## Obowiązkowa klauzula informacyjna dotycząca przetwarzania danych osobowych w przypadku narzędzia dla sygnalistów "SpeakUp"

zgodnie z art. 13 i 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej "Rozporządzenie").

### 1. Informacja o czynności przetwarzania

| | |
|---|---|
| Administrator | Administratorem Państwa danych osobowych jest<br>Heidelberg Materials AG<br>Berliner Strasse 6<br>69120 Heidelberg<br>Niemcy ("HMAG"),<br>tel.: +49 6221 481 0<br>faks: +49 6221 481 13217<br>e-mail: info@heidelbergcement.com<br>wraz z każdą z jej spółek powiązanych korzystających z Systemu SpeakUp ("Partner")<br>(HMAG i Partner działający jako współadministratorzy, zwani dalej "Administratorami") |
| Dane kontaktowe inspektora ochrony danych | Inspektor Ochrony Danych Grupy Heidelberg Materials<br>Heidelberg Materials AG<br>Berliner Strasse 6<br>69120 Heidelberg<br>Niemcy<br>tel.: +49 6221 481 39603<br>e-mail: info.dataprotection@heidelbergmaterials.com<br><br>Można także skontaktować się z inspektorem ochrony danych lub koordynatorem danego Partnera:<br><br>Koordynator Ochrony Danych Osobowych Grupy Górażdże<br>Górażdże Cement S.A.<br>Chorula, ul. Cementowa 1<br>47-316 Górażdże<br>tel. +48 77 777 8195<br>e-mail: odo@gorazdze.pl |

<table>
<tr><td>Opis czynności przetwarzania i współadministracji</td><td colspan="2">Współadministrowanie wynika z faktu, że (i) HMAG wprowadziła w ramach Grupy Heidelberg Materials system SpeakUp (gorąca linia dla sygnalistów) jako obowiązkowy system dokumentowania spraw w zakresie compliance, (ii) jest odpowiedzialna za wstępną fazę gromadzenia danych, (iii) decyduje, czy oraz któremu Partnerowi przypisana jest sprawa oraz (iv) ma dostęp do danych i wykorzystuje je do własnych celów. W kontekście wspólnego administratora HMAG jest właściwa w zakresie przetwarzania danych osobowych w początkowej fazie gromadzenia danych i po niej. Osoba zgłaszająca incydent zgłasza sprawę za pośrednictwem strony internetowej lub telefonicznie. Rozmowy telefoniczne są transkrybowane przez podmiot przetwarzający (People InTouch B.V.), a także infrastruktura IT (strona internetowa) jest zapewniana przez ten podmiot przetwarzający. Zgłoszone incydenty są tłumaczone przez podmiot pod-przetwarzający podmiotu przetwarzającego, a wynik przekazywany jest do HMAG. HMAG decyduje, który Partner (centrala krajowa) zbada sprawę i przydziela sprawę temu Partnerowi. W celu dalszego przetwarzania (określenie działań i środków, komunikacja ze stroną zgłaszającą, dokumentacja/raport z dochodzenia) danych osobowych odpowiedzialnym administratorem jest Partner, ale HMAG ma dostęp do danych i wykorzystuje je na własną odpowiedzialność do celów statystycznych i raportowych w pseudonimizowanej formie. Partner może dodać dalsze dane osobowe i następnie prowadzi dalsze dochodzenie oraz prowadzi sprawę na własną odpowiedzialność.<br><br>W kontekście udostępniania Systemu SpeakUp (tj. czystej infrastruktury IT) swoim Partnerom, HMAG jest podmiotem przetwarzającym dane, a odpowiedni Partner jest administratorem.<br><br>Za te etapy przetwarzania, w których strony nie ustalają wspólnie celów i sposobów przetwarzania danych, każdy Administrator działa na własną odpowiedzialność.</td></tr>
<tr><td rowspan="3">Kategorie danych osobowych podlegających przetwarzaniu</td><td colspan="2">Pracownicy i osoby trzecie mogą zgłaszać przypadki naruszenia zasad Compliance przez telefon lub Internet. W zależności od charakteru zgłoszonego zdarzenia nie można przewidzieć, jakie kategorie danych zostaną zgłoszone. W szczególności przetwarzane mogą być następujące kategorie:</td></tr>
<tr><td>Dane osoby zgłaszającej incydent</td><td>Dane osoby objętej zgłoszeniem</td></tr>
<tr><td>- Dane kontaktowe (imię i nazwisko, stanowisko, adres, adres e-mail, numer telefonu, spółka, kraj), w przypadku gdy zdarzenie nie jest zgłaszane anonimowo.<br>- Plik cookie sesji, jeśli zdarzenie jest zgłaszane za pośrednictwem portalu internetowego (patrz także oświadczenie o ochronie prywatności portalu internetowego, którego gospodarzem i administratorem jest zewnętrzny usługodawca (podmiot przetwarzający) People Intouch B.V.)</td><td>- Dane kontaktowe (imię i nazwisko, stanowisko, adres, adres e-mail, numer telefonu, spółka, kraj)<br>- Treść zgłoszonego zdarzenia (które może obejmować między innymi: dane bankowe, dokumenty potwierdzające określone zachowanie, dokumentację czasu pracy, zdjęcia, monitoring wideo, itp.)<br>- Podjęte działania</td></tr>
</table>

