treatment or damages life or limb or impairs the right to organise and the freedom of association).
- **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 salesperson 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 ask that the reporting person rather uses the category instead of unethical or illegal conduct. However, the naming of a specific category is not a prerequisite for submitting a report).
- **Other compliance-related issues**, which are not covered by the above-listed categories, e.g. violations punishable under the law or subject to fines, violations of applicable EU laws as well as an act or omission in breach of a duty to act that goes beyond the above listed human rights-related and environment-related prohibitions, which is directly capable of impairing one of the protected legal positions of the German Supply Chain Act in a particularly serious manner, and the unlawfulness of which is obvious upon reasonable assessment of all the circumstances in question.

Any reasonable suspicions of such risks or 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 chapter 7.1).

## 4 How to report an incident

### 4.1 General reporting instructions

Complaints can be reported through different channels, such as emails, phone calls, or to the compliance team in person, and to our SpeakUp reporting platform. In case of complaints of Heidelberg Materials employees, they are encouraged to inform their direct supervisor, if they feel comfortable to do so. This is usually the fastest way to resolve issues when the reporting party does not insist on using a formal reporting channel.

In order to facilitate an efficient and effective investigation, the reporting person should disclose as much and as 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? Precise date on which the incident occurred (if possible)
- **Where** did it happen? - name and address of the site/plant where the incident has taken place – this is very important given the big number of locations Heidelberg Materials operates at and of suppliers it works with
- **Why** did it happen? – reasons/factors that led to the incident (background information)
- **How** did it happen? - course of events

## 4.2 Compliance reporting line “SpeakUp”

The Compliance Reporting Line SpeakUp can be used by both employees of Heidelberg Materials and third parties. It provides two ways of access:

### ***Internet:***

SpeakUp is globally accessible using the link <https://heidelbergmaterials.speakup.report/speakup>. The reporting person is offered 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 person is offered a text field to share his/her concerns in any language.

### ***Telephone:***

Access by telephone in most countries is toll-free<sup>3</sup>. After dialling, instructions are provided in the languages of the country the reporting person is calling from. It is necessary to know the company access code which is 107810 for Heidelberg Materials. The phone intake system works like a voice mailbox. This means there is no operator, and the reporting person leaves a message in the language of choice. The message recording is transcribed into writing by the system provider. After the Heidelberg Materials case manager confirmed receipt of the case (according to chapter 7.1) the recording is deleted by the system provider, therefore, Heidelberg Materials competent personnel cannot access the recording but solely the transcript. The reporting person has the right to receive a copy of this transcript to check for errors. The reporting person should indicate this wish during the call and inform where the transcript should be sent.

### ***Report access instructions:***

The report can be re-accessed at any time later on with an individual access number and password. The access number is provided by the SpeakUp system while the password is decided on by the reporting person. The reporting person needs to take notice of the access information. 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 follow-up of the incident.

### **Reports can be submitted via SpeakUp in the following ways:**

- **openly** by providing one's name and contact details when submitting a report,
- **under complete anonymity** (no personal details are provided). SpeakUp offers an anonymous way of communication. The SpeakUp system is then the only available communication channel with the reporting person. This way of reporting makes it necessary for the reporting person to check for questions of the case investigator because the reporting person can't be contacted for further necessary information in any other way.

## 4.3 Alternative telephone reporting options

In few countries, telephone access to SpeakUp is not set up. 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 alternative telephone line can be organised either internally (e.g. communication of Country Compliance Officer's telephone number and invitation by appropriate communication to all em-

---

<sup>3</sup> A list of dialling-in numbers to the SpeakUp reporting system for all countries is available on the internet under this link <https://www.heidelbergmaterials.com/en/governance-and-compliance#speakup> or contact Group Compliance.

ployees and third parties as outlined above to report any compliance incidents by calling this number, warranting a proper and confidential investigation and keeping the name of the reporting person anonymous, if requested) or externally (e.g. by an external lawyer, ombudsperson).

