



Verplichte informatie inzake gegevensbescherming overeenkomstig de AVG voor het klokkenluidersinstrument “SpeakUp” en voor meldingen via e-mail, brief of persoonlijk gesprek

1. Informatie over de specifieke verwerkingsactiviteit

Naam en contactgegevens van de Verwerkingsverantwoordelijken	Heidelberg Materials AG, Berliner Strasse 6, 69120 Heidelberg, Germany (hierna genoemd “HMAG”), Telephone: +49 6221-481-0, Fax: +49 6221-481-13217, Email: info@heidelbergmaterials.com samen met alle gelieerde vennootschappen die gebruikmaken van het SpeakUp-systeem. (HMAG en de gelieerde vennootschappen die als gezamenlijke verwerkingsverantwoordelijken optreden, worden hierna gezamenlijk aangeduid als de “Verwerkingsverantwoordelijken”.)
Contactgegevens van de data protection officers	Heidelberg Materials AG, Group Data Protection Officer, Berliner Strasse 6, 69120 Heidelberg, Germany, Telefoon: +49 6221-481-39603, Email: info.dataprotection@heidelbergmaterials.com U kunt ook contact opnemen met de data protection officers of coördinator voor gegevensbescherming van de betrokken gelieerde vennootschap: BE: Adrien Durieux NL: Silvia Vinken Via: dpb-bene@heidelbergmaterials.com
Beschrijving van de verwerkingsactiviteit en de gezamenlijke verantwoordelijkheid	De gezamenlijke verwerkingsverantwoordelijkheid vloeit voort uit het feit dat: (i) HMAG binnen de Heidelberg Materials Groep het SpeakUp-systeem (meldpunt voor klokkenluiders) heeft ingevoerd als verplicht systeem voor de documentatie van compliancegevallen; (ii) HMAG verantwoordelijk is voor de initiële fase van gegevensverzameling; (iii) HMAG beslist of, en aan welke gelieerde vennootschap, het dossier wordt toegewezen; en (iv) HMAG toegang heeft tot de gegevens en deze voor eigen doeleinden gebruikt. In het kader van deze gezamenlijke verantwoordelijkheid is HMAG bevoegd voor de verwerking van persoonsgegevens tijdens en na de initiële verzamelingsfase. Een melder kan een geval rapporteren via de website of telefonisch. Telefoongesprekken worden getranscribeerd door de verwerker (<i>People Intouch B.V.</i>), die tevens de IT-infrastructuur (website) voor de meldingen levert. De telefonisch gemelde



	gevallen worden getranscribeerd en, indien nodig, in het Engels vertaald; het transcript wordt vervolgens aan HMAG bezorgd. Wanneer meldingen via de website worden gedaan, wordt indien de melding niet in het Engels is een automatische of gewone vertaling uitgevoerd door een vertaler. De verwerker kan bij de uitvoering van zijn diensten onderaannemersinschakelen. HMAG beslist welke gelieerde vennootschap (de betreffende nationale coördinatiefunctie) het geval verder zal onderzoeken en wijst het dossier aan deze vennootschap toe. De gelieerde vennootschap is verantwoordelijk voor de verdere verwerking van de persoonsgegevens (bepaling van acties en maatregelen, communicatie met de melder, documentatie/onderzoeksrapport). HMAG behoudt evenwel toegang tot de gegevens en gebruikt deze onder eigen verantwoordelijkheid voor statistische en rapportagedoeleinden, in gepseudonimiseerde vorm. De gelieerde vennootschap kan bijkomende persoonsgegevens toevoegen en voert vervolgens het verdere onderzoek en de behandeling van het dossier uit onder eigen verantwoordelijkheid. In het kader van de terbeschikkingstelling van het SpeakUp-systeem (d.w.z. de loutere IT-infrastructuur) aan de gelieerde vennootschappen treedt HMAG op als verwerker, terwijl de betrokken gelieerde vennootschap optreedt als verwerkingsverantwoordelijke. Voor die onderdelen van de verwerking waarin de partijen niet gezamenlijk de doeleinden en middelen van de gegevensverwerking bepalen, handelt elke verwerkingsverantwoordelijke onder eigen verantwoordelijkheid.	
Categorieën van persoonsgegevens die worden verwerkt	Werknemers en derden kunnen compliance-incidenten melden via telefoon of elektronisch via de SpeakUp-website, per e-mail, per brief of tijdens een persoonlijk gesprek. Indien een incident niet via het SpeakUp-platform wordt gemeld, wordt het door de bevoegde Compliance Officer in het systeem ingevoerd. Afhankelijk van de aard van het gemelde incident is het niet voorspelbaar welke soorten gegevenscategorieën zullen worden verwerkt. In het bijzonder kunnen de volgende categorieën persoonsgegevens worden verwerkt :	
	Gegevens van de melder van het incident	Gegevens van de persoon over wie het incident wordt gemeld



