HEIDELBERGCEMENT

# Mandatory data protection information pursuant to GDPR for whistleblower tool "SpeakUp"

## 1. Information about specific processing activity

| | |
|---|---|
| Name and contact details of the controllers | HeidelbergCement AG, Berliner Strasse 6, 69120 Heidelberg, Germany („HCAG"), Telephone: +49 6221-481-0<br>Fax: +49 6221-481-13217, email: info@heidelbergcement.com<br>together with each of its affiliated companies that are using the SpeakUp System ("Affiliate")<br>(HCAG and Affiliate acting as joint-controllers, hereinafter referred to as "Controllers") |
| Contact details of the data protection officers | HeidelbergCement AG, Group Data Protection Officer, Berliner Straße 6, 69120 Heidelberg, Germany, Telephone: +49 6221-481-39603<br>email: data.protection@heidelbergcement.com<br>You can also contact the data protection officer or coordinator of the concerned Affiliate. |
| Description of the processing activity and the joint controllership | The joint controllership arises from the fact that (i) HCAG has introduced the SpeakUp system (whistleblower hotline) within the HeidelbergCement Group as mandatory system for documenting compliance cases, (ii) is responsible for the initial data collection phase, (iii) decides if and to which Affiliate the case is assigned and (iv) has access to the data and uses it for own purposes.<br>In context of joint controllership, HCAG is competent for the processing of personal data during and after the initial collection phase. An incident reporter reports a case either through the website or via a phone call. Phone calls are transcribed by the processor (People InTouch B.V.) and also the IT infrastructure (website) is provided by this processor. The reported incidents are translated by a sub-processor of the processor and the result is submitted to HCAG. HCAG decides which Affiliate (country HQ functions) shall investigate the case and assigns the case to such Affiliate. For the further processing (defining actions and measures, communication with reporting party, documentation/investigation report) of personal data the Affiliate is the responsible controller, but HCAG has access to the data and uses them in own responsibility for statistical and reporting purposes in a pseudonymised form. The Affiliate may add further personal data and leads then the further investigation and handles the case under own responsibility. |

<table>
<tr><td></td><td colspan="2">In context of provision of the SpeakUp System (i.e. the pure IT-infrastructure) to its Affiliates, HCAG is the data processor and the respective Affiliate is the controller.<br><br>For such sections of processing, where the parties do not jointly determine the purposes and means of data processing, each Controller is acting in sole responsibility.</td></tr>
<tr><td rowspan="4">Categories of personal data subject to the processing activity</td><td colspan="2">Employees and third parties can report compliance incidents by phone or by web. Depending on the nature of the reported incident, it is unpredictable which kind of data categories are reported. In particular the following categories may be processed:</td></tr>
<tr><td>Data of incident reporter</td><td>Data of person subject to incident reporting</td></tr>
<tr><td>▪ Contact details (name, job-title, address, email-address, phone number, company, country), in case the incident is not reported on an anonymous basis<br>▪ Session cookie if an incident is reported by using the web-portal (see also the privacy statement for the web portal, which is hosted and administered by the external service provider (processor) People Intouch B.V.)<br>▪ Voice, if an incident is reported by phone (only transcript is provided to the Controllers, the recorded voice is only accessible by the processor People Intouch B.V.)<br>▪ Content of the reported incident</td><td>▪ Contact details (name, job-title, address, email-address, phone number, company, country)<br>▪ Content of the reported incident (which could include but is not limited to: bank data, documents evidencing a specific behaviour, working time records, photos, video surveillance, etc.)<br>▪ Taken measures</td></tr>
<tr><td>Data of (potential) witnesses</td><td>Data of investigators and individuals responsible for measures</td></tr>
</table>

