



Informations obligatoires sur la protection des données conformément au RGPD concernant l'outil de signalement « SpeakUp » ainsi que les signalements effectués par e-mail, courrier ou lors d'un entretien en personne

1. Informations relatives à l'activité de traitement spécifique

Nom et coordonnées des responsables du traitement	Heidelberg Materials AG, Berliner Strasse 6, 69120 Heidelberg, Germany (ci-après dénommée "HMAG"), Téléphone: +49 6221-481-0, Fax: +49 6221-481-13217, Email: info@heidelbergmaterials.com ainsi que toute société affiliée utilisant le système SpeakUp. (HMAG et les sociétés affiliées agissant en tant que responsables conjoints du traitement sont ci-après collectivement dénommées les « Responsables du traitement ».)
Coordonnées des délégués à la protection des données	Heidelberg Materials AG, Group Data Protection Officer, Berliner Strasse 6, 69120 Heidelberg, Germany, Téléphone: +49 6221-481-39603, Email: info.dataprotection@heidelbergmaterials.com Vous pouvez également contacter le délégué ou le coordinateur à la protection des données de la société affiliée concernée : BE: Adrien Durieux NL: Silvia Vinken Via: dpb-bene@heidelbergmaterials.com
Description de l'activité de traitement et de la responsabilité conjointe	La responsabilité conjointe découle du fait que : (i) HMAG a mis en place au sein du groupe Heidelberg Materials le système SpeakUp (ligne d'alerte) comme dispositif obligatoire pour la documentation des cas de conformité ; (ii) HMAG est responsable de la phase initiale de collecte des données ; (iii) elle décide si un dossier est attribué à une société affiliée et, le cas échéant, laquelle ; et (iv) elle a accès aux données et les utilise à ses propres fins. Dans le cadre de la responsabilité conjointe, HMAG est compétente pour le traitement des données à caractère personnel durant et après la phase initiale de collecte. Un lanceur d'alerte peut signaler un cas soit via le site web, soit par téléphone. Les appels téléphoniques sont retranscrits par le sous-traitant (<i>People Intouch B.V.</i>), qui fournit également l'infrastructure informatique (site web) utilisée pour le signalement. Les signalements



	effectués par téléphone sont retranscrits et, si nécessaire, traduits en anglais ; la transcription est ensuite transmise à HMAG. Lorsque les signalements sont effectués via le site web, une traduction automatique ou humaine est assurée si la langue utilisée n'est pas l'anglais. Le sous-traitant peut recourir à des sous-traitants dans le cadre de la prestation de ses services. HMAG décide quelle société affiliée (généralement la structure nationale concernée) sera chargée d'examiner le dossier et lui attribue le cas. La société affiliée est responsable du traitement ultérieur des données à caractère personnel (détermination des actions et mesures à prendre, communication avec l'auteur du signalement, documentation/rapport d'enquête). HMAG conserve toutefois un accès aux données et peut les utiliser, sous sa propre responsabilité, à des fins statistiques et de reporting, sous forme pseudonymisée. La société affiliée peut compléter les données à caractère personnel et conduit ensuite l'enquête sous sa propre responsabilité. Dans le cadre de la fourniture du système SpeakUp (c'est-à-dire de la simple infrastructure informatique) aux sociétés affiliées, HMAG agit en qualité de sous-traitant, tandis que la société affiliée concernée agit en qualité de responsable du traitement. Pour les volets du traitement pour lesquels les parties ne déterminent pas conjointement les finalités et les moyens du traitement, chaque responsable agit sous sa propre responsabilité.	
Catégories de données à caractère personnel faisant l'objet du traitement	Les employés et les tiers peuvent signaler des incidents de conformité par téléphone, via le site web SpeakUp, par e-mail, par courrier ou lors d'un entretien en personne. Si un incident n'est pas signalé via la plateforme SpeakUp, il sera saisi dans celle-ci par le responsable conformité compétent. En fonction de la nature de l'incident signalé, il est impossible de prévoir quelles catégories de données seront concernées. Les catégories suivantes peuvent notamment être traitées :	
	Données du lanceur d'alerte	Données de la personne faisant l'objet du signalement
	▪ Coordonnées (nom, fonction, adresse, adresse	▪ Coordonnées (nom, fonction, adresse, adresse



