

DEUTZ- Codice in materia di protezione dei dati personali

Versione 1/2023 | Dicembre 2023



PREFAZIONE

Il sistema di gestione della protezione dei dati (DPMS) per il Gruppo DEUTZ è stato istituito in conformità con gli standard generalmente accettati, il diritto applicabile e su base specifica dell'azienda a seconda della natura e dell'ambito delle attività commerciali e del tipo di dati personali trattati.

Di seguito, descriviamo gli elementi di base del nostro DPMS sulla base dello standard di audit IDW PS 980 e consideriamo IDW PH 9.860.1 (Audit di principi, procedure e misure ai sensi del Regolamento generale sulla protezione dei dati dell'UE (GDPR) e della Legge federale tedesca sulla protezione dei dati (BDSG)) come un elenco non esaustivo.

Il DPMS comprende tutte le misure specifiche per la protezione dei dati che vengono implementate nelle società del Gruppo per conformarsi alle leggi applicabili in materia di protezione dei dati nell'ambito materiale e geografico del "Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, e che abroga la direttiva 95/46/CE" (Regolamento generale sulla protezione dei dati - GDPR)".

L'organizzazione per la protezione dei dati è integrata nell'ambito di un sistema olistico di governance, rischio e conformità (GRC).

Il Consiglio di Amministrazione di DEUTZ nel dicembre 2023

Per motivi di migliore leggibilità, ci asteniamo dall'utilizzare un linguaggio specifico per genere nel seguito. In tutti i casi, tutti i generi sono affrontati allo stesso modo. La formulazione abbreviata è utilizzata esclusivamente per motivi editoriali e non implica alcun giudizio.

CONTENUTO

Prefazione	2
Contenuto	3
Circolo per la protezione dei dati.....	4
Cultura	4
Obiettivi	6
Organizzazione	6
Rischio	8
Programma	8
Comunicazione	10
Monitoraggio	11

CIRCOLO PER LA PROTEZIONE DEI DATI

I clienti, i partner commerciali e i dipendenti hanno il legittimo affidamento che i dati a noi affidati saranno trattati in modo confidenziale e solo per gli scopi previsti. Il presente DPMS si applica a DEUTZ AG e a tutte le partecipazioni di maggioranza associate che sono soggette all'ambito di applicazione territoriale del GDPR. Il suo scopo è quello di attuare i principi derivanti dal GDPR come definiti nella Politica di protezione dei dati di DEUTZ e in conformità con il ciclo normativo sulla protezione dei dati.



CULTURA

DEUTZ si impegna a rispettare il diritto fondamentale alla protezione dei dati. Questo diritto protegge ogni singola persona fisica dall'intrusione nella sua privacy attraverso un uso non necessario, arbitrario o sproporzionato dei dati personali. La salvaguardia di questo diritto fa parte della nostra identità aziendale.

In un'economia sempre più digitalizzata e basata sui dati, le nuove tecnologie per l'elaborazione dei dati portano naturalmente a una maggiore quantità di dati personali e a un loro uso più diversificato. Ciò consente a DEUTZ di diventare più orientata al cliente, innovativa, agile e completamente digitale nei suoi processi interni e nelle attività nei confronti

degli stakeholder. Allo stesso tempo, ciò comporta la sfida di proteggere la privacy delle persone interessate in modo adeguato. Il Gruppo DEUTZ ha quindi un interesse fondamentale nel garantire che le tecnologie innovative e i nuovi modelli di business siano conformi alle normative vigenti in materia di protezione dei dati. Con la crescente digitalizzazione, riteniamo quindi importante che DEUTZ riconosca espressamente la propria responsabilità in materia di dati anche nell'ambito delle sue attività commerciali. Il trattamento responsabile dei dati nell'interesse dei nostri partner commerciali, dei dipendenti e degli altri stakeholder rimarrà quindi uno dei nostri obiettivi in futuro e rafforzerà ulteriormente la fiducia in DEUTZ.

La definizione della strategia di protezione dei dati per soddisfare i requisiti di protezione dei dati ci aiuta a raggiungere questi obiettivi, su misura per le attività specifiche delle società del Gruppo. A tal fine è fondamentale un buon rapporto con tutti gli stakeholder (dipendenti, clienti, partner commerciali, fornitori, azionisti, ecc.). Qualsiasi violazione delle leggi sulla protezione dei dati comporta il rischio di danneggiare in modo permanente la nostra reputazione e può portare a danni considerevoli e gravi conseguenze per l'intero Gruppo DEUTZ. Inoltre, tali violazioni possono anche portare a sanzioni civili o penali per i dipendenti coinvolti.

