DEUTZ-Datenschutzkodex

Version 1/2023 | Stand Dezember 2023

VORWORT

Das Datenschutz-Management-System (DSMS) wurde für den DEUTZ-Konzern unter Berücksichtigung allgemein anerkannter Standards, des geltenden Rechts und unternehmensindividuell in Abhängigkeit von Art und Umfang der Geschäftstätigkeit sowie der Art der verarbeiteten personenbezogenen Daten aufgestellt.

Nachfolgend beschreiben wir die Grundelemente unseres DSMS in Anlehnung an den Prüfungsstandard IDW PS 980 und unter Berücksichtigung des IDW PH 9.860.1 (Prüfung der Grundsätze, Verfahren und Maßnahmen nach der EU-Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG)) als nicht abschließende Aufzählung.

Das DSMS umfasst dabei alle datenschutzspezifischen Maßnahmen, die in den Konzerngesellschaften zur Einhaltung der geltenden Datenschutzgesetze im materiellen und räumlichen Geltungsbereich der „Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO)“ ergriffen werden.

Die Datenschutzorganisation ist als Teil in einem ganzheitlichen Governance, Risk & Compliance (GRC)-System eingebunden.

Der DEUTZ-Vorstand im Dezember 2023

Aus Gründen der besseren Lesbarkeit sehen wir nachfolgend von einer geschlechtsspezifischen Ansprache ab. Es sind in jedem Fall alle Geschlechter gleichermaßen angesprochen. Die verkürzte Sprachform erfolgt ausschließlich aus redaktionellen Gründen und beinhaltet keine Wertung.

INHALT

Vorwort 2

Inhalt 3

Datenschutz-Regelkreis 4

Kultur 4

Ziele 6

Organisation 6

Risiken 8

Programm 8

Kommunikation 11

Überwachung 11

DATENSCHUTZ-REGELKREIS

Bei Kunden, Geschäftspartnern und Beschäftigten besteht die berechtigte Erwartung, dass die uns anvertrauten Daten vertraulich und nur für die vorgesehenen Zwecke verarbeitet werden. Dieses DSMS gilt für die DEUTZ AG und alle verbundenen Mehrheitsbeteiligungen, die dem räumlichen Anwendungsbereich der DSGVO unterliegen. Sein Zweck ist es, die aus der DSGVO abgeleiteten Prinzipien so umzusetzen, wie sie in der Datenschutzrichtlinie von DEUTZ definiert sind und in Anlehnung an den Datenschutz-Regelkreis festgelegt sind.

KULTUR

DEUTZ bekennt sich zum Grundrecht auf Datenschutz. Dieses Recht schützt jede einzelne natürliche Person vor Eingriffen in ihre Privatsphäre durch nicht notwendige, willkürliche oder unverhältnismäßige Nutzung von personenbezogenen Daten. Die Wahrung dieses Rechts liegt im Selbstverständnis unseres unternehmerischen Handelns.

In einer zunehmend digitalisierten und datengetriebenen Wirtschaft führen neue Technologien zur Datenverarbeitung, naturgemäß auch zu größeren Mengen an persönlichen Daten und deren vielfältigerer Nutzung. Dadurch ist es für DEUTZ möglich, in internen Prozessen und den Aktivitäten gegenüber Stakeholdern kundenorientierter,

innovativer, agiler und umfassend digital zu werden. Zugleich geht damit die Herausforderung einher, die Privatsphäre der betroffenen Personen in geeigneter Weise zu schützen. Der DEUTZ-Konzern hat deswegen ein zentrales Interesse daran, dass innovative Technologien und neue Geschäftsmodelle im Einklang mit geltenden Datenschutzbestimmungen stehen. Mit zunehmender Digitalisierung halten wir es daher für wichtig, dass DEUTZ sich auch im Rahmen der unternehmerischen Tätigkeit ausdrücklich zu seiner Datenverantwortung bekennt. Der verantwortungsvolle Umgang mit Daten im Interesse unserer Geschäftspartner, Beschäftigten und anderen Stakeholdern, wird daher auch in Zukunft zu unseren Zielen gehören und das Vertrauen in DEUTZ weiter festigen.

