



Whistleblowing Policy

Scope: Heidelberg Materials Northern Europe
Owner: NEUR Legal, Compliance & Corporate Security
Issued: September 2024
Version: 2.0

Table of contents

1	Introduction	3
2	Internal channels for reporting misconduct	3
3	Who can report?	3
4	What can I report?	4
4.1	Reporting via Whistleblowing Channels	4
4.2	Examples of things that typically may be reported via the Whistleblowing Channel	4
4.3	Examples of things that typically may not be reported via the Whistleblowing Channel	5
5	How do I submit a report?	5
5.1	SpeakUp	5
5.2	Email	6
5.3	Verbally	6
6	What type of information should you include in a report?	6
7	What will happen when I have submitted a report?	6
7.1	Whistleblowing committee will receive the report	6
7.2	Initial confirmation	7
7.3	Investigation	7
7.4	Feedback	7
8	Which rights do I have as a reporting individual?	7
8.1	Reporting anonymously	7
8.2	Confidentiality	8
8.3	Attempt to prevent you from reporting is not allowed	8
8.4	Protection from retaliation	8
8.5	Discharge from liability	8
9	External reporting channels	8
10	Processing of Personal Data	9
10.1	Contact details and personal data controller	9
10.2	Categories of personal data and data subjects	9
10.3	Purposes of processing and legal basis	9
10.4	Retention period	10
10.5	Third party transfers	10
10.6	Data subjects' rights	10
11	Version history	11
	SCHEDULE 1 AUTHORIZED PERSONS/WHISTLEBLOWING COMMITTEES	12

1 Introduction

Heidelberg Materials Northern Europe (“**HM NEUR**” or “**we**”/“**us**”) has the mission to conduct our business with an open business climate and a high level of business ethics. We take seriously any suspicion or concrete indication of a compliance, human rights and/or environment-related violation in our own business area or along our supply chain. Our Code of Business Conduct and our Policy Statement on Human Rights, requires all employees to observe high standards of business ethics in their duties and responsibilities.

This policy sets out how our local whistleblowing channels (the “**Whistleblowing Channels**”), established in accordance with national¹ implementing legislation of the EU Whistleblowing Directive or similar national legislative initiatives (the “**Whistleblowing Acts**”), are set up within HM NEUR.

2 Internal channels for reporting misconduct

In HM NEUR, we have three main ways of reporting misconduct:

1. Local informal reporting channels (for example, your immediate manager or local HR)
2. A global Group-wide reporting channel
3. The Whistleblowing Channels set up pursuant to the requirements of the Whistleblowing Acts for each HM NEUR company with more than 50 workers.

If the misconduct relates to things that may be reported via the Whistleblowing Channels (see Section 4), then the Whistleblowing Channels should be used.

If the misconduct is outside of the scope of what can be reported in the Whistleblowing Channels, you should turn to your immediate manager, another manager you trust or your local HR department. You can also use the global reporting channel set up by Heidelberg Materials Group. For information on what can be reported in that channel and how incoming reports will be handled, please see the Group Compliance Incident Reporting & Case Management Policy.

If you are unsure what channel to use, you can contact Victor Ask at victor.ask@heidelbergmaterials.com for guidance.

3 Who can report?

All who work with us can use the Whistleblowing Channels. This includes:

1. employees²,
2. job seekers
3. volunteers,
4. interns,
5. persons who otherwise perform work under the HM NEUR’s control and management,
6. self-employed persons seeking or performing work,
7. persons who are members of HM NEUR administrative, management or supervisory bodies, and

¹ Sweden, Norway, Denmark, Estonia, Latvia, Lithuania and Iceland.

² For Norway, this Policy only applies to employees, in line with Norwegian law.

8. shareholders who are active in HM NEUR.

Also included are anyone who previously belonged to one of the above categories and learnt of the misconduct in that role.