	▪ Contactgegevens (naam, functie, adres, e-mailadres, telefoonnummer, onderneming, land), indien het incident niet anoniem wordt gemeld. ▪ Sessiecookies, indien een incident via het webportaal wordt gemeld. <i>(Zie ook het privacybeleid voor het webportaal, dat wordt gehost en beheerd door de externe dienstverlener People Intouch B.V. (verwerker).)</i> ▪ De stem van de melder, indien een incident telefonisch wordt gemeld. <i>(Alleen een transcriptie is beschikbaar voor de verantwoordelijken; de opname zelf is enkel toegankelijk voor de verwerker — People Intouch B.V.)</i> ▪ De inhoud van het gemelde incident.	▪ Contactgegevens (naam, functie, adres, e-mailadres, telefoonnummer, onderneming, land). ▪ Inhoud van het gemelde incident (waaronder met name, maar niet uitsluitend: rekeninggegevens, documenten met betrekking tot bepaald gedrag, gegevens over werktijden, foto's, video-opnamen, enz.). ▪ De genomen maatregelen.
	Gegevens van (mogelijke) getuigen	Gegevens van onderzoekers en personen die verantwoordelijk zijn voor maatregelen
	▪ Contactgegevens (naam, functie, adres, e-mailadres, telefoonnummer, onderneming, land) ▪ Het feit dat een persoon een getuige is of mogelijk een getuige zou kunnen zijn, evenals de rol van die persoon in het gemelde incident	▪ Contactgegevens (naam, functie, adres, e-mailadres, telefoonnummer, onderneming, land)



	▪ Gegevens die de getuige zelf aan de verwerkingsverantwoordelijken verstrekt	
Bron van de gegevens	▪ Gegevens van de melder van het incident : de melder verstrekt deze gegevens zelf aan de verwerkingsverantwoordelijken. ▪ Gegevens van de persoon over wie het incident wordt gemeld : deze gegevens worden door de melder van het incident aan de verwerkingsverantwoordelijken meegedeeld. ▪ Gegevens van (mogelijke) getuigen : deze gegevens kunnen afkomstig zijn van de melder van het incident, van de persoon over wie het incident wordt gemeld, of van de (mogelijke) getuige zelf. ▪ Gegevens van onderzoekers (bijvoorbeeld Compliance Officer) en personen die verantwoordelijk zijn voor maatregelen : worden bepaald door de werkgever. ▪ De gelieerde vennootschap (<i>Affiliate</i>) kan persoonsgegevens aanleveren die tijdens het onderzoek zijn verzameld.	
Doeleinden van de verwerking	1. Contactgegevens van de melder van het incident : het doel is om contact op te nemen met de melder om de feiten van de zaak verder te verduidelijken en om hem/haar een antwoord te kunnen geven. 2. Contactgegevens van de persoon over wie het incident wordt gemeld : het doel is om de betrokken persoon te identificeren en een onderzoek te kunnen opstarten. 3. Gegevens van (mogelijke) getuigen : het doel is om contact op te nemen met de (mogelijke) getuige om na te gaan of de persoon inderdaad getuige is en bereid is bij te dragen aan de verduidelijking van de feiten met betrekking tot het gemelde incident. 4. Sessiecookies : het cookie is noodzakelijk voor het goed en efficiënt functioneren van de website. 5. Stem van de melder van het incident : het doel is om andere communicatiemogelijkheden te bieden dan enkel het webportaal, aangezien een internetverbinding of geschikte apparatuur niet voor elke melder beschikbaar kan zijn. 6. Inhoud van het gemelde incident : het doel is om kennis te nemen van (potentiële) compliance-risico's binnen de organisatie, de inhoud van de meldingen zorgvuldig te onderzoeken en op te treden wanneer schendingen van	



