Policy sulla protezione dei Dati Personali

Gruppo HeidelbergCement

Ambito di applicazione:	HeidelbergCement AG e tutte le società controllate direttamente o indirettamente da HeidelbergCement AG nell'Unione Europea (EU) o nello Spazio Economico Europeo (SEE) e le società al di fuori di UE/SEE se rispettano i criteri della presente Politica
Autore:	Direzione Legale di Gruppo
Pubblicazione:	18 maggio 2018

HEIDELBERGCEMENT

INDICE

§ 1 Significato, obiettivo 3
§ 2 Ambito di applicazione 3
§ 3 Definizioni 3
§ 4 Organizzazione per la protezione dei Dati Personali 4
§ 5 Trattamento dei Dati Personali 5
§ 6 Categorie particolari di Dati Personali 6
§ 7 Trasmissione/inoltro dei Dati Personali 6
§ 8 Fornitori di servizi esterni 7
§ 9 Evitare e minimizzare i Dati; protezione dei Dati fin dalla progettazione e in caso di default 7
§ 10 Diritti degli Interessati 8
§ 11 Richieste di informazione di terzi relative agli Interessati 8
§ 12 Registrazione delle attività di Trattamento 9
§ 13 Segretezza dei Dati 9
§ 14 Reclami 9
§ 15 Verifiche 9
§ 16 Indagini interne 10
§ 17 Violazioni della protezione dei Dati 10
§ 18 Conseguenze delle violazioni 10
§ 19 Contatti 10

§ 1 Significato, obiettivo

(1) La presente Politica stabilisce regole obbligatorie per la tutela dei Dati Personali in conformità alla legge.

(2) I diritti delle persone fisiche concernenti i loro Dati Personali devono essere salvaguardati e protetti attraverso la presente Policy.

§ 2 Ambito di applicazione

(1) La Politica si applica a:

(i) tutte le società del Gruppo HeidelbergCement che hanno sede all'interno dell'Unione Europea /SEE, ossia a HeidelbergCement AG e a tutte le società del gruppo che dipendono da essa, e alle società affiliate nella misura in cui abbiano la sede all'interno dell'Unione Europea /SEE. Società "che dipende" significa che HeidelbergCement AG possiede direttamente o indirettamente la maggioranza dei diritti di voto o nel management della società;

(ii) tutte le società del Gruppo HeidelbergCement che hanno sede al di fuori dell'Unione Europea/SEE ma offrono beni o servizi a persone situate nell'Unione Europea /SEE; oppure

(iii) al comportamento delle persone interessate, nella misura in cui il comportamento di tali persone si svolga nell'Unione Europea / SEE.

(2) La Politica si applica anche a tutti i dipendenti delle predette società.

(3) I requisiti e i divieti stabiliti dalla presente Policy si applicano alla gestione di tutti i Dati Personali, indipendentemente dal fatto che essa sia effettuata elettronicamente o in forma cartacea. Si applicano anche a tutte le tipologie di parti interessate (clienti, dipendenti, fornitori, ecc.).

§ 3 Definizioni

(1) Ai fini della presente Politica valgono le definizioni del Regolamento UE 2016/679 (Regolamento Generale sulla Protezione dei Dati). In particolare

(a) "Dati Personali": qualsiasi informazione riguardante una persona fisica identificata o identificabile ("Interessato"); o attraverso cui una persona fisica può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di codice, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

(b) "Trattamento": qualsiasi operazione o insieme di operazioni concernente Dati Personali, compiute con o senza l'ausilio di processi automatizzati, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma

messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione. I termini "Trattamento" e "trattato" saranno interpretati in base a questa definizione.

c) "Titolare del Trattamento": la persona fisica o giuridica, l'autorità pubblica, o altro organo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del Trattamento dei Dati Personali; se le finalità e i mezzi di tale Trattamento sono determinati dal diritto dell'Unione o degli Stati membri, l'identità del Titolare del Trattamento può essere stabilita in base ai criteri rilevanti in base al diritto dell'Unione o degli Stati membri,

ovverosia, il Titolare del Trattamento è la persona giuridica all'interno del gruppo, comprese tutte le articolazioni interne e le filiali dipendenti che raccoglie, tratta o usa i Dati Personali per se stesso oppure ordina che ciò sia compiuto da altri. L'identità del Titolare del Trattamento viene decisa di volta in volta in base a chi stabilisce finalità e mezzi del Trattamento dei Dati Personali.

(d) "Responsabile del Trattamento" è la persona fisica o giuridica, l'autorità pubblica, o altro organo che tratta Dati Personali per conto del Titolare del Trattamento.