Die Festlegung der Datenschutz-Strategie zum Umgang mit datenschutzrechtlichen Anforderungen hilft uns diese Ziele – abgestimmt auf die konkreten Aktivitäten der Konzerngesellschaften – zu erreichen. Grundlegend ist dabei ein gutes Verhältnis zu sämtlichen Stakeholdern (Beschäftigte, Kunden, Geschäftspartner, Lieferanten, Anteilseigner usw.). Jeder Verstoß gegen Datenschutzgesetze birgt die Gefahr, unseren Ruf dauerhaft zu schädigen, und kann zu erheblichen Schäden und schwerwiegenden Folgen für den gesamten DEUTZ-Konzern führen. Darüber hinaus können derartige Verstöße, ebenso für die beteiligten Beschäftigten, zu zivil- oder strafrechtlichen Sanktionen führen.

Bei DEUTZ ist ethisches und juristisch korrektes Handeln ein Kernprinzip, das bereits im „DEUTZ Verhaltenskontext“ zum Ausdruck kommt und selbstverständlich die Einhaltung des Datenschutzrechts umfasst. Dies wird unterstützt durch das grundlegende bei DEUTZ bestehende Verständnis, dass die Einhaltung der geltenden Gesetze im Konfliktfall stets Vorrang vor den Geschäftszielen hat.

Darüber hinaus basiert unsere „Datenschutzrichtlinie“ auf dem grundlegenden Verständnis, dass jede Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen, insbesondere der Datenschutz-Grundverordnung (DSGVO) erfolgen muss.

ZIELE

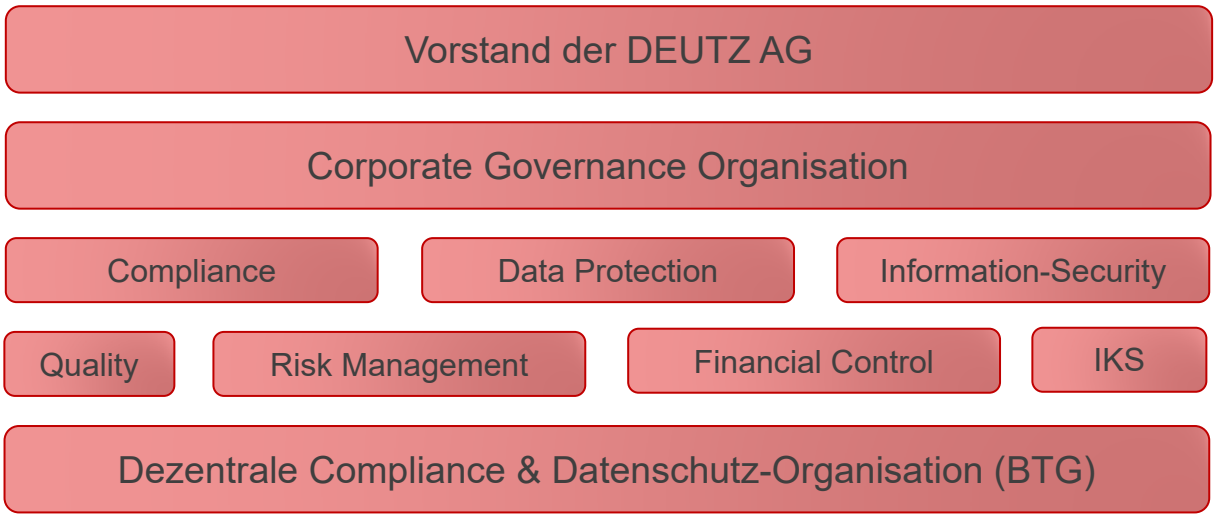
Die Rechtspflichten aus den jeweiligen Datenschutzbestimmungen – insbesondere aus der Datenschutz-Grundverordnung (DSGVO) und dem Bundesdatenschutzgesetz (BDSG) – stellen komplexe und strenge Anforderungen an denjenigen, der personenbezogene Daten verarbeitet. Unser Ziel ist es, dass alle datenschutzrechtlichen Vorgaben konzernweit eingehalten werden.