- The person who takes the calls must meet the requirements set out in section 7 (in particular impartiality, not bound by instructions). 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 and the necessary resources to conduct the respective task.
- The alternative telephone line must be well communicated and easily accessible, not only to employees but third parties. Every employee and third party as outlined above 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 Heidelberg Materials Group Compliance provided when setting up the SpeakUp system as a sample and by printing posters which will be posted at each site).
- Incoming reports as well as notices of results or interim results following taken measures must be properly documented, as outlined below in chapter 7.2.
- The reports must be followed-up quickly, competently, and confidentially as outlined below in chapter 7.1.

Please do not hesitate to contact Heidelberg Materials Group Compliance (<https://www.heidelberg-materials.com/en/governance-and-compliance>) in case of concerns that these requirements are not completely fulfilled.

#### **4.4 Reporting in physical meeting**

A reporting person has the right to ask for a physical meeting with the competent personnel to report a compliance incident. The competent personnel ensures that such meeting takes place within a reasonable time frame and that it is appropriately documented in writing. The meeting may be recorded only with consent of the reporting person. If a recording is made, then a written transcript is prepared, and the reporting person has the right to ask to confirm the transcript by signing it off. The recording will be deleted once a written transcript has been prepared. The documentation related to the respective reports will be deleted in accordance with the applicable laws.

#### **4.5 External reporting channels**

The EU Whistleblowing Directive makes it mandatory for all EU member states to implement external reporting channels for, among others, employees, self-employed persons, shareholders and management personnel, any person working under the supervision and direction of contractors, subcontractors, and suppliers. These channels may be different in each EU member state. The EU Country Compliance Officers make sure that the respective external reporting channel of their country is appropriately communicated in the respective country.

### **5 General principles when processing reports**

These general principles, as further specified in this policy, should underlie the processing of reports:

- **Confidentiality:** All persons to whom incidents are reported are obliged to handle the cases confidentially.
- **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 person.

- **Anonymity:** In case an incident was reported anonymously, the investigator may offer through a message in SpeakUp to initiate a conversation, in particular in the form of a personal talk or telephone call, however, if the reporting party prefers not to disclose its 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 at all times.

## 6 Confidentiality

The confidentiality of the identity of the reporting person is one of Heidelberg Materials' highest priorities. The incident reporting system maintains the confidentiality of identity of the reporting person, persons that are subject of the report as well as any third party mentioned in the report. Heidelberg Materials only shares information on a "need to know"-basis for the case investigation and follow up measures. Information about the identity of a reporting person and other information from which a reporting person's identity can be directly or indirectly derived may not be disclosed, without the explicit consent of the reporting person, to employees other than authorized employees who are competent to receive or follow up on reports. Heidelberg Materials obliges the competent personnel and all persons entrusted with the procedure to secrecy and also trains them in it. Heidelberg Materials ensures confidentiality even after the procedure has been completed.

In addition, the incident reporting system ensures confidentiality regarding the person concerned and any third party mentioned in the report. It also prevents unauthorized access. Nevertheless, competent personnel might share such information with public authorities, if necessary to prevent a breach of law or where necessary to safeguard the rights of defense of the person concerned.

In individual cases, non-anonymous reporting persons may be called as a witness in court.

## 7 Measures following reports

### 7.1 Process steps

Once a compliance incident has been raised through one of the reporting channels, Heidelberg Materials will take the following steps:

- **Confirmation and documentation of receipt:**

The first point of contact will file the compliance incident with the Group Compliance Officer or respective Country Compliance Officer, who will inform the persons as outlined in the table below depending on the nature and financial impact of the incident.

Category	Persons to be informed
Serious cases as e.g.: <ul style="list-style-type: none"> <li>▪ Fraud / Embezzlement etc. ≥ 100,000 EUR (likely damage) per incident</li> <li>▪ Corruption (active/passive bribery, governmental officials and/or Heidelberg Materials Group management involved)</li> <li>▪ Child abuse, forced labour or other incidents of special interest for Heidelberg Materials Group</li> </ul>	<ul style="list-style-type: none"> <li>▪ CEO, CFO or relevant Area Board Member</li> <li>▪ Group Compliance</li> <li>▪ Country Compliance Officer</li> </ul>
Human rights cases, including child and forced labour and cases of environmental	<ul style="list-style-type: none"> <li>▪ Group Compliance</li> <li>▪ Country Compliance Officer</li> </ul>

risk with impact on human rights (incidents which fall under the German Supply Chain Due Diligence Act)	<ul style="list-style-type: none"> <li>▪ Group Human Rights Officer</li> <li>▪ Country Human Rights Coordinator</li> </ul>
Other incidents (e.g. fraud/embezzlement < 100,000 EUR likely damage per incident)	<ul style="list-style-type: none"> <li>▪ Country Compliance Officer</li> <li>▪ Supervisor of suspected person &amp; head of unit/department</li> <li>▪ If any other unit/department is affected, head of other unit/department</li> </ul>