| | | |
|---|---|---|
| | - Głos, w przypadku zgłoszenia zdarzenia telefonicznie (Administratorom przekazywana jest jedynie transkrypcja, nagranie głosu jest dostępne wyłącznie dla podmiotu przetwarzającego People Intouch B.V.)<br>- Treść zgłoszonego zdarzenia | |
| | Dane (potencjalnych) świadków | Dane osób badających zgłoszenie i osób odpowiedzialnych za środki zaradcze |
| | - Dane kontaktowe (imię i nazwisko, stanowisko, adres, adres e-mail, numer telefonu, spółka, kraj)<br>- Fakt, że dana osoba jest lub może być świadkiem oraz rola tej osoby w zgłoszonym zdarzeniu<br>- Dane podawane przez świadka Administratorom | - Dane kontaktowe (imię i nazwisko, stanowisko, adres, adres e-mail, numer telefonu, spółka, kraj) |
| Źródło danych osobowych | - W przypadku osoby zgłaszającej zdarzenie: osoba zgłaszająca zdarzenie samodzielnie przekazuje swoje dane Administratorom.<br>- Osoba objęta zgłoszeniem: dane przekazywane są Administratorom przez osobę zgłaszającą zdarzenie.<br>- Dane (potencjalnych) świadków: dane są przekazywane przez osobę zgłaszającą zdarzenie, osobę objętą zgłoszeniem lub przez samego (potencjalnego) świadka.<br>- Dane osób badających dochodzenie (np. Compliance Officera) i osób odpowiedzialnych za środki zaradcze: ustalane przez pracodawcę.<br>- Partner może dostarczyć dane osobowe zebrane w trakcie dochodzenia. | |
| Cel przetwarzania danych osobowych: | 1. Dane kontaktowe osoby zgłaszającej zdarzenie: celem jest skontaktowanie się z osobą zgłaszającą zdarzenie w celu dalszego wyjaśnienia faktów w sprawie i udzielenia mu/jej odpowiedzi.<br>2. Dane kontaktowe osoby, której dotyczy zgłoszenie: celem jest identyfikacja każdej osoby, której dotyczy zgłoszenie i rozpoczęcie dochodzenia.<br>3. Dane (potencjalnego) świadka: celem jest nawiązanie kontaktu z (potencjalnym) świadkiem w celu sprawdzenia, czy dana osoba rzeczywiście jest świadkiem i czy chce przyczynić się do wyjaśnienia faktów związanych ze zgłoszonym zdarzeniem.<br>4. Plik cookie sesji: plik cookie jest niezbędny do sprawnego funkcjonowania witryny.<br>5. Głos osoby zgłaszającej zdarzenie: celem jest otwarcie innych kanałów komunikacji niż tylko portal internetowy, ponieważ połączenie internetowe lub sprzęt mogą nie być dostępne dla każdego zgłaszającego incydent. | |