| | | |
|---|---|---|
| | ▪ Contact details (name, job-title, address, email-address, phone number, company, country)<br>▪ Fact, that a person is or might be a witness and role of such person in a reported incident<br>▪ Data the witness provides him-/herself to the Controllers | ▪ Contact details (name, job-title, address, email-address, phone number, company, country) |
| Source of the personal data | ▪ For data incident reporter: The data incident reporter is providing the data him-/herself to the Controllers.<br>▪ Person subject to incident reporting: Data are submitted by a data incident reporter to the Controllers.<br>▪ Data of (potential) witnesses: Data are provided by a data incident reporter, a person subject to incident reporting or the (potential) witness him-/herself.<br>▪ Data of investigators (e.g. Compliance Officer) and individuals responsible for measures: Determination by the employer.<br>▪ Affiliate may provide personal data which are gathered in the course of an investigation. | |
| The personal data is processed for the following purposes | 1. Contact details of incident reporter: Purpose is getting in contact with an incident reporter in order to clarify further the case facts and provide him/her an answer.<br>2. Contact details of person subject to incident reporting: Purpose is identifying any person who is subject to an incident reporting and to start investigation.<br>3. Data of (potential) witness: Purpose is getting in contact with a (potential) witness in order to investigate if the person is indeed a witness and willing to contribute to clarify the facts related to the reported incident.<br>4. Session cookie: The cookie is necessary for the efficient function of the website.<br>5. Voice of incident reporter: Purpose is to open other communication channels than only web-portal, as an internet connection or hardware may not be available to each incident reporter.<br>6. Content of the reported incident: Purpose is to learn about (potential) compliance risks in the organization; to check the content of the reported incidents diligently; and to act in case violations of legal obligations or (internal) regulations are detected. | |

| | |
|---|---|
| | 7. Data about investigation and taken measures: Purpose is to document all steps in investigation and to solve the case properly.<br>8. Data of investigators and individuals responsible for measures: Purpose is the administration and clarification of responsibilities.<br>9. All data mentioned before under point 1-8 are used as well for statistical and reporting purposes (in a pseudonymised form). |
| Legal basis for the data processing of the purposes mentioned under 1-9 above | Legal basis for the data processing under<br><br>1. above is: Art. 6 (1) sentence 1 letter a) GDPR in case an incident reporter decides to report no-anonymously and submits her/his personal contact details to the Controllers.<br><br>2. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' legitimate interest is to identify persons within its organization who may not act in accordance with applicable laws or (internal and external) regulations and to contact such persons or use their contact details to start legal proceeding. Further the contact details may be needed for informing a person subject to an incident reporting about the fact that an incident was reported, in which such person was mentioned.<br><br>3. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' legitimate interest is to identify persons who can contribute to the clarification of a reported incident, so that the Controllers can verify facts and take the appropriate measures to close a case.<br><br>4. above is: Art. 6 (1) letter f) GDPR. The Controllers' legitimate interest is to operate the website, which is not technically possible without setting the necessary cookie.<br><br>5. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' interest is to learn about compliance incidents within the organization and as Internet or computer hardware might not be available everywhere, persons might not be able to report incidents in case no other reporting channel is available. Also phone connection might be considered safer by reporters. Therefore the phone option is offered as a second reporting channel.<br><br>6. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' interest is to learn about compliance incidents within the organization and to stop any inappropriate/illegal behaviour. The |