4 What can I report?

4.1 Reporting via Whistleblowing Channels

Reports in the Whistleblowing Channel may only refer to misconduct in a work-related context and must meet the following criteria depending on the country in which the Whistleblowing Channel is set up:

Country(ies)	Criteria for what can be reported in the Whistleblowing Channels
Sweden, Iceland, Estonia, Lithuania and Latvia	There must either be a public interest in the emergence of the misconduct or the misconduct must be in breach of Union law, i.e. EU acts or laws implementing such legislation.
Norway	Misconduct must refer to censurable conditions, irregularities or issues of concern, <i>i.e.</i> breaches of rules of law, written ethical guidelines of the Group (Company Code of Conduct) or ethical standards with widespread endorsement in the community. ³
Denmark	Misconduct must refer to violations of EU law or otherwise regard serious offences or other serious matters.

Note that you do not have to have proof of your suspicions in order to report, but all reports must be made in good faith and you must have reasonable grounds to assume that the information about the misconduct is true, and that the reported misconduct falls under the scope of application of the Whistleblowing Acts.

4.2 Examples of things that typically may be reported via the Whistleblowing Channel

- i. **Criminal activity:** Serious criminal activity (e.g. violence, threats of violence, theft, possession of stolen goods or otherwise illegally acquired property, vandalism, unlawful deprivation of freedom);
- ii. **Fraudulent activities:** Fraudulent activities such as wrongful accounting, breaches of internal control procedures, embezzlement of assets or fraud, tax crime, illegal or non-transparent use of public funds or property;
- iii. **Non-compliance with laws:** Violations of legislation that HM NEUR is required to comply with;
- iv. **Corruption:** Bribery and corruption such as giving or taking bribes, including interference or unlawful influence on investigations conducted by law enforcement authorities or in the enforcement of justice;

³ It should be noted that the threshold for what constitutes whistleblowing under Norwegian law (including case law), *i.e.* whether an employee's note of concern is considered whistleblowing, is relatively low compared to many other countries.

- v. **Money laundering:** Violations of money laundering and/or financing of terrorism legislation or financing of illegal activities;
- vi. **Competition Law:** Violations of competition law or public procurement legislation, for example, exchange of price sensitive information and illegal cooperation between competitors;
- vii. **Conflicts of interest:** Conflicts of interest, such as providing undue benefits to a family member in employment procedures or supplier contacts;
- viii. **Environmental issues / sustainability:** Serious threats to the environment and or the climate, for example, harmful soil change, water pollution, air pollution, harmful noise emission or excessive water consumption.
- ix. **Health and Safety:** Work-related health and safety issues, such as under-reporting of accidents, any workplace or work-related condition that potentially compromises the health, safety, and well-being of workers, customers, vendors, visitors or others;
- x. **Personal data and IT systems:** Serious violations of protective legislation regarding personal life and personal data, and network and information systems;
- xi. **Discrimination:** Any discrimination on the bases of 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, sexual orientation, or gender identify or expression.
- xii. **Harassment:** Any harassment, for example unwanted ongoing verbal or physical behaviour of an inappropriate nature.
- xiii. **Human Rights violations:** Human rights violations, such as the use of child labour, modern slavery, or not paying an adequate living wage;
- xiv. **Breaches of core HM Policies:** Serious breaches of HM NEUR's Code of Business Conduct, our Policy Statement on Human Rights or this Policy.

4.3 Examples of things that typically may not be reported via the Whistleblowing Channel

Complaints and matters such as poor management (leadership), alcohol or drug problems (unless they are creating an unsafe work environment), petty theft at work, and minor work environment issues shall typically not be reported via the Whistleblowing Channel. You are instead directed to report such issues to your immediate manger, local HR, another manger you trust or use the global Group-wide reporting channel (if the misconduct is included in the scope of that channel)⁴.

5 How do I submit a report?

5.1 SpeakUp

You submit your report in the Whistleblowing Channel by accessing our SpeakUp-system via the following link: [SpeakUp](#). To provide your report, please follow the steps below:

1. Select "New report".
2. Select your preferred language you will use in the report.

⁴ These examples may not be applicable for Norway. In case you require more detailed guidance, please feel free to contact NEUR Legal & Compliance at the contact details below.