	e-mail, numéro de téléphone, société, pays) si le signalement n'est pas anonyme. ▪ Cookie de session si le signalement est effectué via le portail web. (Voir également la politique de confidentialité du portail web, hébergé et géré par le prestataire externe <i>People Intouch B.V.</i> — sous-traitant). ▪ Voix du lanceur d'alerte lorsque le signalement est effectué par téléphone. (Seule une transcription est accessible aux personnes responsables ; l'enregistrement vocal lui-même n'est accessible qu'au sous-traitant <i>People Intouch B.V.</i>). ▪ Le contenu de l'incident signalé	e-mail, numéro de téléphone, société, pays). ▪ Contenu de l'incident signalé (en ce compris, mais sans s'y limiter: données de compte, documents liés à un comportement spécifique, données sur le temps de travail, enregistrements photos ou vidéos, etc.). ▪ Mesures prises.
	Données des (potentiels) témoins	Données des enquêteurs et des personnes chargées des mesures
	▪ Coordonnées (nom, fonction, adresse, adresse e-mail, numéro de téléphone, société, pays)	▪ Coordonnées (nom, fonction, adresse, adresse e-mail, numéro de téléphone, société, pays)



	▪ Fait dont une personne est ou pourrait être témoin, ainsi que le rôle de cette personne dans l'incident signalé ▪ Données que le témoin fournit lui-même aux responsables du traitement	
Source des données à caractère personnel	▪ Données du lanceur d'alerte : le lanceur d'alerte fournit lui-même ses données aux responsables du traitement. ▪ Données de la personne faisant l'objet du signalement : ces données sont communiquées par le lanceur d'alerte aux responsables du traitement. ▪ Données des (potentiels) témoins : ces données peuvent être fournies par le lanceur d'alerte, la personne faisant l'objet du signalement ou le témoin lui-même. ▪ Données des enquêteurs (par ex. responsable conformité) et des personnes chargées des mesures : ces données sont déterminées par l'employeur. ▪ Une société affiliée peut également fournir des données à caractère personnel collectées au cours d'une enquête.	
Les données à caractère personnel sont traitées aux fins suivantes	1. Coordonnées du lanceur d'alerte : permettre de contacter le lanceur d'alerte afin de clarifier les faits du dossier et de lui fournir une réponse 2. Coordonnées de la personne faisant l'objet du signalement : identifier toute personne visée par un signalement et initier l'enquête. 3. Données des (potentiels) témoins : permettre de contacter un témoin potentiel afin de vérifier s'il est effectivement témoin et s'il est disposé à contribuer à la clarification des faits liés à l'incident signalé. 4. Cookie de session : assurer le bon fonctionnement technique et efficace du site web.	



	5. Voix du lanceur d'alerte : permettre d'ouvrir d'autres canaux de communication que le portail web, dans la mesure où une connexion internet ou un équipement technique peut ne pas être disponible pour tous les lanceurs d'alerte. 6. Contenu de l'incident signalé : permettre d'identifier d'éventuels risques de conformité au sein de l'organisation, d'examiner avec diligence le contenu des signalements et d'agir en cas de violation d'obligations légales ou de règlements (internes ou externes). 7. Données relatives à l'enquête et aux mesures prises : documenter toutes les étapes de l'enquête et assurer un traitement adéquat du dossier. 8. Données des enquêteurs et des personnes chargées des mesures : permettre la gestion et la clarification des responsabilités. 9. L'ensemble des données mentionnées aux points 1 à 8 peut également être utilisé à des fins statistiques et de reporting (sous forme pseudonymisée).
Base juridique du traitement des données pour les finalités mentionnées aux points 1 à 9	Base juridique concernant le traitement des données: Pour le point 1 ci-dessus: article 6, paragraphe 1, phrase 1, point a) du RGPD, lorsque le lanceur d'alerte choisit de révéler son identité et de communiquer ses coordonnées personnelles aux responsables du traitement. Pour le point 2 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est d'identifier, au sein de leur organisation, les personnes susceptibles de ne pas agir conformément aux lois applicables ou aux règlements (internes ou externes), de les contacter ou d'utiliser leurs coordonnées pour engager une procédure juridique. Les coordonnées peuvent également être nécessaires pour informer la personne visée qu'un signalement la concernant a été déposé. Pour le point 3 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est d'identifier les personnes pouvant contribuer à la clarification d'un incident signalé, afin de