Jeder einzelne bei DEUTZ ist dafür verantwortlich, personenbezogene Daten angemessen vertraulich zu behandeln und vor Missbrauch zu schützen, damit niemand durch den Umgang mit diesen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Alle Beschäftigten bei DEUTZ werden mit personenbezogenen Daten unserer Kunden, Geschäftspartner und ihren Kollegen sorgfältig und vertraulich umgehen und das geltende Recht beachten. Jede Person, die im DEUTZ Konzern für eine Aktivität, die personenbezogene Daten betrifft, verantwortlich ist, organisiert die Verarbeitung (Erhebung, Nutzung, Speicherung, Löschung etc.) personenbezogener Daten so, dass die Einhaltung geltenden Rechts gewährleistet wird. Diese Erwartungen übertragen wir in unseren „Verhaltenscodex für Lieferanten“ auch auf unsere Lieferanten.

ORGANISATION

Der DEUTZ-Konzern besteht aus der DEUTZ AG als Konzernmutter und zahlreichen Gesellschaften, an denen die DEUTZ AG mit mehr als 50 % beteiligt ist. Diese Beteiligungsgesellschaften (BTG) sind in die zentrale Governance Structure eingebunden.

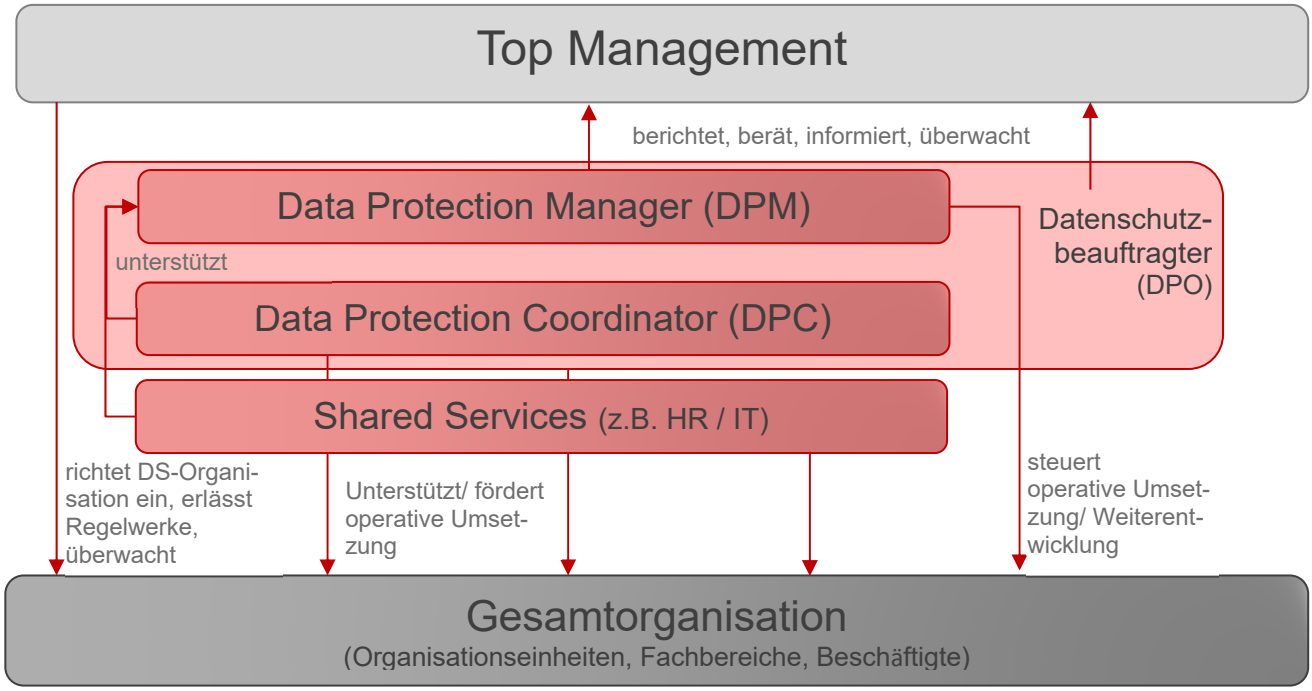


Innerhalb der Beteiligungsgesellschaften muss die Einhaltung der Datenschutzanforderungen hinsichtlich jeder einzelnen Verarbeitung von personenbezogenen Daten („Verarbeitungstätigkeit“), auf Gesellschaftsebene sichergestellt sein. Der Vorstand

trägt die Gesamtverantwortung für die Einhaltung der geltenden Gesetze und internen Standards.

DEUTZ hat ein interdisziplinäres „Datenschutz-Team“ eingerichtet, das für die Steuerung und Überwachung der Datenschutzorganisation zuständig ist. Soweit gesetzlich vorgesehen, ernennt jede Konzerngesellschaft einen fachkundigen Datenschutzbeauftragten (DPO), der die gesetzlich definierten Aufgaben, insbesondere die Funktion als Ansprechpartner für Betroffene, wahrnimmt.

Für jeden Geschäftsbereich ist zudem ein Data Protection Manager (DPM) ernannt. Die DPM sind über die gesetzlichen Pflichten eines DPO hinaus für die Einhaltung der datenschutzrechtlichen Vorgaben zuständig. Die Leitung delegiert an den DPM die Wahrnehmung ihrer datenschutzrechtlichen Pflichten.