The Group Compliance Officer or the respective Country Compliance Officer documents the receipt of reports. Additionally, seven days after receipt of the compliance incident by the Group Compliance Officer or the respective Country Compliance Officer, the compliance personnel sends a message via the SpeakUp-tool (or via another appropriate communication channel like email etc. if the message was received outside the SpeakUp system) to the reporting person with the following content as far as possible to provide at this early stage of the process: (i) acknowledgement of receipt of the report; (ii) information on next steps and their timing (expected timing of each step), (iii) information on the reporting person's rights regarding protection from adverse treatment and punishment.

Reports on serious violations of human rights and environmental obligations are prioritised here and in the further steps below.

- **Check of scope of application:**

The Group Compliance Officer or the respective Country Compliance Officer examines whether the reported incident falls within the types of incidents outlined under 3. If this is not the case, the Compliance Officer or their compliance personnel sends the reporting person a notification with a brief explanation. The case is then closed.

If the reported incident falls within the scope of application, the responsibility for the case is determined. For this purpose, the Group Compliance Officer or the respective Country Compliance Officer decides who is responsible for the further case processing and assigns the case to a specific case manager among the compliance personnel.

- **Clarification of responsibility for handling of reports**

The Group Compliance Officer or the respective Country Compliance Officer is responsible for the process of handling of reports and the monitoring of the case management system. All reports are handled by trained competent personnel (compliance personnel and all persons assigned as investigators to any compliance incident) who are qualified to process reports in line with the applicable law and in accordance with Heidelberg Materials Governance Documents (i.e., company values, policies, procedures, and guidelines).

The competent personnel are responsible for handling the respective hints or complaints in an impartial way. They are independent and not bound by instructions of their superiors when managing cases and handling incidence reports. Moreover, they are bound to secrecy (see chapter 6). The case manager decides how a case is investigated and appoints additional investigators if needed. Investigators can then be people from the compliance personnel, competent departments, and/or external qualified investigators.

The investigation process is described in detail in the SpeakUp *Investigation Guide* which is available to all competent personnel.

The competent personnel, in particular the case manager and the assigned investigators have sufficient time resources to understand and assess the situation and the procedure from the perspective of the reporting person and to be able to deal with it in the further procedure.

Depending on the nature of the incident, the competent personnel can be:

- **Group or respective Country Human Rights Coordinator**
- **Head of the department or business unit in which the incident has taken place**

- **Head of the department relevant for the nature of the incident (e.g., Health and Safety, Environment, Legal, IT)**
- **Head of respective organisational unit (e.g., Company Manager, Country General Manager)**
- **Group Internal Audit or Country Auditor**
- **Compliance Officer responsible for respective organisational unit or Head of Group Compliance**
- **External parties such as audit firms, police, public prosecution department, etc.**

The result of the assessment of the scope of application, the decision on responsibility in the individual case and possible notifications to the reporting person are documented. This procedural step is usually finalised within the first seven days after receipt of the report.

If required, the case can also be sent to public authorities for independent investigations.

▪ **Establishing the facts of the case:**

The competent personnel investigates and checks the facts of the reported incident by conducting interviews, checking documents or communicating with the reporting person. In this context of joint assessment of the facts, the parties involved also talk about the expectations of the reporting person with regard to possible preventive or remedial measures.

Any proceedings related to a report may be closed due to lack of proof or for other reasons. This is particularly the case if the report is unsubstantiated on the factual level to such an extent that it does not allow for any further specific investigation, even in cooperation with the reporting person. The decision on closing the proceedings must be formally documented.

This procedural step is targeted to be completed within 60 days after receipt of the report. The time frame can be longer for good reasons, e.g., major scope investigations involving internal audit or external investigators, or necessity of follow-up work due to newly provided information during an investigation process.