(e) "Terzo" è la persona fisica o giuridica, l'autorità pubblica, o altro organo che non sia l'Interessato, il Titolare del Trattamento, il Responsabile del Trattamento e le persone autorizzate al Trattamento dei Dati Personali sotto l'autorità diretta del Titolare o del Responsabile.

Un terzo è quindi ogni persona od organo che non sia il Titolare del Trattamento, pertanto può essere anche un'altra entità giuridica appartenente al gruppo.

§ 4 Organizzazione per la protezione dei Dati Personali

(1) Il Consiglio d'Amministrazione e il management delle società del gruppo sono tenuti ad assicurare la protezione dei Dati Personali nell'ambito delle loro responsabilità. Sono obbligati a garantire il rispetto dei requisiti legali relativi alla protezione dei dati e di quelli contenuti nella presente Politica.

(2) HeidelbergCement AG ha nominato un Responsabile di gruppo per le protezione dei Dati Personali (il "Responsabile di Gruppo della Protezione dei Dati"). Il Responsabile di Gruppo della Protezione dei Dati svolgerà i suoi compiti in modo indipendente, senza ricevere ordini/istruzioni e applicando la propria competenza specialistica. Riferirà al Consiglio di Amministrazione di HeidelbergCement AG. Il Responsabile di Gruppo della Protezione dei Dati verificherà il rispetto della presente Politica. Ha la responsabilità di sviluppare e aggiornare le politiche per la protezione dei dati del gruppo.

(3) Ciascun Consiglio di Amministrazione e gruppo dirigente delle società deve nominare un Coordinatore per la Protezione dei Dati, che collaborerà con il Responsabile di Gruppo della Protezione dei Dati e avrà la responsabilità del rispetto delle leggi sulla protezione dei dati nella relativa società del gruppo ("Coordinatore per la Protezione dei Dati"). Inoltre, se la legge lo richiede, la società del gruppo deve nominare un responsabile della protezione dei dati, il "Responsabile Aziendale della Protezione dei Dati" (in aggiunta alla nomina del Responsabile di Gruppo della Protezione dei Dati).

(4) Il monitoraggio delle regole sulla protezione dei dati e delle istruzioni interne del gruppo è responsabilità dei Responsabili Aziendali della Protezione dei Dati o dei Coordinatori per la Protezione dei Dati, i quali informeranno regolarmente il Responsabile di Gruppo della Protezione dei Dati sulla loro attività. Devono comunicare rischi particolari e/o significativi inerenti la protezione dei dati al Responsabile di Gruppo della Protezione dei Dati subito dopo esserne venuti a conoscenza.

(5) I Consigli di Amministrazione e il gruppo dirigente delle società del gruppo devono coadiuvare il Responsabile di Gruppo della Protezione dei Dati e i Coordinatori per la Protezione dei Dati/Responsabili Aziendali della Protezione dei Dati nelle loro attività. I responsabili dei progetti e dei processi aziendali devono comunicare per tempo al Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati eventuali nuovi Trattamenti di Dati Personali prima dell'inizio del Trattamento, per consentire una valutazione e identificazione di eventuali rischi associati al nuovo Trattamento e per adottare adeguati strumenti di controllo, se necessari.

(6) I Coordinatori per la Protezione dei Dati/Responsabili Aziendali della Protezione dei Dati dovranno assicurare che i dipendenti della relativa società del gruppo ricevano una formazione adeguata in relazione agli obblighi giuridici relativi alla protezione dei dati e quelli contenuti nella presente Politica. Il Responsabile di Gruppo della Protezione dei Dati dovrà mettere a disposizione i materiali formativi (per esempio, corsi di e-Learning) e fornirà supporto e consulenza al Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati.

§ 5 Trattamento dei Dati Personali

(1) In linea di principio, il Trattamento dei Dati Personali è vietato a meno che esista una base legale per detto Trattamento. I Dati Personali possono essere legittimamente trattati per i seguenti motivi:

- Se il Trattamento è necessario all'esecuzione di un contratto di cui l'Interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso.
- Se e nella misura in cui l'Interessato presti il proprio consenso (è necessaria una qualche forma di consenso espresso poiché il silenzio, le caselle precompilate o l'inattività non rappresentano un consenso. Il consenso deve essere altresì verificabile, ovvero è necessario tenere una qualche forma di registro sul modi e tempi del suo ottenimento.
- Se una disposizione di legge richiede o permette il Trattamento.
- In caso di altri elementi oggettivi che lo permettono, ad esempio se necessario per la salvaguardia degli interessi vitali dell'Interessato.
- Se il Trattamento è necessario per il perseguimento del legittimo interesse del Titolare del Trattamento, eccetto il caso in cui i diritti dell'Interessato prevalgano su tale interesse legittimo.