3. Choose a password for your report.
4. From the roll down list, select your local Heidelberg Materials entity.
5. Enter your message and describe the misconduct. Attachments are available. Click “Send message”.

5.2 Email

You can also submit your report by sending an email to Peter Linderoth (peter.linderoth@heidelbergmaterials.com) or Victor Ask (victor.ask@heidelbergmaterials.com).

5.3 Verbally

You have the right to submit your report verbally, either by telephone or by requesting an in-person meeting. If you want to report verbally, you are welcome to contact us in writing via the above e-mail addresses. We will schedule such a meeting within a reasonable time and always, unless you are not available, no later than 2 weeks from the time the request is received.

If you choose to report verbally, we will document the report through a recording, provided you agree to this, or by establishing a protocol. You will be given the opportunity to check, correct and approve the protocol.

6 What type of information should you include in a report?

Examples of information that you should include in your report are;

- a) Date, time and place of the event;
- b) A description of what happened and possibly your part in the event, or other relevant information about the circumstances of the issue;
- c) Information about how the event was discovered;
- d) The relevant persons’ names, positions and the legal entity they pertain to;
- e) Witnesses, if any;
- f) Other information that sheds further light on the event and that helps in processing your report.

To make it easier for us to investigate your report, we encourage you to be as specific and exhaustive as possible when submitting your report.

We also encourage you to provide us with your name and contact details as anonymous reports are often more difficult to investigate.

7 What will happen when I have submitted a report?

7.1 Whistleblowing committee will receive the report

Once you have submitted a report, it will be received by a committee of specially designated authorized persons (“the **Whistleblowing Committee**”).

The persons who are part of the Whistleblowing Committee have been appointed by each HM NEUR entity with more than 50 workers as authorized persons to, on behalf of the employer, in an independent and unaffiliated manner, receive reports, have contact with reporting individuals, and follow up (investigate)

what is reported. Designated persons appointed by each employer in HM NEUR with more than 50 workers are listed in [Schedule 1](#).

7.2 Initial confirmation

Normally, you will receive a confirmation that the Whistleblowing Committee has received your report within **seven days** (two days for Lithuania) of you submitting your report.

The Whistleblowing Committee will initially assess whether your report covers such misconduct that can be reported via the Whistleblowing Channel and if the report meet formal requirements stipulated by the Whistleblowing Acts. If that assessment concludes that the report is not in scope of the Whistleblowing Channel, you will normally also be notified **within seven days** of you submitting your report.

7.3 Investigation

If your report includes such misconduct that can be reported via the Whistleblowing Channel, the Whistleblowing Committee will then review your report and decide on appropriate measures to investigate the suspected misconduct. The Whistleblowing Committee may contact you to ask follow-up questions.

The investigation may require the involvement of other internal functions or external expertise, such as IT expertise, legal advisers, auditing companies or forensic investigation companies.

If a member of the Whistleblowing Committee itself is affected by a report or otherwise has a conflict of interest, that person will not participate in the investigation or otherwise be allowed to take part in the matter.

7.4 Feedback

No later than **three months** (2 months for Latvia) after you received a confirmation of receipt of the report, the Whistleblowing Committee will, to a reasonable extent, provide you with feedback on investigative measures taken. You will also receive feedback when the investigation is complete.

After a preliminary investigation has taken place and all relevant evidence has been secured, the person concerned, i.e., the person(s) who is the subject of a report, will, at minimum, to the extent required by law, be informed about the persons responsible for investigating the report and the issues of the report.

8 Which rights do I have as a reporting individual?

8.1 Reporting anonymously

You have the opportunity to submit your report anonymously, for example in SpeakUp or from an e-mail address that does not obviously belong to you. If you choose to report anonymously, the Whistleblowing Committee will not try to find out who submitted the report. Although it is possible to remain anonymous, we encourage you to provide your name and contact details as anonymous reports are often harder to investigate.

8.2 Confidentiality

If you provide your name when submitting a report, your identity will be treated with strict confidentiality. The Whistleblowing Committee may not, unless in specific circumstances permitted by law, disclose information that may reveal your identity or the identity of any other person who appears in the report.

