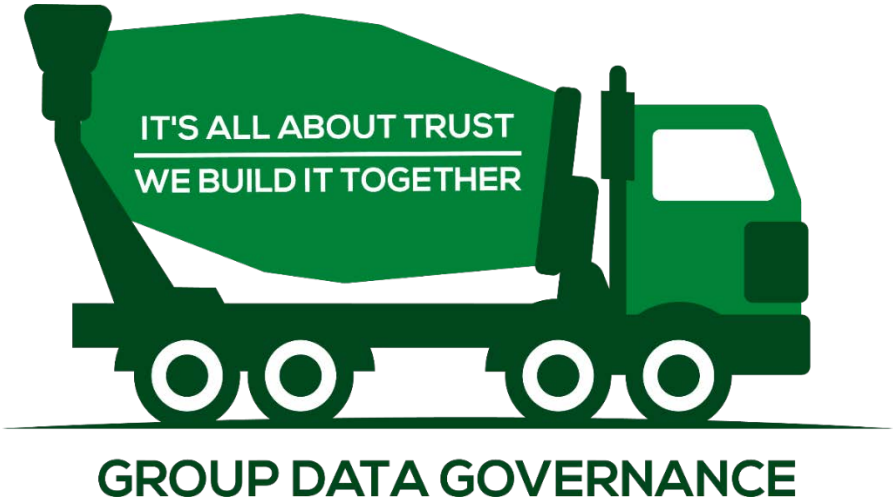
Politica quadro sulla protezione dei Dati Personali

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
Aggiornamento:	12 Febbraio 2021
Autore dell'aggiornamento:	Group Data Governance



INDICE

§ 1 Significato, obiettivo 3
§ 2 Ambito di applicazione 3
§ 3 Definizioni 4
§ 4 Organizzazione per la protezione dei Dati Personali 4
§ 5 Trattamento dei Dati Personali 5
§ 6 Categorie particolari di Dati Personali 7
§ 7 Trasmissione/inoltro dei Dati Personali 7
§ 8 Fornitori di servizi esterni 7
§ 9 Evitare e minimizzare i Dati; protezione dei Dati fin dalla progettazione e in caso di default 8
§ 10 Diritti degli Interessati 8
§ 11 Richieste di informazioni di terzi relative agli Interessati 8
§ 12 Registrazione delle attività di Trattamento 9
§ 13 Trattamenti nuovi o modificati …… 9
§ 14 Segretezza dei Dati 10
§ 15 Reclami e Violazioni dei Dati Personali 10
§ 16 Verifiche 11
§ 17 Indagini interne 11
§ 18 Formazione, Comunicazione e Reporting 11
§ 19 Contatti 11
Allegato A – Politica e Documento organizzativo….. 12
Allegato B – Categorie dei Dati di Heidelberg Cement … 15
Allegato C – Flusso di processo della Protezione dei Dati di Heidelberg Cement … 16

§ 1 Significato, obiettivo

(1) Come stabilito nel Codice di Comportamento di HeidelbergCement, HeidelbergCement mantiene standard elevati per proteggere i dati personali di dipendenti, clienti, fornitori e altre parti interessate. La Politica quadro sulla protezione dei dati e tutte le Linee guida che ne derivano dimostrano il rispetto dei diritti individuali e della privacy di tutti gli individui da cui HeidelbergCement riceve e tratta i Dati personali.

(2) La presente Politica quadro sulla protezione dei dati stabilisce le norme obbligatorie per una protezione sostenibile dei dati personali e in conformità alla legge. Inoltre, fornisce una panoramica delle norme sulla protezione dei dati implementate all'interno di HeidelbergCement a seguito dell''introduzione del Regolamento UE 2016/679, il Regolamento generale sulla protezione dei dati (di seguito: GDPR).

(3) L'obiettivo delle seguenti regole è garantire che i dati personali siano raccolti, archiviati, elaborati e salvaguardati in modo conforme alla legge.

§ 2 Ambito di applicazione

(1) Questa Politica quadro 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) Questa Politica quadro 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.).

(4) La presente Politica quadro sulla protezione dei dati è arricchita da numerose linee guida che delineano dettagli significativi relativi al sistema di gestione della protezione dei dati (di seguito "Linee guida"). Per maggiori dettagli si rinvia all'Allegato A – Organizzazione delle Policy e dei Documenti. I riferimenti alle Linee Guida migliorative si trovano di seguito.