(2) I Dati Personali possono essere trattati esclusivamente per uno scopo determinato in precedenza e di conseguenza possono essere utilizzati e inoltrati solo nella misura in cui ciò sia compatibile con lo scopo precedentemente determinato. Sono vietati la custodia (conservazione) e qualsiasi forma di Trattamento dei Dati Personali senza uno scopo specifico.

(3) Al momento della raccolta dei Dati Personali, è obbligatorio per legge comunicare all'Interessato quanto segue: la finalità prevista, la base legale del Trattamento, l'identità del Titolare del Trattamento, i contatti del Responsabile Aziendale della Protezione dei Dati/Coordinatore per la Protezione dei Dati, le categorie di destinatari dei Dati Personali, il tempo di conservazione, i dettagli relativi a eventuali trasferimenti in altri Paesi e le necessarie protezioni, l'esistenza dei diritti dell'Interessato in relazione al Trattamento, come l'Interessato può obiettare, il diritto dell'Interessato di ritirare il consenso al Trattamento, il diritto a presentare reclamo presso l'Autorità di controllo, se il fornire i Dati personali fa parte di un requisito o di un obbligo giuridico o contrattuale e le possibili conseguenze della mancata comunicazione dei Dati Personali e se esiste un processo decisionale automatizzato in relazione ai Dati Personali, una volta ottenuti.

Si deve verificare con il Coordinatore per la Protezione dei Dati o il Responsabile Aziendale della Protezione dei Dati se esistono linee guida nazionali che devono essere tenute in considerazione al momento di ottenere e/o trattare i Dati Personali.

(4) I Dati Personali devono essere corretti e, se necessario, aggiornati. Devono anche essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. L'ambito del Trattamento deve essere necessario e pertinente rispetto allo scopo previsto. Le società del gruppo devono assicurare l'implementazione di adeguati processi interni. Anche i database devono essere controllati regolarmente per valutarne accuratezza, necessità e pertinenza e i risultati devono essere documentati. I Dati Personali devono essere conservati esclusivamente in una forma che consente l'identificazione degli Interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

(5) I Dati Personali devono essere trattati in maniera da garantirne la sicurezza, compresa la protezione, mediante misure tecniche e organizzative idonee, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali.

(6) Se possibile, ci si dovrebbe astenere dalla gestione dei Dati Personali. Sono preferibili Pseudonimi o un Trattamento in forma anonima.

§ 6 Categorie particolari di Dati Personali

In linea di principio, categorie particolari di Dati Personali come per esempio i dati relativi a origine razziale o etnica, opinioni politiche, convinzioni religiose o ideologiche, l'appartenenza sindacale e dati genetici, biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona possono essere raccolti e trattati esclusivamente con il consenso esplicito dell'Interessato o se ciò è permesso da un'autorizzazione di legge. Se si intendono trattare dati appartenenti a queste Categorie particolari, è necessario consultarsi in largo anticipo con il Coordinatore per la Protezione dei Dati o il Responsabile Aziendale della Protezione dei Dati per accertarsi dell'esistenza di una delle condizioni che ne permettono il trattamento.

§ 7 Trasmissione / inoltro dei Dati Personali

(1) La trasmissione dei Dati Personali a terzi che non rientrano nel capitolo 8 della presente Politica è permesso esclusivamente in base a un'autorizzazione di legge o se si è ottenuto in

anticipo il consenso dell'Interessato (si vedano le regole di cui al precedente capitolo 5, paragrafo (1) circa il significato di 'consenso') .

(2) Se il destinatario dei Dati Personali si trova al di fuori dell'Unione Europea o dello Spazio Economico Europeo sono necessarie misure particolari per proteggere diritti degli Interessati. Si deve evitare la trasmissione dei dati in assenza di adeguati standard di protezione adottati dal destinatario o se non è possibile determinarne lo standard (per esempio con un accordo o particolari clausole contrattuali, Privacy Shield).

§ 8 Fornitori di servizi esterni

(1) Il Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati deve essere informato in anticipo nel caso in cui i fornitori di servizi esterni devono avere accesso ai Dati Personali.