If information that can identify you is to nevertheless be disclosed (authorized disclosure under the Whistleblowing Acts or other laws or regulations), you will be informed of this, unless such notice is prohibited by law or regulation or risks impeding the investigation.

8.3 Attempt to prevent you from reporting is not allowed

If you report in good faith and have reasonable grounds to assume that the information about the misconduct is true, and that the reported misconduct falls under the scope the Whistleblowing Acts, it is strictly forbidden for HM NEUR, or anyone within our business, to prevent or attempt to prevent you from reporting (suspected) misconduct.

8.4 Protection from retaliation

If you report in good faith and have reasonable grounds to assume that the information about the misconduct is true, and that the reported misconduct falls under the scope the Whistleblowing Acts, you are also legally protected from retaliation by HM NEUR or HM NEUR employees. No HM NEUR employee or worker shall be penalized or subject to disciplinary action because they acted in accordance with this Policy. Nor may any retaliation be made against a person who assists you in your reporting (e.g. a safety representative), someone who is that related to you (e.g. a family member), or any legal entity that you own, work for or otherwise have a connection to.

If you believe that you have been the subject of retaliation for acting in accordance with this Policy, you should report this via the Whistleblowing Channel as soon as possible.

8.5 Discharge from liability

You, who in good faith reports misconduct in accordance with this Policy and who have reasonable grounds to believe that your report is necessary in order to rectify such misconduct, shall not be held liable by HM NEUR for having breached contractual non-disclosure obligations, regulations governing data collection or similar obligations. Exceptions from this discharge of liability may be set out in the relevant Whistleblowing Acts.

9 External reporting channels

You also have the possibility to report misconduct to any of the external reporting functions established by certain authorities in your jurisdiction or by EU institutions, bodies or firms. These authorities are tasked with receiving, following up and providing feedback on reports of misconduct within their specific areas of responsibility.

If you have are unsure to which authority you should submit your report, please contact Victor Ask at victor.ask@heidelbergmaterials.com for guidance.

10 Processing of Personal Data

10.1 Contact details and personal data controller

Each HM NEUR entity is the personal data controller for the personal data processed in its Whistleblowing Channel. You will find contact information to each HM NEUR entity below in [Schedule 1](#).

If you have questions regarding how we process personal data about you, you may contact us as set out in [Schedule 1](#). If you have any objections or complaints about the way we process your personal data, you have the right to file a complaint to the Data Protection Authority in your jurisdiction:

- [Sweden](#): Swedish Authority for Privacy Protection (sw. *Integritetsskyddsmyndigheten*)
- [Denmark](#): Danish Data Protection Agency (dk. *Datatilsynet*)
- [Estonia](#): Estonian Data Protection Inspectorate (ee. *Andmekaitse Inspektsioon*)
- [Latvia](#): Data State Inspectorate (lv. *Datu valsts inspekcija*)
- [Lithuania](#): State Data Protection Inspectorate (lt. *Valstybinė duomenų apsaugos inspekcija*)
- [Norway](#): Norwegian Data Protection Authority (nb. *Datatilsynet*)
- [Iceland](#): Icelandic Data Protection Authority (is. *Persónuvernd*)

10.2 Categories of personal data and data subjects

Whistleblowing reports typically contain personal data, which directly or indirectly pertain to a natural person. The information can be attributable to the person who submits a report, the subject of a report, and to other individuals mentioned in the report, such as witnesses (“**Relevant Person(s)**”).

Personal data that may be processed about Relevant Persons in connection with a report may include name, address, city, gender, nationality or other characteristics of the person relevant to the reported misconduct, roles or functions, contact information (including telephone number), details of the reported event, measures taken, and other types of personal data collected within the scope of the investigation, e.g. interviews but also via e.g. phone records, computer files, audio files, IP-addresses and other technical data, as well as e-mails.

Depending on the nature of the matter, we may also process sensitive personal data about Relevant Persons, such as data about race or ethnic origin, political opinions, religious or philosophical beliefs, union membership and data about health or sex life. When submitting a report, you should avoid disclosing sensitive personal data that is not relevant to the case.