In DEUTZ, la condotta etica e legalmente corretta è un principio fondamentale che è già espresso nel "Codice di condotta DEUTZ" e include naturalmente il rispetto della legge sulla protezione dei dati. Ciò è supportato dalla consapevolezza fondamentale di DEUTZ che il rispetto delle leggi applicabili ha sempre la precedenza sugli obiettivi aziendali in caso di conflitto.

Inoltre, la nostra "Politica sulla protezione dei dati" si basa sulla comprensione fondamentale che qualsiasi trattamento dei dati personali deve essere effettuato in conformità con le leggi applicabili in materia di protezione dei dati, in particolare il Regolamento generale sulla protezione dei dati (GDPR).

OBIETTIVI

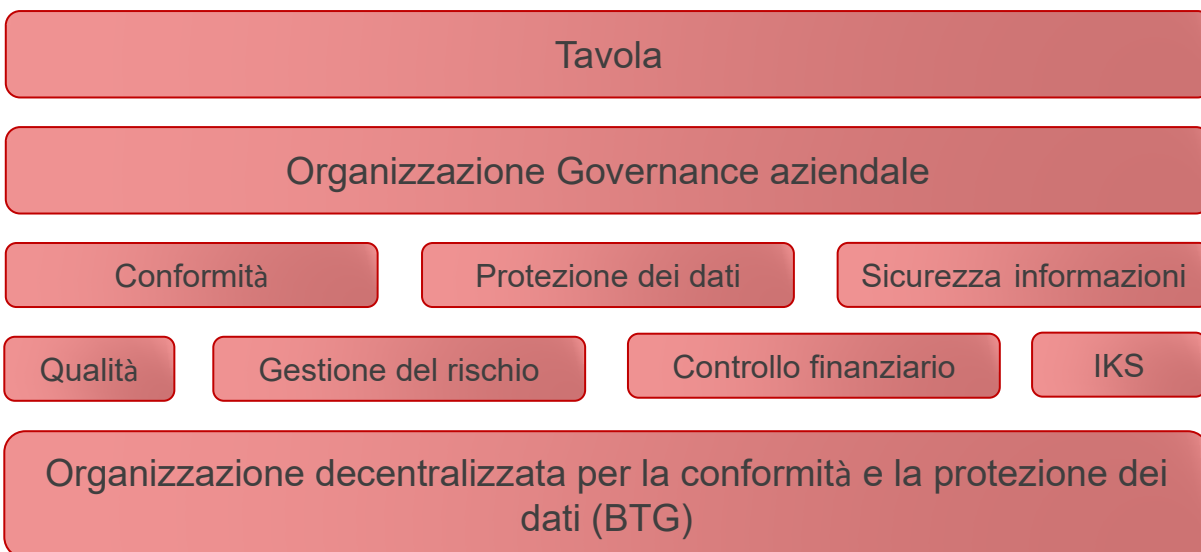
Gli obblighi legali derivanti dalle rispettive normative sulla protezione dei dati, in particolare il Regolamento generale sulla protezione dei dati (GDPR) e la Legge federale sulla protezione dei dati (BDSG), impongono requisiti complessi e rigorosi a coloro che trattano dati personali. Il nostro obiettivo è garantire che tutte le normative sulla protezione dei dati siano rispettate in tutto il Gruppo.

Ogni individuo in DEUTZ è responsabile del trattamento dei dati personali con la dovuta riservatezza e della loro protezione da abusi in modo che il trattamento di questi dati non violi i diritti personali di nessuno.

Tutti i dipendenti di DEUTZ tratteranno i dati personali dei nostri clienti, partner commerciali e dei loro colleghi con cura e riservatezza e rispetteranno la legge applicabile. Ogni persona all'interno del Gruppo DEUTZ che è responsabile di un'attività che coinvolge dati personali organizzerà il trattamento (raccolta, utilizzo, conservazione, cancellazione, ecc.) dei dati personali in modo tale da garantire il rispetto della legge applicabile. Trasferiamo queste aspettative anche ai nostri fornitori nel nostro "Codice di condotta per i fornitori".