(5) La presente Politica quadro e le linee guida migliorative sono obbligatorie per tutte le società con sede legale all'interno del SEE. Questi documenti implementano i requisiti minimi per la conformità alla protezione dei dati, pertanto, le politiche locali potrebbero introdurre standard più elevati. Tutte le società del Gruppo HeidelbergCement, con sede legale al di fuori del SEE, sono invitate a introdurre la Politica quadro sulla protezione dei dati e le Linee guida o misure simili nella loro area di responsabilità. Tuttavia, l'attuazione sarà su base volontaria.

§ 3 Definizioni

(1) Ai fini della presente Politica e delle Linee Guida applicative 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 Managing Board 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 e nelle sue Linee Guida applicative.

(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 Managing Board di HeidelbergCement AG.

(3) Il Responsabile di Gruppo della Protezione dei Dati verificherà il rispetto della presente Politica, delle sue linee guida attuative e delle legislazioni applicabili. Ha la responsabilità di sviluppare e aggiornare le Politiche e le LInee Guida attuative per la protezione dei dati del Gruppo.

(4) Il Managing Board e il management delle società locali devono 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").

(5) 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".

(6) Il Managing Board 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.

(7) Per ulteriori dettagli si faccia riferimento alle "Linee Guida: Organizzazione e Responsabilità della Funzione Group Data Governance"

§ 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:

(a) 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.
(b) 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 sui modi e tempi del suo ottenimento.
(c) 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.
(d) 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:

(a) la finalità prevista,
(b) la base legale del Trattamento,
(c) l'identità del Titolare del Trattamento,
(d) i contatti del Responsabile Aziendale della Protezione dei Dati/Coordinatore per la Protezione dei Dati,
(e) le categorie di destinatari dei Dati Personali,
(f) il tempo di conservazione,
(g) i dettagli relativi a eventuali trasferimenti in altri Paesi e le necessarie protezioni,
(h) l'esistenza dei diritti dell'Interessato in relazione al Trattamento,
(i) come l'Interessato può obiettare,
(j) il diritto dell'Interessato di ritirare il consenso al Trattamento,
(k) il diritto a presentare reclamo presso l'Autorità di controllo,

Il Coordinatore per la Protezione dei Dati o il Responsabile Aziendale della Protezione dei Dati deve assicurare che siano implementati e rispettati eventuali ulteriori requisiti di legge.

(4) I Dati Personali devono essere corretti e, se necessario, aggiornati. Devono anche essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità. E' responsabilità del "Process Owner" dimostrare di essersi conformato a questi principi

(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. 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

(1) 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.

(2) Se si intendono trattare dati appartenenti a queste Categorie particolari, è necessario consultarsi preventivamente con il Coordinatore per la Protezione dei Dati o il Responsabile Aziendale della Protezione dei Dati.

(3) Si prega di leggere l'Allegato B – Categorie di Dati di Heidelberg Cement per maggiori dettagli.

§ 7 Trasmissione / inoltro dei Dati Personali

(1) La trasmissione dei Dati Personali a terzi è permesso esclusivamente in base a un'autorizzazione di legge o se si è ottenuto in anticipo il consenso dell'Interessato.

(2) L'accesso (da remoto) ai Dati Personali è egualmente trattato in modo lecito come il trasferimento dei Dati Personali a un ambiente IT separato

(3) 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 e ulteriori misure tecnico-organizzative stabilite contrattualmente).

§ 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:

– Il fornitore ha implementato 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.

- Disponibilità del fornitore a sottoscrivere 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)

(3) Se Heidelberg Cement decidesse di servirsi di un fornitore per trattare Dati Personali, è necessario sottoscrivere un accordo sulla protezione dei dati prima che inizi il Trattamento.

(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 pseudo-anonimi, per quanto sia possibile in base all'uso previsto.

(2) Lo stesso vale per la selezione e la progettazione dei sistemi informatici 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 la tutela dei dati personali "by design and default" .

§ 10 Diritti degli Interessati

(1) Gli Interessati hanno diritto di richiedere informazioni sui loro Dati Personali acquisiti, conservati e trattati in azienda.