▪ **Remedial action:**

If the assessment of the facts leads to the identification of violations that have already occurred or are imminent, the competent personnel develop remedial measures. If violations of the protective goods of the LkSG are identified, such remedial measures will be developed in exchange with the reporting person. These remedial measures must prevent, stop, or at least minimise the (imminent) violation. Such remedial measures may especially include: Disciplinary measures, civil claims, criminal prosecution and elimination of detected shortcomings. In addition, preventive measures must be taken to prevent or minimise the risk of further violations.

No later than **90 days after submission of the incident report**, the reporting person shall receive feedback on any remedial actions planned or already taken and the reasons for such action. This must be done in a form that does not impede internal investigations and does not affect the rights of the persons who are the subject of the investigation or named in the report.

The remedial measures are then implemented by the competent personnel.

▪ **Review:**

The competent personnel, in particular the case manager, carry out the following reviews:

- Case-related review: the implementation and outcome of the remedial action(s) will be followed up. The assessment of the outcome will be evaluated. The timeline depends on the due dates of the agreed on measures.
- General review: the effectiveness of the LkSG-complaint procedure and of the remedial action as a whole is reviewed annually and on an ad hoc basis and, if necessary, improved. This general review of the procedure is carried out on the basis of suitable key performance indicators (KPIs), such as the number of complaints (also with a view to their use by different target groups), the proportion of complaints resolved or the average duration of processing.

## **7.2 Documentation and reporting**

The competent personnel, in particular the case manager, shall document every procedural step that they undertake 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.

In case the Group Compliance Officer or the respective Country Compliance Officer is not involved in the investigation, they 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 Group Compliance Officer or the respective Country Compliance Officer is also responsible to monitor compliance with the procedural rules laid down here, in particular, when not directly involved in the investigation.

## **8 Non-retaliation of reporting persons**

Heidelberg Materials does not tolerate any discrimination, retaliation, or sanctions against reporting persons (employees and third parties). Heidelberg Materials assures each employee that reporting in accordance with these principles will not affect their employment, opportunities, career, or duties. Heidelberg Materials takes the following measures to protect reporting persons from discrimination, retaliation, or sanctions in accordance with the legal requirements:

Heidelberg Materials protects the confidentiality of the reporting person's identity (see chapter 6) and sets high standards for data protection (see chapter 10). This, combined with the possibility of anonymous reporting (see chapter 4), helps to minimise the risk of retaliation. Further, Heidelberg Materials remains in contact with the reporting person even after the conclusion of the procedure to ensure that they are not endangered by retaliation in the aftermath.

If Heidelberg Materials becomes aware that employees or suppliers are using retaliation against reporting persons, Heidelberg Materials will work with the source of the retaliation to stop it.

If anyone becomes aware of any retaliation in connection with a report of an employee or third party, they should immediately contact the Group Compliance Officer or the respective Country Compliance Officer. Those reports will be investigated confidentially. Reporting persons are entitled to compensation if retaliatory measures are taken against them or if an attempt is made to prevent them from reporting.

The protection against retaliation also covers mediators, third parties connected to the reporting person who are at risk of retaliation in a work-related context and companies and authorities that the reporting person owns or works for or is otherwise associated with in a work-related context.

## **9 Misuse of compliance incident reporting**

Misuse of the reporting systems does not have to be dealt with according to the above procedure.

This applies in particular to deliberately raising false allegations as well as sending a large number of identical reports to the competent personnel. In such a case, Heidelberg Materials would not be obliged to acknowledge receipt.

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. If a report turns out to be clearly unfounded, the contents of the report and any personal data associated with the report will be deleted from the system immediately and the reporting person will be informed.

## **10 Data protection**

Competent personnel ensures that applicable data protection law is adhered to while investigating a case and when documenting it, including the respective data retention rules.

## **11 Contact and further information**

For more information please contact:

Roland Sterr

Director Group Legal & Compliance

Phone: +49 6221 481-13663

Email: [roland.sterr@heidelbergmaterials.com](mailto:roland.sterr@heidelbergmaterials.com)

or for employees: your local Country Compliance Officer/Legal Counsel.