	vérifier les faits et de prendre les mesures appropriées pour clore le dossier. Pour le point 4 ci-dessus: article 6, paragraphe 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est d'assurer le fonctionnement du site web, ce qui n'est pas techniquement possible sans l'installation du cookie nécessaire. Pour le point 5 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est de permettre la prise de connaissance d'incidents de conformité au sein de l'organisation. Dans la mesure où une connexion Internet ou un équipement informatique peut ne pas être disponible partout, certaines personnes pourraient être dans l'impossibilité de signaler un incident si aucun autre canal n'est accessible. De plus, la communication téléphonique peut être perçue comme plus sûre par certains lanceurs d'alerte. C'est pourquoi l'option de signalement par téléphone est proposée comme deuxième canal de communication. Pour le point 6 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est de détecter les incidents de conformité au sein de l'organisation et de mettre un terme à tout comportement inapproprié ou illégal. La base juridique applicable au traitement du contenu de l'incident signalé peut également être l'article 88 du RGPD, combiné avec la législation nationale sur la protection des données (par exemple, en Allemagne : § 26, paragraphe 1, BDSG — <i>Bundesdatenschutzgesetz</i>, loi fédérale allemande sur la protection des données), lorsque le contenu signalé concerne un salarié lié par un contrat de travail de droit allemand. Pour le point 7 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est de documenter une enquête afin de démontrer sa régularité. Pour le point 8 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables
--	--



	du traitement est d'assurer la traçabilité des actions et des mesures et la correction des situations non conformes Pour le point 9 ci-dessus: article 6, paragraphe 1, phrase 1, point f) du RGPD. L'intérêt légitime des responsables du traitement est d'analyser les cas à des fins statistiques et de rendre compte des cas de conformité à la direction concernée sous forme pseudonymisée, afin d'optimiser les opérations et de permettre à la direction de remplir ses obligations en matière de mise en place d'un système de conformité efficace.
Destinataires ou catégories de destinataires des données à caractère personnel	▪ Responsables du traitement ▪ Prestataires de services externes, par exemple <i>People Intouch B.V.</i> ▪ Le cas échéant : avocats externes, autorités (p. ex. police, ministère public, tribunaux) ou organismes administratifs ou autorités de contrôle (p. ex. autorité de protection des données, autorité de la concurrence, BAFIN)
Nécessité de la collecte des données	Les responsables du traitement sont légalement tenus de mettre en œuvre un système de gestion de la conformité efficace et des mécanismes de contrôle appropriés. Des obligations spécifiques à cet égard découlent notamment de la loi sur la protection des lanceurs d'alerte (<i>Whistleblower Protection Act</i>) et de la loi sur le devoir de vigilance dans les chaînes d'approvisionnement (<i>Supply Chain Due Diligence Act</i>).
Lieu du traitement et transfert vers des pays tiers	Sur le plan technique, les données sont traitées sur une plateforme hébergée par un prestataire de services externe ayant son siège aux Pays-Bas. Les données sont également traitées en Allemagne, dans le pays où se trouve le lanceur d'alerte, ainsi que dans tout pays concerné par l'incident signalé. Les données doivent, si nécessaire, être transmises à des autorités (étrangères) lorsque cela repose sur un fondement juridique. Les destinataires mentionnés ci-dessus peuvent donc être établis dans des pays situés en dehors de l'Espace économique européen (« <i>pays tiers</i> »). Dans ces pays, le niveau de protection des données peut ne pas être