	wettelijke verplichtingen of (interne) voorschriften worden vastgesteld. 7. Gegevens over het onderzoek en de genomen maatregelen : het doel is om alle stappen van het onderzoek te documenteren en het dossier op correcte wijze af te handelen. 8. Gegevens van onderzoekers en personen die verantwoordelijk zijn voor maatregelen : het doel is het beheer en de verduidelijking van verantwoordelijkheden. 9. Alle onder de punten 1 tot en met 8 vermelde gegevens worden tevens gebruikt voor statistische en rapportagedoeleinden (in gepseudonimiseerde vorm).
Rechtsgrond voor de verwerking van de gegevens voor de hierboven vermelde doeleinden (punten 1-9)	Rechtsgrond voor de verwerking van de gegevens: Voor punt 1: artikel 6, lid 1, eerste zin, onder a) AVG - in gevallen waarin de melder van het incident ervoor kiest zijn/haar identiteit bekend te maken en persoonlijke contactgegevens aan de verwerkingsverantwoordelijken verstrekt. Voor punt 2: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin personen binnen de organisatie te identificeren die mogelijk niet handelen in overeenstemming met de toepasselijke wetgeving of met interne en externe voorschriften, en om met deze personen contact op te nemen of hun contactgegevens te gebruiken voor het opstarten van juridische procedures. Daarnaast kunnen de contactgegevens nodig zijn om een persoon over wie een incident is gemeld, te informeren over het feit dat een melding werd ingediend waarin hij/zij wordt genoemd. Voor punt 3: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin personen te identificeren die kunnen bijdragen tot de opheldering van een gemeld incident, zodat de verwerkingsverantwoordelijken de feiten kunnen verifiëren en passende maatregelen kunnen nemen om het dossier af te sluiten. Voor punt 4: artikel 6, lid 1, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin de website te



	kunnen laten functioneren; dit is technisch niet mogelijk zonder het plaatsen van het noodzakelijke cookie. Voor punt 5: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin kennis te nemen van compliance-incidenten binnen de organisatie. Omdat internettoegang of computerapparatuur niet overal beschikbaar is, zouden bepaalde personen geen incidenten kunnen melden indien er geen alternatief meldingskanaal voorhanden was. Bovendien kan een telefonische melding door sommige melders als veiliger worden beschouwd. Daarom wordt de telefonische optie aangeboden als tweede meldingskanaal. Voor punt 6: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin kennis te nemen van compliance-incidenten binnen de organisatie en elk ongepast of onwettig gedrag te stoppen. De rechtsgrond voor de verwerking van de inhoud van de gemelde incidenten kan tevens artikel 88 AVG zijn, in samenhang met de toepasselijke nationale wetgeving inzake gegevensbescherming (bijvoorbeeld in Duitsland: § 26, lid 1, BDSG - <i>Bundesdatenschutzgesetz</i>), wanneer de gemelde inhoud betrekking heeft op een werknemer die partij is bij een Duitse arbeidsovereenkomst. Voor punt 7: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin het onderzoek te documenteren om de juistheid en regelmatigheid ervan aan te tonen. Voor punt 8: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin de traceerbaarheid van de genomen acties en maatregelen te waarborgen en de niet-conforme situatie te corrigeren. Voor punt 9: artikel 6, lid 1, eerste zin, onder f) AVG - het gerechtvaardigde belang van de verwerkingsverantwoordelijken bestaat erin de gevallen te analyseren voor statistische doeleinden en om, in
--	---



	gepseudonimiseerde vorm, te rapporteren over compliancegevallen aan het bevoegde management, zodat de bedrijfsvoering kan worden geoptimaliseerd en het management kan voldoen aan zijn verplichting om een doeltreffend compliance-systeem te waarborgen.
Ontvangers van de gegevens	▪ Verwerkingsverantwoordelijken ▪ Externe dienstverleners, bijvoorbeeld <i>People Intouch B.V.</i> ▪ In voorkomend geval : externe advocaten, overheidsinstanties (zoals politie, openbaar ministerie, rechtbank) of administratieve organen of toezichthoudende autoriteiten (zoals de gegevensbeschermingsautoriteit, de mededingingsautoriteit, of de <i>BAFIN</i>).
Noodzaak van de gegevensverzameling	De verwerkingsverantwoordelijken zijn wettelijk verplicht een doeltreffend compliancebeheer en interne controlemechanismen te implementeren. Specifieke verplichtingen op dit vlak vloeien onder meer voort uit de Wet bescherming klokkenluiders (<i>Whistleblower Protection Act</i>) en de Wet op de zorgplicht in de toeleveringsketen (<i>Supply Chain Due Diligence Act</i>).
Plaats van verwerking en doorgifte aan derde landen	Technisch gezien worden de gegevens verwerkt op een platform dat wordt gehost door een externe dienstverlener met maatschappelijke zetel in Nederland. De gegevens worden bovendien verwerkt in Duitsland, in het land waar de melder van het incident zich bevindt, en in elk land dat door het gemelde incident wordt geraakt. Indien nodig moeten de gegevens ook worden doorgegeven aan (buitenlandse) autoriteiten, voor zover dit gebaseerd is op een wettelijke grondslag. Daarom kunnen de hierboven vermelde ontvangers ook gevestigd zijn in landen buiten de Europese Economische Ruimte (EER), zogenaamde <i>derde landen</i>. In dergelijke derde landen kan het niveau van gegevensbescherming mogelijk niet in dezelfde mate worden gewaarborgd als binnen de EER. Wanneer gegevens naar een derde land worden doorgegeven, zorgen de verwerkingsverantwoordelijken ervoor dat deze doorgifte uitsluitend plaatsvindt in overeenstemming met de wettelijke bepalingen van Hoofdstuk V van de AVG.
Bewaartermijn van de persoonsgegevens	▪ De geluidsopname wordt door de dienstverlener <i>People Intouch</i> verwijderd binnen 24 uur nadat de