(2) Quando si elaborano richieste di informazioni di un Interessato, la sua identità deve essere stabilita senza dubbi.

(3) Per ulteriori dettagli si rinvia alle Linee-Guida: "Richieste dei Soggetti Interessati".

§ 11 Richieste di informazioni 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

(a) l'identità del richiedente è stata stabilita senza alcun dubbio;
(b) una disposizione di legge obbliga a fornire l'informazione,
(c) il terzo che chiede l'informazione può dimostrare di avere un interesse legittimo al riguardo e
(d) fintanto che la richiesta non confligga con i diritti e le libertà dei Soggetti Interessati o altri requisiti legali o obbligazioni del Gruppo HeidelbergCement

§ 12 Registrazione delle attività di Trattamento

(1) L'introduzione di registri delle attività di trattamento per ciascuna società è obbligatoria per legge. È responsabilità del Titolare del trattamento introdurre ciascun trattamento nei registri delle attività di trattamento. A livello di Gruppo il DPO di Gruppo e a livello nazionale ciascun Coordinatore dei Dati Personali locale supporta i Process Owner in questo compito ed è responsabile del mantenimento generale dei registri aziendali.

(2) Il contenuto obbligatorio dei registri delle attività di trattamento deve contenere le seguenti informazioni:

(a) il nome e i dati di contatto del Titolare/Contitolare del trattamento, del rappresentante del Titolare e del Responsabile della protezione dei dati;
(b) le finalità del trattamento;
(c) una descrizione delle categorie di Interessati e delle categorie di Dati Personali;
(d) le categorie di destinatari a cui i Dati Personali sono stati o saranno trasmessi; trasferimenti di Dati Personali verso un paese terzo o un'organizzazione internazionale al di fuori del SEE e la documentazione delle garanzie adeguate;
(e) i termini temporali previsti per la cancellazione delle diverse categorie di Dati Personali;
(f) una descrizione generale delle misure di sicurezza tecniche e organizzative.

(3) 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. Dovrà altresì assicurare che sia rispettato ed eseguito ogni specifico regolamento o legge nazionale.

(4) Ciascuna azienda deve conservare i registri delle attività di trattamento indipendentemente dal suo ruolo nel trattamento, ad es. in qualità di Titolare del trattamento o di Responsabile del trattamento.

§ 13 Trattamenti nuovi o modificati

(1) Il rispettivo Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati o il DPO di gruppo sarà preventivamente coinvolto in ogni nuovo trattamento. Il Titolare del Processo è responsabile della corretta consultazione con il DPO di Gruppo e Locale. Per maggiori dettagli fare riferimento all'Allegato C – Flusso di lavoro del processo di protezione dei dati di HeidelbergCement.

(2) Se è prevista un'implementazione internazionale del trattamento o del progetto, deve essere coinvolto il DPO del Gruppo.

(3) L'obiettivo dei requisiti di protezione dei dati dipende dal trattamento specifico. Il rispettivo Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati locale o il DPO di gruppo valuta e comunica i requisiti per il trattamento al titolare del processo responsabile e ad altri soggetti interessati.

(4) Il rispettivo Coordinatore per la Protezione dei Dati/Responsabile Aziendale della Protezione dei Dati locale o il DPO di gruppo comunica se è necessaria una valutazione di impatto sulla protezione dei dati (di seguito: DPIA) per il trattamento specifico. La DPIA è un processo volto a identificare e ridurre al minimo i rischi per la protezione dei dati di un'attività di trattamento che potrebbe esporre gli Interessati a rischi elevati. Il Titolare del Processo è responsabile di avviare ed eseguire la DPIA con il supporto del rispettivo DPC Locale o del DPO di Gruppo.

(5) Per ulteriori dettagli sulla valutazione dei rischi per i diritti e le libertà degli interessati derivanti dal trattamento dei dati personali, si prega di fare riferimento alla “Linea guida: valutazione dell’impatto sulla protezione dei dati” e al modello “Matrice dei rischi sulla protezione dei dati”.

§ 14 Segretezza dei Dati

(1) E’ vietato raccogliere, trattare o utilizzare Dati Personali senza autorizzazione. Prima di iniziare l’attività di trattamento, i dipendenti sono vincolati alla regola della “necessità di conoscere” e dell’“obbligo di segretezza.