	garanti dans la même mesure que dans l'Espace économique européen. Si un transfert vers un pays tiers est effectué, les responsables du traitement veilleront à ce qu'il le soit uniquement conformément aux dispositions légales applicables (chapitre V du RGPD).
Durée de conservation des données à caractère personnel	▪ L'enregistrement vocal est supprimé par le prestataire <i>People Intouch</i> dans un délai de 24 heures après que les responsables du traitement ont reçu la transcription dans le système SpeakUp, auquel seuls les responsables ont accès. L'enregistrement vocal est toutefois conservé dans le système de sauvegarde pendant 5 jours. ▪ Les données du dossier dans le système SpeakUp sont conservées pendant 3 ans après la clôture du dossier. ▪ Dans certains cas individuels, les données peuvent être conservées plus longtemps si un responsable du traitement dispose d'un intérêt légitime à leur conservation au-delà de cette durée (par exemple, pour la défense ou la poursuite de réclamations juridiques).

2. Vos droits en tant que personne concernée

En tant que personne concernée, vous pouvez à tout moment contacter l'un ou l'autre des responsables du traitement en particulier le délégué à la protection des données du Groupe Heidelberg Materials par un message informel envoyé aux coordonnées mentionnées ci-dessus, afin d'exercer vos droits conformément au RGPD.

Chaque responsable informera l'autre de l'exercice des droits d'une personne concernée et lui fournira toutes les informations nécessaires. En cas de demande d'accès fondée sur l'article 15 du RGPD, le responsable à qui le dossier a été attribué fournira les informations demandées.

Vos droits sont les suivants :

- Droit d'accès (*article 15 RGPD*) – le droit d'obtenir des informations sur les données traitées ainsi qu'une copie des données concernées,
- Droit de rectification (*article 16 RGPD*) – le droit de demander la rectification des données inexacts ou le complément des données incomplètes,
- Droit à l'effacement des données (*article 17 RGPD*) - le droit de demander l'effacement des données à caractère personnel et, dans le cas où ces données auraient été rendues publiques, le droit d'informer les autres responsables du traitement de cette demande d'effacement,



- Droit à la limitation du traitement (*article 18 RGPD*) - le droit de demander la limitation du traitement de ses données personnelles,
- Droit à la portabilité des données (*article 20 RGPD*) - le droit, lorsque les conditions prévues à l'article 20 du RGPD sont remplies, de recevoir les données à caractère personnel vous concernant dans un format structuré, couramment utilisé et lisible par machine, ainsi que le droit de transmettre ces données à un autre responsable du traitement,
- Droit d'opposition (*article 21 RGPD*) - le droit de s'opposer, à tout moment et pour des raisons tenant à votre situation particulière, au traitement de vos données à caractère personnel fondé sur l'article 6, paragraphe 1, phrase 1, point f) du RGPD, avec effet pour l'avenir; dans ce cas, les responsables du traitement cesseront de traiter vos données, à moins qu'ils ne démontrent l'existence de motifs légitimes impérieux justifiant le traitement, qui prévalent sur vos intérêts, droits et libertés, ou que le traitement demeure nécessaire à la constatation, l'exercice ou la défense de droits en justice,
- Droit de retrait du consentement (*article 7, paragraphe 3, RGPD*) - le droit de retirer à tout moment votre consentement afin de mettre fin à un traitement fondé sur celui-ci. Le retrait du consentement n'affecte pas la licéité du traitement fondé sur le consentement effectué avant le retrait,
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle, conformément à l'article 77 du RGPD - Sans préjudice de tout autre recours administratif ou judiciaire, vous pouvez notamment déposer une réclamation dans l'État membre où se trouve votre résidence habituelle, votre lieu de travail ou le lieu de l'infraction présumée, si vous estimez que le traitement de vos données à caractère personnel enfreint le RGPD.

Vous êtes également invité à nous contacter directement en premier lieu : un appel téléphonique permet souvent de clarifier rapidement de nombreux points.