	verwerkingsverantwoordelijken het transcript in het SpeakUp-systeem hebben ontvangen, waartoe enkel de verwerkingsverantwoordelijken toegang hebben. De geluidsopname blijft gedurende 5 dagen bewaard in het back-upsysteem. ▪ De dossiergegevens in het SpeakUp-systeem worden bewaard gedurende 3 jaar na de afsluiting van het dossier. ▪ In uitzonderlijke gevallen kunnen de gegevens gedurende een langere periode worden bewaard indien een verwerkingsverantwoordelijke een gerechtvaardigd belang heeft om de gegevens langer te bewaren dan de hierboven vermelde termijn (bijvoorbeeld ter verdediging tegen of voor het instellen van juridische vorderingen).
--	--

2. Uw rechten als betrokkene

Als betrokkene kunt u te allen tijde contact opnemen met een van de verwerkingsverantwoordelijken, en in het bijzonder met de Group Data Protection Officer van Heidelberg Materials, via een informeel bericht naar de hierboven vermelde contactgegevens, om uw rechten overeenkomstig de AVG uit te oefenen. Elke verwerkingsverantwoordelijke zal de andere verwerkingsverantwoordelijke informeren over de uitoefening van de rechten van een betrokkene en de andere partij alle noodzakelijke informatie verstrekken. Wanneer u een verzoek tot inzage indient overeenkomstig artikel 15 AVG, zal de verwerkingsverantwoordelijke aan wie het incident werd toegewezen deze informatie verstrekken.

Uw rechten zijn de volgende :

- Recht op inzage (*artikel 15 AVG*) - het recht om informatie te verkrijgen over de verwerkte gegevens, alsook een kopie van de verwerkte gegevens te ontvangen,
- Recht op rectificatie (*artikel 16 AVG*) - het recht om onjuiste persoonsgegevens te laten verbeteren of onvolledige gegevens aan te vullen,
- Recht op gegevenswissing (*artikel 17 AVG*) - het recht om te verzoeken dat uw persoonsgegevens worden gewist en, indien deze persoonsgegevens openbaar zijn gemaakt, om andere verwerkingsverantwoordelijken te informeren over uw verzoek tot wissing,
- Recht op beperking van de verwerking (*artikel 18 AVG*) - het recht om te verzoeken dat de verwerking van uw persoonsgegevens wordt beperkt,
- Recht op gegevensoverdraagbaarheid (*artikel 20 AVG*) - indien aan de in dit artikel vermelde voorwaarden is voldaan, het recht om de u betreffende persoonsgegevens te ontvangen in een gestructureerd, gangbaar en machineleesbaar formaat, alsook het recht om deze gegevens over te dragen aan een andere verwerkingsverantwoordelijke,
- Recht van bezwaar (*artikel 21 AVG*) - het recht om, om redenen die verband houden met uw specifieke situatie, te allen tijde bezwaar te maken tegen de verwerking van uw



persoonsgegevens die gebaseerd is op artikel 6, lid 1, onder f), AVG, met werking voor de toekomst; in dat geval zullen de verwerkingsverantwoordelijken uw persoonsgegevens niet langer verwerken, tenzij zij dwingende gerechtvaardigde gronden voor de verwerking kunnen aantonen die zwaarder wegen dan uw belangen, rechten en vrijheden, of indien de verwerking nog steeds noodzakelijk is voor de instelling, uitoefening of verdediging van rechtsvorderingen,

- Recht om toestemming in te trekken (*artikel 7, lid 3, AVG*) - het recht om uw toestemming te allen tijde in te trekken en zo verdere verwerking van persoonsgegevens die op uw toestemming is gebaseerd, te voorkomen. De intrekking van de toestemming tast de rechtmatigheid van de verwerking op basis van de toestemming vóór de intrekking niet aan,
- Recht om een klacht in te dienen bij een toezichthoudende autoriteit (*artikel 77 AVG*) - dit recht verleent u, onverminderd andere administratieve of gerechtelijke rechtsmiddelen, de mogelijkheid om een klacht in te dienen, met name in de lidstaat waar u gewoonlijk verblijft, werkt, of waar de vermeende inbreuk heeft plaatsgevonden, indien u van mening bent dat de verwerking van uw persoonsgegevens in strijd is met de AVG.

U kunt uiteraard ook eerst rechtstreeks contact met ons opnemen. In een telefonisch gesprek kunnen, zoals u weet, vaak al veel zaken worden opgehelderd.