| | |
|---|---|
| | 6. Treść zgłaszanego zdarzenia: celem jest poznanie (potencjalnych) ryzyk compliance w organizacji, skrupulatne sprawdzanie treści zgłaszanych zdarzeń oraz podjęcie działań w przypadku wykrycia naruszeń obowiązków prawnych lub przepisów (wewnętrznych).<br>7. Dane o dochodzeniu i podjętych środkach: celem jest udokumentowanie wszystkich etapów śledztwa i prawidłowe rozwiązanie sprawy.<br>8. Dane osób badających zgłoszenie i osób odpowiedzialnych za środki zaradcze: celem jest administracja i wyjaśnienie obowiązków.<br>9. Wszelkie dane, o których mowa wcześniej w pkt. 1-8, wykorzystywane są także w celach statystycznych i raportowych (w formie pseudonimizowanej). |
| Podstawa prawna przetwarzania danych | Podstawą prawną przetwarzania danych opisanych powyżej jest:<br>1. Punkt 1 powyżej: art. 6 ust. 1 a) Rozporządzenia, w przypadku, gdy osoba zgłaszająca zdarzenie zdecyduje się nie zgłaszać anonimowo i przekaże swoje dane kontaktowe Administratorom<br>2. Punkt 2 powyżej: art. 6 ust. 1 f) Rozporządzenia. Prawnie uzasadnionym interesem Administratorów jest identyfikacja w swojej organizacji osób, które mogą działać niezgodnie z obowiązującymi przepisami prawa lub regulacjami (wewnętrznymi i zewnętrznymi) oraz kontakt z takimi osobami lub wykorzystanie ich danych kontaktowych w celu wszczęcia postępowania prawnego. Ponadto dane kontaktowe mogą być potrzebne w celu poinformowania osoby objętej zgłoszeniem zdarzenia o fakcie zgłoszenia zdarzenia, w którym wspomniana została taka osoba.<br>3. Punkt 3 powyżej: art. 6 ust. 1 f) Rozporządzenia. Prawnie uzasadnionym interesem Administratorów jest wskazanie osób, które mogą przyczynić się do wyjaśnienia zgłoszonego zdarzenia, aby Administratorzy mogli zweryfikować fakty i podjąć odpowiednie działania w celu zamknięcia sprawy.<br>4. Punkt 4 powyżej: art. 6 ust. 1 f) Rozporządzenia. Prawnie uzasadnionym interesem Administratorów jest prowadzenie tego serwisu internetowego, co nie jest technicznie możliwe bez ustawienia niezbędnego pliku cookie.<br>5. Punkt 5 powyżej: art. 6 ust. 1 f) Rozporządzenia. W interesie Administratorów jest zdobywanie wiedzy na temat zdarzeń Compliance w organizacji, a ponieważ Internet lub sprzęt komputerowy mogą nie być wszędzie dostępne, osoby mogą nie być w stanie składać zgłoszeń, jeśli nie jest dostępny żaden inny kanał zgłaszania. Również połączenie telefoniczne może zostać uznane przez osoby zgłaszające za bezpieczniejsze. Dlatego jako drugi kanał raportowania oferowana jest opcja telefonu.<br>6. Punkt 6 powyżej: art. 6 ust. 1 f) Rozporządzenia. W interesie Administratorów jest zdobywanie wiedzy o zdarzeniach związanych z przestrzeganiem przepisów w organizacji i powstrzymywanie wszelkich niewłaściwych/nielegalnych zachowań. Podstawą prawną takiego przetwarzania treści zgłoszonego zdarzenia może być także art. 88 RODO w związku z ewentualnymi lokalnymi przepisami o ochronie danych.<br>7. Punkt 7 powyżej: art. 6 ust. 1 f) Rozporządzenia. W interesie Administratorów leży udokumentowanie śledztwa w celu wykazania jego prawidłowości. |

| | |
|---|---|
| | 8. Punkt 8 powyżej: art. 6 ust. 1 f) Rozporządzenia. W interesie Administratorów leży zidentyfikowanie działań i środków oraz naprawienie sytuacji niezgodnej z przepisami.<br>9. Punkt 9 powyżej: art. 6 ust. 1 f) Rozporządzenia. W interesie Administratorów leży analiza przypadków do celów statystycznych i zgłaszanie przypadków braku zgodności odpowiedniemu kierownictwu w pseudonimizowanej formie, aby można było zoptymalizować operacje biznesowe, a kierownictwo mogło wywiązać się ze swoich obowiązków w celu zapewnienia skutecznego systemu zgodności. |
| Odbiorca lub kategorie odbiorców danych osobowych | Państwa dane osobowe będą dostępne dla:<br>- Administratorów,<br>- zewnętrznych dostawców usług, m.in. People InTouch B.V.,<br>- w zależności od przypadku: prawników zewnętrznych, władz (np. policji, prokuratury, sądu) lub organów administracyjnych lub organy nadzorczych (np. urząd ochrony danych osobowych, urząd antymonopolowy) |
| Konieczność gromadzenia danych | Administratorzy są prawnie zobowiązani do wdrożenia skutecznego zarządzania i kontroli zgodności. |
| Miejsce przetwarzania i transfer do krajów trzecich | Technicznie rzecz biorąc, dane przetwarzane są na platformie hostowanej przez zewnętrznego usługodawcę z siedzibą w Holandii.<br>Dane będą przetwarzane także w Niemczech, w kraju, w którym znajduje się osoba zgłaszająca zdarzenie oraz w każdym kraju, którego dotyczy zgłoszone zdarzenie.<br>Dane należy w razie potrzeby przekazać także władzom (zagranicznym), o ile opiera się to na podstawie prawnej.<br>W związku z tym wyżej wymienieni odbiorcy mogą mieć także siedzibę w krajach spoza Europejskiego Obszaru Gospodarczego ("kraje trzecie"). W krajach trzecich poziom ochrony danych może nie być gwarantowany w takim samym stopniu jak w Europejskim Obszarze Gospodarczym. W przypadku przekazywania danych do państwa trzeciego Administratorzy zadbają o to, aby ich przekazanie odbyło się wyłącznie zgodnie z przepisami prawa (Rozdział V RODO). |
| Okres przechowywania danych osobowych | - Nagranie głosu jest usuwane przez usługodawcę People Intouch po upływie 24 godzin od otrzymania przez Administratorów transkrypcji w Systemie Zarządzania Zgłoszeniami (dalej "CMS"). Jest przechowywane przez 5 dni w systemie zapasowym.<br>- Dane sprawy w Systemie SpeakUp (systemie, w którym Administratorzy komunikują się ze zgłaszającym zdarzenie oraz części systemu, do której dostęp mają wyłącznie Administratorzy) są anonimizowane przez People Intouch po 14 dniach od zamknięcia sprawy.<br>- Dane spraw w module CMS przechowywane są przez 3 lata od zakończenia sprawy.<br>- W pojedynczych przypadkach dane są przechowywane przez dłuższy okres, w przypadku gdy Administrator ma prawnie uzasadniony interes do przechowywania danych przez okres dłuższy niż wskazany powyżej (np. obrona lub dochodzenie roszczeń prawnych). |