A report can also mean that personal data about violations of law that include suspected or confirmed crimes may be processed.

Information that is not relevant to the processing of a report in an obvious way will be deleted as soon as possible.

10.3 Purposes of processing and legal basis

Personal data is processed primarily for the purpose of processing and investigating a follow-up case. Personal data processed for this purpose may also be processed for the purpose of fulfilling a disclosure that; (i) is necessary in order to take action in connection with what has emerged in a matter; (ii) is necessary for reports to be used as evidence in legal proceedings; and (iii) is in accordance with applicable laws and regulations.

The legal basis for the processing of personal data is our legal obligation to provide a Whistleblowing Channel under the Whistleblowing Acts.

As described above, we may, depending on the nature of the case, also process sensitive personal data. The legal basis for our processing of sensitive personal data is that the processing is necessary in the interests of an important public interest, on the basis of Union law or the national legislation of the Member States. In some cases, we may also process sensitive personal data when it is necessary for us to be able to fulfil our obligations and exercise our special rights within areas of labour law, social security and social protection.

We may also process personal data on violations of the law that include suspected or confirmed crimes. Such processing is necessary to fulfil our legal obligation to provide a whistleblowing channel in accordance with the Whistleblowing Acts.

We may in some cases also process personal data in order to take action in connection with a report. We then rely on our legitimate interest in processing personal data in order to be able to take action in connection with the report. To the extent that sensitive personal data or data on breaches of the law need to be processed, this is done on the grounds that it is necessary to establish, assert or defend a legal claim.

10.4 Retention period

The personal data will only be stored by us for as long as necessary to investigate a report and take relevant measures in relation to the result of such investigation. Personal data that occurs in a follow-up matter is never processed for longer than two years (5 years for Lithuania) after the matter is closed. Superfluous personal data and personal data that is not relevant to the reported event will be deleted or anonymized as soon as possible.

Personal data processed to establish, assert or defend a legal claim will be stored until the legal proceedings are completed and during the subsequent limitation period.

10.5 Third party transfers

Data that emerges from a report and in a follow-up matter will be treated with the greatest possible confidentiality, and will not be disclosed to more persons than is necessary with regard to the purposes of the processing.

In order to fulfil the purposes of the processing of personal data, the personal data may however be transferred to other Heidelberg Material companies and third parties, such as external legal advisers, accounting firms, forensic investigation companies or other service providers that are necessary to detect, investigate and rectify serious breaches. We may also share personal data with police authorities and/or other relevant authorities, regulators or courts to safeguard our interests or exercise our rights.

If third parties act as personal data processors for us for the personal data processing in question, we will enter into the necessary personal data agreements with such third parties.

Your personal data will not be transferred to countries outside the EU/EEA.

10.6 Data subjects' rights

If we receive a report which includes your personal data or if your personal data is collected within the scope of an investigation, we will provide you with information thereof.

You will be notified as soon as possible after an initial investigation has taken place and all relevant evidence is secured. In this connection, you will receive information about:

- The identity of the person(s) who is/ are responsible for the investigation of the report.
- A description of the contents of the report.

You may have a right of access to the report that was submitted about you. Please see below about your general GDPR rights. However, your right to access to the report may be limited in accordance with the Whistleblowing Acts.

You are further entitled to know what personal data we are processing about you, and you can request a copy of such data. Please note that to the extent that the disclosure of your personal data may compromise an investigation, we may not be able to meet your request. You are entitled to have incorrect personal data about you rectified, and in some cases you may request that we delete your personal data. You are also entitled to object to certain processing of your personal data, and request that the processing of your personal data should be restricted.

11 Version history

Changes of persons designated to be a part of the whistleblowing committee from time to time will not be reflected in the below table.

Date	Version	Author	Overview of changes
June 2023	1.0	NEUR Legal, Compliance & Corporate Security	Policy was created for Sweden
September 2024	2.0	NEUR Legal, Compliance & Corporate Security	Policy was modified to fit local legislation in other NEUR countries and adjusted based on lessons learned during the year.