(2) Inoltre, i dipendenti con particolari obblighi di non divulgazione saranno obbligati a sottoscrivere uno specifico impegno.

§ 15 Reclami e violazioni dei Dati Personali

(1) Ciascun Interessato ha diritto di obiettare al Trattamento dei propri Dati Personali se dovesse ritenere che i suoi diritti sono stati violati.

(2) Inoltre, i dipendenti possono comunicare in qualsiasi momento eventuali violazioni alla presente Politica quadro, anche se la violazione non riguarda i suoi Dati Personali.

(3) In caso di incidenti relativi ai dati, il Coordinatore per la Protezione dei Dati/ Responsabile Aziendale della Protezione dei Dati e il DPO di Gruppo devono essere informati senza indugio, per garantire che la segnalazione all'autorità di controllo avvenga nelle 72 ore.

(4) Qualsiasi violazione della protezione dei dati di un dipendente può portare ad azioni disciplinari ai sensi del diritto del lavoro, inclusa, nel peggiore dei casi, la risoluzione del contratto di lavoro. Sono possibili anche sanzioni penali e conseguenze civili, come ad esempio il risarcimento dei danni.

(5) I soggetti responsabili per la gestione dei reclami e gestione degli incidenti (violazioni) sono il Coordinatore per la Protezione dei Dati/ Responsabile Aziendale della Protezione dei Dati o il Responsabile di Gruppo della Protezione dei Dati.

(6) Per ulteriori dettagli si rimanda alla “Linea guida: gestione degli incidenti relativi ai dati personali”.

§ 16 Verifiche

(1) Per garantire uno standard adeguato/corretto di protezione dei dati in accordo con le leggi applicabili, 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 quadro e delle sue Linee Guida attuative 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 Managing Board o al management locale e al responsabile dei relativi processi.

§ 17 Indagini interne

(1) Eventuali indagini interne (ad ese. 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, la presente Politica quadro e le sue Linee Guida attuative. 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) 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.

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

§ 18 Formazione, Comunicazione e Reportistica

(1) La Funzione di Gruppo Data Governance è responsabile della sensibilizzazione sulle questioni relative alla protezione dei dati all'interno del Gruppo HeidelbergCement attraverso la progettazione, l'implementazione e il mantenimento di misure regolari di formazione e comunicazione. Queste misure possono differire nella portata, ad es. solo per gruppi di stakeholder selezionati e forma, ad es. e-learning, formazione in presenza, formazione virtuale, opuscoli informativi.

(2) Ciascun DPO locale è responsabile di implementare le misure del Gruppo a livello locale e di introdurre eventuali ulteriori misure di formazione e comunicazione a livello locale, se necessario.

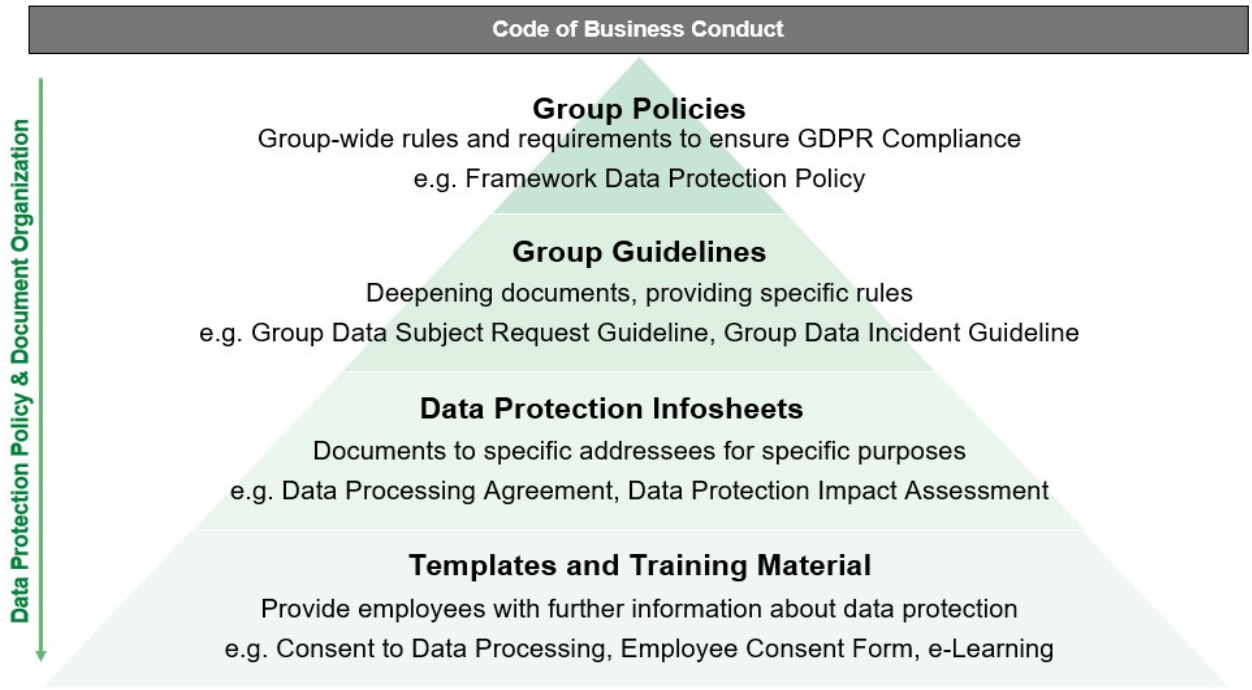
(3) Il DPO locale è obbligato a riferire frequentemente alla propria direzione locale e al DPO del gruppo. Si prega di fare riferimento alle "Linee guida: Reporting per Paese".