**2. Państwa prawa jako osób, których dane dotyczą**

Jako osoby, których dane dotyczą, mogą Państwo w każdej chwili skontaktować się z którymkolwiek z Administratorów, w szczególności z inspektorem ochrony danych Grupy Heidelberg Materials, wysyłając nieformalną wiadomość pod podanymi powyżej danymi kontaktowymi, w celu realizacji swoich praw zgodnie z RODO. Każdy Administrator poinformuje drugiego Administratora o skorzystaniu przez osobę, której dane dotyczą, z praw oraz przekaże temu drugiemu Administratorowi wszelkie niezbędne informacje. W przypadku, gdy złożą Państwo wniosek o dostęp zgodnie z art. 15 RODO, Administrator, któremu przypisano zdarzenie, przekaże wymagane informacje.

Państwa prawa są następujące:

- prawo do uzyskania informacji o przetwarzanych danych, a także kopię przetwarzanych danych (prawo dostępu, art. 15 Rozporządzenia);
- prawo do żądania sprostowania niedokładnych danych lub uzupełnienia niekompletnych danych (prawo do sprostowania, art. 16 Rozporządzenia);
- prawo do żądania usunięcia danych osobowych oraz w przypadku podania do wiadomości publicznej danych osobowych, informacji dla innych administratorów o żądaniu usunięcia (prawo do usunięcia, art. 17 Rozporządzenia);
- prawo do żądania ograniczenia przetwarzania (prawo do ograniczenia przetwarzania, art. 18 Rozporządzenia);
- prawo – w przypadku spełnienia warunków określonych w art. 20 Rozporządzenia – do otrzymania danych osobowych dotyczących użytkownika w ustrukturyzowanym, powszechnie używanym i nadanym maszynowo formacie oraz prawo do przekazania tych danych innemu administratorowi w celu ich przetwarzania (prawo do przenoszenia danych, art. 20 Rozporządzenia);
- prawo, ze względu na Państwa szczególną sytuację, do wniesienia sprzeciwu w dowolnym momencie do przetwarzania danych osobowych dotyczących Państwa, które opiera się na art. 6 ust. 1 f) Rozporządzenia, ze skutkiem na przyszłość (prawo do sprzeciwu, art. 21 Rozporządzenia); w takim przypadku administrator nie przetwarza już Państwa danych osobowych, chyba że administrator wykaże istotne uzasadnione podstawy przetwarzania, które przeważają nad Państwa interesami, prawami i wolnościami, lub do ustalenia, wykonania lub obrony roszczeń prawnych;
- prawo do cofnięcia zgody w dowolnym momencie, aby zapobiec przetwarzaniu danych, które jest oparte na Państwa zgodzie. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (prawo do odstąpienia, art. 7 ust. 3. Rozporządzenia);
- prawo do wniesienia skargi do organu nadzorczego zgodnie z art. 77 Rozporządzenia, na podstawie którego bez uszczerbku dla innego administracyjnego lub sądowego środka ochrony prawnej, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, złożycie Państwo skargę, jeżeli uznacie, że przetwarzanie danych osobowych dotyczące Państwa naruszają Rozporządzenia: Prezes Urzędu Ochrony Danych Osobowych z siedzibą w Warszawie przy ul. Stawki 2, 00-193 Warszawa