| | |
|---|---|
| | legal basis for this processing of the content of the reported incident may also be Art. 88 GDPR in conjunction with any local data protection laws (e.g. in Germany: § 26 (1) BDSG (German Data Protection Act), in case the reported content concerns an employee who is a party to a German employment contract).<br><br>7. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' interest is to document an investigation in order to evidence its correctness.<br><br>8. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' interest is the traceability of actions and measures and rectification of the non-compliant situation.<br><br>9. above is: Art. 6 (1) sentence 1 letter f) GDPR. The Controllers' interest is to analyse the cases for statistical purposes and to report about compliance cases to the respective management in a pseudonymised form, so that business operations can be optimized and management can comply with its obligations to ensure an effective compliance system. |
| Recipient or categories of recipients of the personal data | ▪ Controllers<br>▪ External service providers, e.g. People InTouch B.V.<br>▪ As the case may be: external lawyers, authorities (e.g. police, state attorney, court) or administrative bodies or supervisory authorities (e.g. data protection authority, cartel office, BAFIN) |
| Necessity of the data collection | The Controllers are obliged by law to implement an effective compliance management and controls. |
| Place of processing and transmission to third countries | Technically the data are processed on a platform hosted by an external service provider with registered seat in The Netherlands.<br><br>The data will be processed as well in Germany, in the country where the incident reporter is located and any country which is affected by the reported incident.<br><br>Data must be, if necessary, also transmitted to (foreign) authorities, insofar as it is based on legal grounds.<br><br>Hence, the above mentioned recipients may also be based in countries outside the European Economic Area ("third countries"). In third countries, the data protection level may possibly not guaranteed to the same extent as in the European Economic Area. If data is transmitted to a third country, Controllers will ensure that the transmission thereof is executed only in accordance with the statutory provisions (Chapter V GDPR). |

| | |
|---|---|
| Duration for which the personal data are stored | ▪ Voice recording is deleted by the service provider People Intouch after 24 hours, after the Controllers have received the transcript in the Case Management System. It is kept for 5 days on the back-up system.<br>▪ Case data in the SpeakUp System (the system in which the Controllers' communicate with the incident reporter as well as the part of the system to which only the Controllers have access) are anonymized by People Intouch after 14 days, after a case is closed.<br>▪ Case data in the CMS module is stored for 3 years after a case is closed.<br>▪ In single cases the data are stored for a longer period, in case a Controller has a legitimate interest to store the data for a longer period than the aforementioned (e.g. defending against or pursuing legal claims). |

## 2. Your rights as data subject

As a data subject, you may contact either of the Controllers, in particular HeidelbergCement's Group Data Protection officer at any time with an informal message under the contact data mentioned above, in order to exercise your rights in accordance with GDPR. Each Controller will inform the other Controller about the exertion of the rights of a data subject and provide the respective other Controller with all necessary information. In case you request access according to Article 15 GDPR, the Controller to whom the incident was assigned will provide this information.

Your rights are as follows:

- the right to obtain information about the data processed as well as a copy of the data processed (Right of access, Art. 15 GDPR),
- the right to request rectification of inaccurate data or completion of incomplete data (Right of rectification, Art. 16 GDPR),
- the right to request erasure of personal data and in case that personal data was made public, the information to other controllers about the erasure request (Right of erasure, Art. 17 GDPR),
- the right to request restriction of processing (Right to restriction of processing, Art. 18 GDPR),
- the right – in the event that the conditions set out in Art. 20 GDPR are met – to receive the personal data concerning yourself in a structured, commonly used and machine-readable format and the right to transmit those data to another controller for processing (Right to data portability, Art. 20 GDPR),
- the right, on grounds relating to your particular situation, to object at any time to processing of your personal data which is based on Art. 6 (1) sentence 1 letter f) GDPR, with future effect (Right to object, Art. 21 GDPR); in such case, the Controllers no longer process your personal data, unless they demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or the data processing is still necessary for the establishment, exercise or defence of legal claims,

- the right to withdraw a consent at any time in order to prevent data processing which is based on your consent. The withdrawal of consent shall not affect the lawfulness of processing based on the consent prior to the withdrawal (Right to withdrawal, Art. 7 (3) GDPR),
- the right to lodge a complaint with a supervisory authority in accordance with Art. 77 GDPR, pursuant to which you shall without prejudice to any other administrative or judicial remedy, in particular in the Member State of your habitual residence, place of work or place of the alleged infringement, lodge a complaint, if you consider that the processing of personal data relating to you infringes the GDPR.

  You are also welcome to contact us first. In a telephone call, as you know, many things can be clarified.