§ 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

Allegato A - Politica e Documenti Organizzativi



Introduzione

(1) Questi principi specificano le regole fondamentali relative all'organizzazione dei documenti sulla protezione dei dati come stabilito nel § 2 (4).

(2) Il Sistema di Gestione della Protezione dei Dati (di seguito: DPMS) di HeidelbergCement si basa sulla logica stabilita dal Codice di Comportamento Aziendale di HeidelbergCement. Qui si afferma che HeidelbergCement mantiene standard elevati per proteggere i dati personali di dipendenti, clienti, fornitori e altre parti interessate. Inoltre, tutti i dipendenti hanno l'obbligo generale di rispettare i requisiti di protezione dei dati e di sicurezza delle informazioni.

(4) Tale obbligo generale si inquadra all'interno dei quattro livelli della Politica e Organizzazione dei Documenti del DPMS che sono di seguito descritti.

Descrizione della Politica e Organizzazione dei Documenti

(1) La Politica e l'Organizzazione dei Documenti si compone di quattro Livelli:

(a) A un primo livello, le Politiche del Gruppo affrontano regole e requisiti di base a livello di gruppo per garantire la conformità al GDPR, ad es. la Politica quadro sulla Protezione dei Dati.

L'obiettivo è definire un insieme di regole generali, che è soggetto a ulteriore concretizzazione tramite Linee Guida e altri documenti ai livelli successivi.

La comunicazione e la traduzione nella lingua locale nonché l'attuazione delle presenti norme generali sono obbligatorie in tutto il Gruppo sono di responsabilità del Coordinatore locale per la protezione dei dati (di seguito: DPO locale).

(b) Ad un secondo livello, le Linee Guida di Gruppo affrontano questioni fondamentali selezionate del GDPR, che mirano a evidenziare l'importanza dell'implementazione di determinati processi e a fornire un approccio armonizzato per farlo.

La comunicazione e la traduzione nella lingua locale devono essere assicurate dal DPO locale. Le politiche locali che introducono standard più elevati rispetto alla Linea Guida di Gruppo possono valorizzare il documento impostato a livello locale.

(c) Le schede informative sulla protezione dei dati di terzo livello mirano a fornire indicazioni generali su argomenti specifici, ad es. informazioni sui requisiti di base di una valutazione d'impatto sulla protezione dei dati.

Le Schede informative possono essere fornite dal Group Data Governance ("GDG") o essere redatte a livello locale dal DPO locale. Le schede informative consentiranno alle unità aziendali interessate di seguire procedure definite e fornire liste di controllo per facilitare la conformità ai requisiti GDPR pertinenti.

La comunicazione e la traduzione nella lingua locale devono essere assicurate dal DPO locale.