ORGANIZZAZIONE

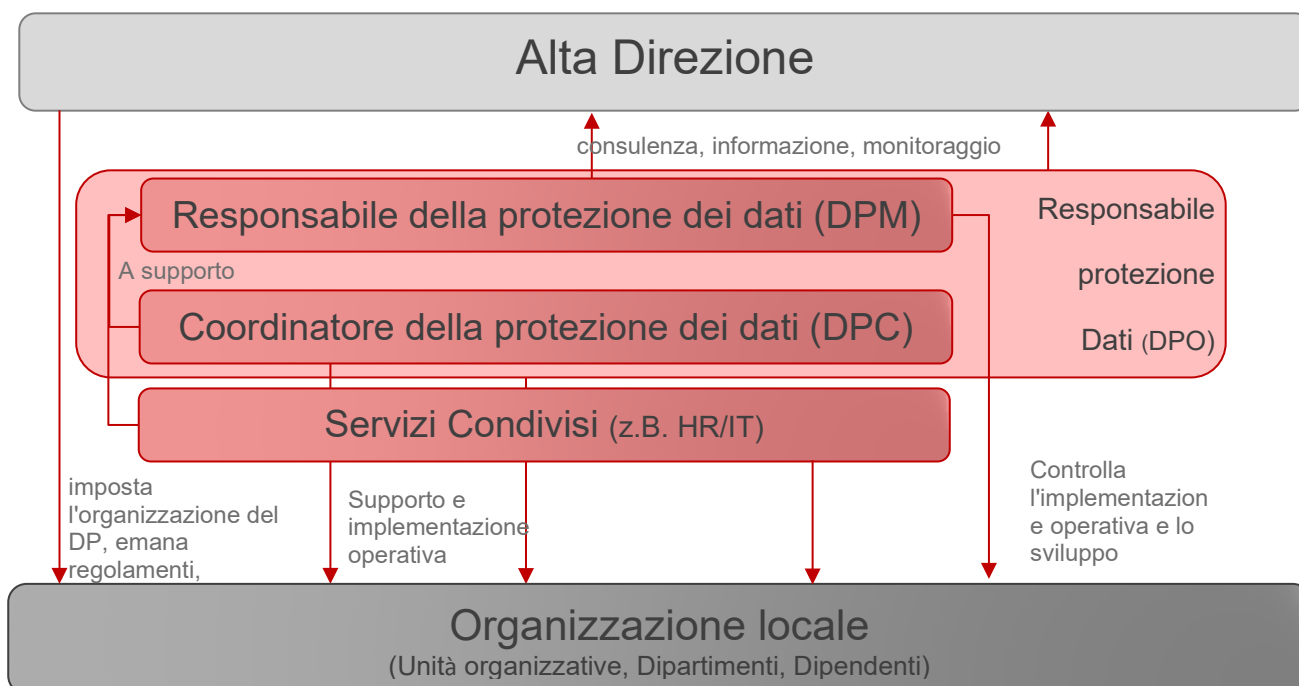
Il Gruppo DEUTZ è costituito da DEUTZ AG come società madre e da numerose società in cui DEUTZ AG detiene una partecipazione superiore al 50 per cento. Queste società associate (BTG) sono integrate nella struttura di governance centrale.



All'interno delle società affiliate, il rispetto dei requisiti in materia di protezione dei dati deve essere garantito a livello aziendale per ogni singolo trattamento di dati personali ("attività di trattamento"). Il Consiglio di Gestione ha la responsabilità generale del rispetto delle leggi applicabili e degli standard interni.

DEUTZ ha istituito un team interdisciplinare per la protezione dei dati che è responsabile della gestione e del monitoraggio dell'organizzazione per la protezione dei dati. Ove richiesto dalla legge, ciascuna società del Gruppo nomina un responsabile esperto della protezione dei dati (DPO) che svolge i compiti definiti dalla legge, in particolare la funzione di referente per gli interessati.

Per ogni divisione aziendale è stato inoltre nominato un Responsabile della protezione dei dati (DPM). Oltre ai doveri statuari di un DPO, i DPM sono responsabili del rispetto delle norme sulla protezione dei dati. La direzione delega al DPM l'adempimento dei propri obblighi in materia di protezione dei dati.