SCHEDULE 1 - AUTHORIZED PERSONS/WHISTLEBLOWING COMMITTEES

The following persons have been appointed by the respective companies in the HM NEUR as authorized persons in accordance with the Whistleblowing Acts. Authorized persons are, on behalf of each specified HM NEUR, authorized to receive reports, follow up on what has been reported and have contact with and provide feedback to reporting individuals.

1 Sweden

Company	Contact information to personal data controller	Whistleblowing Committee
Heidelberg Materials Sweden AB (556000-6057)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Marieviksgatan 25, Box 47055, 117 43 Stockholm	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck
Heidelberg Materials Cement Sverige AB (556013-5864)	info@cementa.se , +46 72 143 54 72 Box 47210, 100 74 Stockholm.	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Jenny Wallin Sander
Heidelberg Materials Betong Sverige AB (556188-3892)	info@betongindustri.se , +46 72 143 54 72 Marieviksgatan 25, 100 74 Stockholm.	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Anna-Lena Wikgren
Heidelberg Materials Precast Abetong AB (556055-7356)	info@abetong.se , +46 72 143 54 72 Box 24, 351 03 Växjö.	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Catarina Bergkvist

Heidelberg Materials Precast Contiga AB (556270-5979)	info@contiga.se , +46 72 143 54 72 Box 94, 761 21 Norrtälje.	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Staffan Broberg
Heidelberg Materials Ballast Sverige AB (556016-1183)	info@jehander.se , +46 72 143 54 72 Box 47124, 100 74 Stockholm.	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Anna-Lena Wikgren

2 Norway

Company	Contact information to personal data controller	Whistleblowing Committee
Heidelberg Materials Norway AS (980910369)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Lilleakerveien 2A, 0283 OSLO	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck
Heidelberg Materials Sement Norge AS (934949145)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Lilleakerveien 2A, 0283 OSLO	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Helle Davidsen
Heidelberg Materials Tilslag Norge AS (918414304)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Vassbotnen 1, 4313 SANDNES	Hartmut Drescher Peter Linderoth Victor Ask

		Kajsa Runnbeck Anne Tjordal
Heidelberg Materials Betong Norge AS (934468740)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Lilleakerveien 2A, 0283 OSLO	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Kari-Åsta Trulsrud
Heidelberg Materials Prefab Norge AS (971507837)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Peer Gynts vei 1, 1535 MOSS	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Elin Röed
Mibau Stema Norge AS (958990022)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Jelsavegen 512, 4234 JELSA	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Anne Tjordal

3 Iceland

Company	Contact information to personal data controller	Whistleblowing Committee
BM Vallá ehf (450510-0680)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Breiðhöfða 3 110 Reykjavík 412 5000	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Helga Fjóla Sæmundsdóttir

4 Denmark

Company	Contact information to personal data controller	Whistleblowing Committee
Heidelberg Materials Beton Danmark A/S (29189137)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Fredensvej 40, 4100 Ringsted	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Karina Busk Madsen
Heidelberg Materials Precast Denmark A/S (33255047)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Mads Clausens Vej 58, 6360 Tinglev	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck

5 Estonia

Company	Contact information to personal data controller	Whistleblowing Committee
Heidelberg Materials Kunda AS (1015677)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Jaama 2, 44106 Kunda	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck Ulle Kukk

6 Latvia

Company	Contact information to personal data controller	Whistleblowing Committee
Heidelberg Materials SBC Latvia SIA (40003709915)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Zeltiņu iela 130 LV-2167 Mārupe, Mārupes	Hartmut Drescher Peter Linderoth Victor Ask

		Kajsa Runnbeck
--	--	----------------

7 Lithuania

Company	Contact information to personal data controller	Whistleblowing Committee
UAB Heidelberg Materials Lietuva Betonai (304102190)	victor.ask@heidelbergmaterials.com +46 72 143 54 72 Technikos g. 7K, Kaunas.	Hartmut Drescher Peter Linderoth Victor Ask Kajsa Runnbeck