(d) I modelli e il materiale di formazione al quarto livello completano la politica e l'organizzazione dei documenti fornendo informazioni aggiuntive specifiche alle parti interessate sugli argomenti relativi alla protezione dei dati che possono apparire ripetutamente nell'ambito della normale attività operativa.

La comunicazione e la traduzione nella lingua locale devono essere assicurate dal DPO locale.

(2) Una panoramica delle politiche e dei documenti attualmente esistenti, nonché informazioni sull'applicabilità, sono fornite nella Panoramica delle Politiche e delle Linee Guida:

Panoramica delle politiche e delle linee guida

La tabella seguente fornisce una panoramica di tutte le Politiche (Livello 1) e le Linee Guida (Livello 2) esistenti ordinate per rispettiva categoria.

Category	Policy	Policy Available	Guideline	Guideline Available
Data Protection Compliance	Framework Policy	✓		
Strategy & Governance	Framework Policy	✓	• GDG Organization & Responsibilities	✓
Risk Management	Framework Policy		• DPIA	✓
Guidelines & Controls			• Personal Data Retention • TOMs • Clean Desk Policy	✓ ✓ ✓
Culture & Support	Framework Policy	✓		
Monitoring & Reporting	Framework Policy		• Country Reporting	✓
Audit & Certification	Framework Policy	✓		
Incident Response	Framework Policy	✓	• Data Incident Handling • Data Subject Request	✓ ✓

(3) Applicabilità dei documenti di livello 2-4

Come stabilito dalla Politica quadro sulla Protezione dei Dati, l'implementazione di tutti i documenti di livello 2-4 è obbligatoria in tutti i paesi del SEE e volontaria per tutti gli altri paesi ed entità del Gruppo HeidelbergCement.

Allegato B – Categorie di Dati di HeidelbergCement

Data categories	Sub-categories	High risk categories
Personal master data	Name, birth data, age, private address, private email address, nationality, gender, private phone numbers, marital status, relatives' data, hobbies, personal preferences (e.g. food, travel), knowledge, driver license, car license plate, visa, tax card data, health insurance, social media accounts, health insurance number	Criminal records certificate, passport copies, racial origin, ethnic origin, biometric data (fingerprints, face recognition, eye recognition), religious beliefs, philosophical beliefs, (political) opinion, sexual orientation, social security number, legal case files, damages records, health data (esp. disabilities, sick notes, long-term diseases, allergies, health reports)
Special categories of data subject data	Specific role as shareholder, supervisory board member, managing board member or insider, shareholder number, number of shares, share class, type of ownership of shares, number of admission ticket, check digit, information about proposals, questions and nomination suggestions	Information about insider-qualification, information about legal and natural persons closely affiliated
Employment master data	CV, job applications, company car information, company car license plate, company car driving bans, remuneration, tariff data, personnel number, benefits, training record, qualifications, travel data, time sheets and recordings, shift plans, absence times, active directory (e.g. job title, business address, business phone number, email, org chart), employees insurances	Work accidents (Health & Safety), trade union membership, assessment test results, photo, video, video surveillance data, performance reviews, (former) employers' references, warnings, (suspected) compliance violations, sick notices, health checks, (suspected) substance abuse, vaccinations
Business contact details and contract data (third parties)	Job title, business address, business phone number, email, social media account, commercial register data, land register data, order, order history, order confirmation, delivery address, invoice address, delivery notices (paper and electronic), bids, offers, receipts, export documents, customs documents	Signatures
Financial data	Bank account data, deposit documents, tax data, invoices, payment orders, checks documents, donation receipts, capital forming payments, credit agency details	Credit card data, credit status, credit worthiness, attachment orders, bank vouchers and bank guarantees, bank statements, bank books, bill books
Communication data	Emails, attachments, SMS, iMessage and similar applications, Microsoft Teams (similar applications) messages and videos during calls/phone conferences (without recording), metadata, contents of emails and other communication, meeting protocols or file notes, customer content data (connected experiences)	Voice messages, call recordings, Microsoft Teams recordings
Digital protocol data	Location, geolocation, geofencing, physical access data, access permissions, car license plate, drivers' logbook, tool tracking, system tracking, user ID, username, IP address, timestamps, versioning of files, last login, consent tracking, digital calendar	Live GPS tracking, video surveillance data, toll data, cookies, pixel

Allegato C – Flusso di Processo della protezione dei dati di HeidelbergCement