La protezione operativa dei dati (come garantire la liceità del trattamento dei dati; la gestione dei responsabili del trattamento; il rispetto dei processi interni di gestione della protezione dei dati, il monitoraggio, la preparazione di una documentazione idonea a dimostrare la conformità alla documentazione per dimostrare la conformità al GDPR, ecc.) è compito del Responsabile della protezione dei dati. Dispongono di conoscenze sufficienti e delle risorse necessarie per svolgere i loro compiti, nonché dell'autorità per modificare o sospendere il

trattamento dei dati. Group IT fornisce supporto nella definizione di misure tecniche e organizzative in conformità al GDPR e ad altri ordinamenti giuridici pertinenti e nell'implementazione di processi che garantiscano il rispetto dei principi di "privacy by design" nell'introduzione o nella modifica del trattamento dei dati personali. trattamento dei dati personali, i principi di privacy by design e privacy by default sono considerati "Privacy by Default".

RISCHIO

Nell'ambito di un approccio integrato di corporate governance, il Gruppo DEUTZ gestisce un sistema completo di gestione dei rischi a livello di Gruppo. All'interno di questo sistema vengono inoltre registrati e gestiti i principali rischi per la protezione dei dati. I rischi per la protezione dei dati sono valutati sia dal punto di vista della persona fisica interessata dal trattamento dei dati ("interessato") sia dal punto di vista dell'azienda. La valutazione del rischio risulta essenzialmente dalla categoria di dati trattati e dai mezzi utilizzati, dal rischio potenziale e dalla complessità del trattamento.

Il rischio di ogni singolo trattamento è valutato utilizzando una metodologia separata che considera sia le tipologie di dati trattati che il tipo specifico di trattamento. In questo modo è possibile determinare se il trattamento dei dati personali rappresenta un rischio solo perché i dati personali vengono trattati, se sono interessate categorie speciali di dati personali o se determinate categorie di dati e fattori di rischio indicano un aumento del rischio di un'attività di trattamento durante il trattamento.

PROGRAMMA

Il DPMS si basa su principi di Gruppo vincolanti a livello globale e su linee guida supplementari. Il fulcro del DPMS sono i "principi di elaborazione". L'obiettivo di questi è quello di creare standard organizzativi minimi e un quadro uniforme per il trattamento e la protezione dei dati personali all'interno del Gruppo e di prevenire danni a DEUTZ. Possono essere integrati da ulteriori linee guida che si applicano a specifici paesi o unità aziendali per garantire la piena conformità ai requisiti di protezione dei dati.

Il nostro programma di protezione dei dati comprende:

- Elaborazione degli ordini
- Diritti degli interessati
- Trasferimenti da paesi terzi

- Concetti di cancellazione
- Obblighi di comunicazione e notifica
- Misure tecniche e organizzative
- Registro delle attività di trattamento

Un "Piano di risposta agli incidenti", fornisce il quadro per l'identificazione efficace, la gestione interna e la segnalazione esterna delle violazioni dei dati. Le violazioni dei dati identificate nell'ambito di un'indagine, di processi di monitoraggio generale o in qualsiasi altro modo, devono essere segnalate immediatamente al DPM competente in conformità con i requisiti della Direttiva e nella forma ivi specificata. Il DPO informa il titolare del trattamento sull'eventuale necessità di una notifica alle autorità di protezione dei dati e/o agli interessati dalla violazione e, in caso affermativo, emette la notifica.

La nostra "Linee guida sulla protezione dei dati" obbliga ogni azienda del Gruppo a tenere un registro delle attività di trattamento pertinenti (registro dei trattamenti) e ad attuare un processo per tenere conto delle modifiche e garantire l'accuratezza e la completezza delle attività di trattamento. DEUTZ utilizza un software di gestione della protezione dei dati per gestire tali attività relative alla protezione dei dati.

Per ogni singola attività di trattamento, è necessario assicurarsi che il trattamento sia effettuato nel rispetto di tutte le normative applicabili. I "responsabili del trattamento/progetto" garantiscono il trattamento lecito, ossia garantiscono che una normativa legale applicabile o il consenso dell'interessato consentano l'utilizzo dei dati personali e che tutti gli altri principi del trattamento lecito dei dati siano rispettati in ogni momento.