(2) I fornitori di servizi che possono accedere ai Dati Personali devono essere selezionati attentamente prima di effettuare un ordine. La selezione deve essere documentata e deve prendere in considerazione in particolare i seguenti aspetti:

- Idoneità del fornitore al gestire i Dati Personali
- Misure di sicurezza tecniche e organizzative per proteggere adeguatamente i Dati Personali, tra cui certificati di protezione dei dati, misure e linee guida di sicurezza informatica, conferma della durata della conservazione dei Dati Personali e relative misure di sicurezza.
- Esperienza del fornitore sul mercato
- Se il fornitore del servizio sottoscrive stipulare specifiche clausole contrattuali per documentare la natura del Trattamento e che impongono al fornitore del servizio obblighi adeguati di protezione dei Dati Personali,
- Altri aspetti, che consentono di dedurre l'affidabilità del fornitore (documentazione circa la protezione dei dati, disponibilità a collaborare, tempi di reazione, precedenti violazioni della protezione dei dati ecc.)

(3) Se un fornitore di servizi dovesse Trattare Dati Personali su ordine, è necessario un accordo sulla protezione dei dati prima che inizi il Trattamento, nel quale regolamentare gli aspetti relativi alla protezione dei dati e alla sicurezza informatica.

(4) Il fornitore di servizi deve essere regolarmente monitorato rispetto alle misure tecnico organizzative concordate ai sensi del contratto e il risultato delle verifiche deve essere registrato.

§ 9 Evitare e minimizzare i Dati; protezione dei Dati fin dalla progettazione e di default

(1) La gestione dei Dati Personali deve essere orientata alla finalità di trattare il minor numero possibile di Dati Personali dell'Interessato. I Dati Personali devono essere resi anonimi o pseudoanonimi, per quanto sia possibile in base all'uso previsto.

(2) Lo stesso vale per la selezione e la progettazione dei sistemi per il trattamento dei dati. La protezione dei dati deve essere inclusa fin dall'inizio nelle specifiche e nell'architettura dei sistemi

di trattamento dati, per facilitare il rispetto dei principi di protezione dei dati e della privacy definiti nel presente documento. I sistemi per il Trattamento dei dati non possono intervenire sui diritti degli Interessati attraverso impostazioni predefinite.

§ 10 Diritti degli Interessati

(1) Gli Interessati hanno diritto di essere informati sui Dati Personali conservati in azienda che li riguardano in quanto individui. Quando si ottengono dei Dati Personali, gli Interessati devono essere informati circa le questioni definite nel capitolo 5, paragrafo (3) della presente Politica.

(2) Quando si elaborano richieste di informazioni di un Interessato, la sua identità deve essere stabilita senza dubbi. Al riguardo, il Titolare deve richiedere una copia della carta d'identità o del passaporto personale dell'Interessato, da cui evincere nome, indirizzo e data di nascita. Saranno accettate solo copie della carta d'identità in forma cartacea, la scansione non è permessa. La copia della carta d'identità sarà poi distrutta senza indugio, in base alle norme sulla protezione dei dati, dopo che l'informazione è stata fornita.

(3) Quando si riceve da un Interessato la richiesta di fornire informazioni circa il Trattamento dei suoi Dati Personali, si deve rispondere all'Interessato per iscritto, specificando, oltre ai Dati Personali disponibili che lo riguardano, quali sono le finalità del Trattamento, le categorie dei dati trattati, i destinatari a cui sono stati comunicati i suoi Dati Personali, il tempo di conservazione, informazioni sul diritto alla rettifica o cancellazione dei Dati Personali, informazioni sull'esistenza del diritto di presentare reclamo presso l'autorità competente e informazioni sull'origine dei dati.

(4) I Coordinatori per la Protezione dei Dati/Responsabili Aziendali della Protezione dei Dati o il Responsabile di Gruppo della Protezione dei Dati saranno a disposizione per chiarimenti in caso di richieste di informazioni da parte degli Interessati.

(5) Devono essere rispettati i limiti di tempo stabiliti dalla legge per rispondere alle richieste degli Interessati; le informazioni devono essere fornite senza indugio entro un mese dalla richiesta. Tale periodo può essere esteso in caso di richieste complesse o numerose.

§ 11 Richieste di informazione di terzi relative agli Interessati

Se un terzo dovesse chiedere informazioni relative a soggetti Interessati, per esempio chiedere Dati Personali relativi a clienti o dipendenti di una società del gruppo, tali dati possono essere comunicati al terzo solo se

- il terzo che chiede l'informazione può dimostrare di avere un interesse legittimo al riguardo, e
- una disposizione di legge obbliga a fornire l'informazione, e
- l'identità del richiedente è stata stabilita senza alcun dubbio.