Ciò include la garanzia dell'attuazione di misure tecniche e organizzative adeguate per proteggere i dati personali, compresa la protezione contro il trattamento non autorizzato, illecito o l'alterazione delle finalità e contro la perdita, la distruzione o il danno accidentali, nonché le misure per una cancellazione corretta e tempestiva, tenendo conto dello stato dell'arte e della natura, dell'ambito, del contesto e delle finalità del trattamento, nonché del rischio di varia probabilità e gravità per i diritti e le libertà di interessati. Inoltre, i "responsabili del trattamento/progetto" forniscono agli interessati informazioni trasparenti ("informative sulla protezione dei dati") sul trattamento dei dati che consentono loro di far valere efficacemente i diritti che spettano loro ai sensi delle leggi sulla protezione dei dati.

La messa in servizio o le modifiche ai responsabili del trattamento sono segnalate all'organizzazione per la protezione dei dati dai "responsabili di processo/progetto". Tutti i responsabili del trattamento sono regolarmente controllati per verificarne l'affidabilità nell'erogazione dei servizi e il rispetto di misure tecniche e organizzative adeguate; I controlli vengono effettuati, ad esempio, attraverso interviste, autovalutazioni, revisioni di documenti, indagini in loco o altre misure adeguate. I DPM mantengono una panoramica di tutti i processori commissionati dalla rispettiva divisione aziendale. Se il trattamento comporta trasferimenti di dati a destinatari in un paese al di fuori dell'Unione Europea (paese terzo), i responsabili del processo/progetto segnalano tali trasferimenti di dati; adeguate misure di protezione e la garanzia dei diritti di terzi nei confronti del rispettivo DPM; L'esecutività e i mezzi di ricorso effettivi sono riesaminati periodicamente.

In qualità di Gruppo che opera a livello globale, DEUTZ si affida a trasferimenti internazionali interni di dati per rendere i dati disponibili ai relativi responsabili del trattamento. A questo proposito, abbiamo definito i requisiti per il trasferimento dei dati all'interno del Gruppo. Esistono accordi standard tra le relative società affiliate, ad esempio, e clausole contrattuali standard. Tali misure prevedono garanzie adeguate, diritti degli interessati applicabili e mezzi di ricorso efficaci per gli interessati.

COMUNICAZIONE

La comunicazione e la sensibilizzazione in materia di protezione dei dati sono ampiamente diversificate e spaziano da informazioni generali, su punti di condivisione o altri canali accessibili a tutti i dipendenti o indirizzati a reparti specifici, a informazioni dettagliate mirate sull'intranet DEUTZ (Protezione dei dati), che si rivolge a singoli gruppi di interesse, fino alle discussioni all'interno della cerchia degli stakeholder della protezione dei dati.

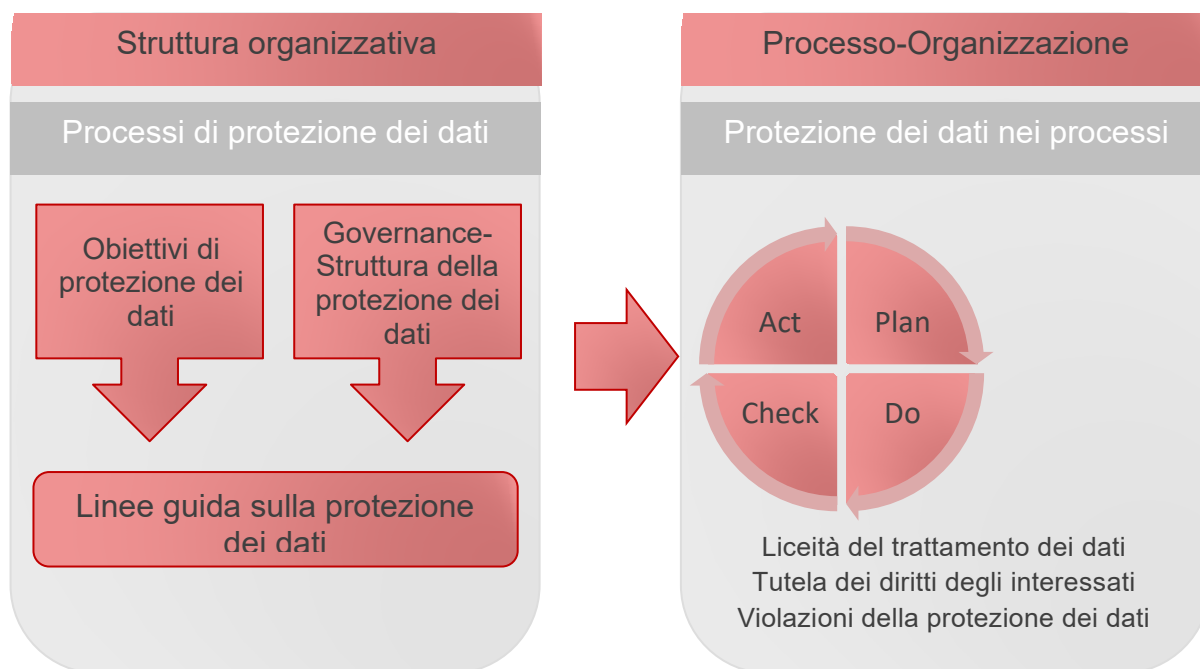
DEUTZ riferisce annualmente sui propri progressi in materia di protezione dei dati nell'ambito del suo rapporto annuale sui progressi in materia di protezione dei dati. I processi e gli standard di protezione dei dati vengono comunicati ai nostri dipendenti a diversi livelli. Le misure di formazione e sensibilizzazione sono adattate al profilo di rischio delle aree di business e alle attività specifiche dei destinatari. Ciò include una formazione di base sul GDPR sotto forma di e-learning, che è obbligatoria per tutti i dipendenti del Gruppo DEUTZ. Inoltre, vengono offerti sia corsi di e-learning volontari che corsi di formazione faccia a faccia per dipartimenti specializzati e "decisori in materia di protezione dei dati".

La consapevolezza che la protezione dei dati è una responsabilità di tutti è rafforzata dall'"obbligo di mantenere la segretezza dei dati e delle telecomunicazioni", di cui tutti i dipendenti sono informati prima di iniziare a lavorare. I dipendenti possono richiedere una consulenza adeguata su questioni relative alla protezione dei dati. Sono liberi di contattare in qualsiasi momento i responsabili della protezione dei dati competenti dell'organizzazione per la protezione dei dati. organizzazione in qualsiasi momento. L'ulteriore sviluppo del concetto di formazione sulla protezione dei dati, in particolare per quanto riguarda la formazione dei responsabili della protezione dei dati e di altri collaboratori interni basata su un approccio basato sul rischio (ad es. HR, IT del gruppo e marketing in relazione ai dati dei clienti), è fortemente previsto nel DPMS.

MONITORAGGIO

Il continuo sviluppo dei nostri concetti, contenuti e strumenti per garantire un'adeguata protezione dei dati ha ulteriormente migliorato l'efficacia dell'attuale sistema di gestione della protezione dei dati (DPMS).

Il DPMS aiuta DEUTZ a pianificare, implementare e rivedere regolarmente le misure per il rispetto delle normative sulla protezione dei dati in modo strutturato. I responsabili della



protezione dei dati che lavorano nell'organizzazione per la protezione dei dati analizzano e utilizzano i risultati degli audit per ridurre costantemente i rischi per la protezione dei dati.

L'efficacia delle misure di protezione dei dati viene verificata anche da controlli interni e indagini di audit interno.

L'organizzazione per la protezione dei dati collabora con il dipartimento di audit interno, che prepara ed esegue la maggior parte degli audit interni all'interno del Gruppo DEUTZ sulla base di un piano di audit basato sul rischio.

Le questioni legali relative alla protezione dei dati vengono discusse e coordinate con i consulenti legali interni ed esterni e viene fornita consulenza su ulteriori miglioramenti e nuovi requisiti normativi. L'organizzazione per la protezione dei dati è attivamente collegata in rete in forum esterni, il che consente uno scambio di conoscenze e un benchmarking dei processi con colleghi specializzati.

Le migliori pratiche vengono identificate, implementate e portano a miglioramenti nei processi di protezione dei dati in DEUTZ. L'identificazione delle carenze di controllo e l'attuazione di misure appropriate fanno parte della rendicontazione sulla protezione dei dati, compreso lo sviluppo di importanti attività di conformità che vengono implementate in diverse società del Gruppo.

DEUTZ AG

Ottostr. 1

51149 Köln

Telefono: +49 (0) 221 822-0

Telefax: +49 (0) 221 822-3525

E-mail: ir@deutz.com

www.deutz.com