§ 12 Registrazione delle attività di Trattamento

(1) Ogni Titolare o Responsabile o il rispettivo Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati terrà, nel Paese sotto la propria responsabilità, un registro di tutte le attività di Trattamento. Si tratta di un requisito di legge.

(2) Il Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati dovrà predisporre una mappatura dei processi per il Trattamento dei Dati Personali (registro delle attività di Trattamento) e metterla a disposizione del Responsabile di Gruppo della Protezione dei Dati.

§ 13 Segretezza dei Dati

(1) Ai dipendenti è vietato raccogliere, trattare o utilizzare Dati Personali senza autorizzazione. Essi sono tenuti alla segretezza dei dati prima di iniziare l'attività, ovvero nel momento in cui entrano in un rapporto di lavoro con il Titolare. (2) Inoltre, i dipendenti con particolari obblighi di non divulgazione saranno obbligati a ciò per iscritto da parte del Consiglio di Amministrazione o del management della società.

§ 14 Reclami

(1) Ciascun Interessato ha diritto di obiettare al Trattamento dei propri Dati Personali se dovesse ritenere che i suoi diritti sono stati violati. I dipendenti possono comunicare in qualsiasi momento eventuali violazioni alla presente Politica.

(2) I soggetti responsabili per la gestione dei reclami sono il Coordinatore per la Protezione dei Dati/ Responsabile Aziendale della Protezione dei Dati o il Responsabile di Gruppo della Protezione dei Dati.

§ 15 Ispezioni

(1) Per garantire uno standard adeguato/corretto di protezione dei dati, i relativi processi saranno verificati con regolari ispezioni interne o esterne. Si devono adottare interventi correttivi diretti in caso siano scoperte violazioni della presente Politica o si identifichino aree di miglioramento.

(2) I risultati delle ispezioni devono essere documentati. La documentazione deve essere trasmessa al Responsabile di Gruppo della Protezione dei Dati, al Coordinatore per la Protezione dei Dati /Responsabile Aziendale della Protezione dei Dati, al Consiglio di Amministrazione o al management e al responsabile dei relativi processi.

(3) L'ispezione è completata con successo se tutte le misure documentate nella relazione sono state adottate. Se necessario, si effettueranno ispezioni successive per verificare l'adozione di tutti gli interventi correttivi stabiliti.

§ 16 Indagini interne

(1) Eventuali indagini interne per chiarire fatti e per evitare o rilevare reati penali o gravi violazioni degli obblighi nel rapporto di lavoro saranno svolte rispettando rigorosamente le norme di legge sulla protezione dei dati. In particolare, eventuali Dati Personali raccolti e usati per indagini interne devono essere necessari e rilevanti per il conseguimento della finalità dell'indagine e devono essere proporzionati ai diritti degli Interessati.

(2) Eventuali azioni correttive adottate rispetto al trattamento dei Dati Personali dell'Interessato devono essere comunicate al più presto.

(3) Per qualsiasi indagine interna, il Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati in questione deve essere coinvolto fin dall'inizio nella scelta e progettazione delle azioni correttive.

§ 17 Violazioni della protezione dei dati

(1) Se si dovessero comunicare illecitamente Dati Personali a terzi o se tali dati venissero persi durante il Trattamento da un'azienda del gruppo, il Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati in questione o il Responsabile di Gruppo della Protezione dei Dati devono essere informati senza indugio, in modo da poter rispettare i tempi di legge relativi agli obblighi di comunicazione in caso di violazioni della protezione dei dati all'autorità di controllo in questione (ossia entro 72 ore da quando l'azienda viene a conoscenza della violazione per qualsiasi evento comunicabile).

(2) Il report di una violazione deve contenere tutte le informazioni necessarie per chiarire i fatti, in particolare l'ente destinatario, le persone coinvolte e la tipologia ed entità dei Dati Personali trasmessi.

(3) Il Responsabile di Gruppo della Protezione dei Dati avrà la responsabilità esclusiva di assumere la decisione di informare gli Interessati o le autorità di controllo di qualsiasi violazione. Il Responsabile di Gruppo della Protezione dei Dati può delegare questo compito al Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati.

§ 18 Conseguenze delle violazioni

Una violazione della presente Politica può condurre ad azioni disciplinari in base alla legge sul lavoro applicabile, compresa la rescissione anticipata del rapporto. Possono altresì derivare sanzioni ai sensi del codice penale e del codice civile, come il risarcimento dei danni.

§ 19 Contatti

Il Responsabile di Gruppo della Protezione dei Dati può essere contattato a:

HeidelbergCement AG
Berliner Straße 6
69120 Heidelberg
E-mail: data.protection@heidelbergcement.com