Der operative Datenschutz (wie z. B. die Sicherstellung der Rechtmäßigkeit von Datenverarbeitungen; das Management von Auftragsverarbeitern; die Einhaltung der internen Datenschutz-Management-Prozesse, die Überwachung, Erstellung einer geeigneten Dokumentation zum Nachweis der Einhaltung der DSGVO etc.) ist Aufgabe der Data Protection Manager. Sie verfügen über ausreichendes Wissen und die erforderlichen Ressourcen zur Erfüllung ihrer Aufgaben sowie über die Befugnis, Datenverarbeitungen zu ändern oder auszusetzen. Die Konzern IT unterstützet dabei, technische und organisatorische Maßnahmen in Übereinstimmung mit der DSGVO und anderen relevanten Rechtsordnungen zu definieren und Prozesse zu

implementieren, die sicherstellen, dass bei der Einführung oder Änderung einer Verarbeitung personenbezogener Daten die Prinzipien „Privacy by Design“ und „Privacy by Default“ berücksichtigt werden.

RISIKEN

Im Rahmen eines integrierten Corporate-Governance-Ansatzes betreibt der DEUTZ Konzern ein umfassendes konzernweites Risikomanagementsystem. Innerhalb dieses Systems werden auch die wesentlichen Datenschutzrisiken erfasst und gesteuert. Dabei werden Datenschutzrisiken sowohl aus der Sicht der von der Datenverarbeitung betroffenen natürlichen Person („Betroffene“) beurteilt als auch aus Sicht des Unternehmens. Die Bewertung des Risikos resultiert dabei im Wesentlichen aus der Kategorie der verarbeiteten Daten und den dabei eingesetzten Mitteln, dem Gefahrenpotential und der Komplexität der Verarbeitung.

Das Risiko jeder einzelnen Verarbeitung wird dabei nach einer eigenen Methodik bewertet, die sowohl die verarbeiteten Datentypen als auch die konkrete Art der Verarbeitung berücksichtigt. Damit kann festgestellt werden, ob die Verarbeitung personenbezogener Daten allein aufgrund des Umstands ein Risiko darstellt, dass überhaupt personenbezogene Daten verarbeitet werden, ob spezielle Kategorien personenbezogener Daten betroffen sind oder ob bestimmte Datenkategorien und Risikofaktoren auf ein erhöhtes Risiko einer Verarbeitungstätigkeit bei der Verarbeitung hinweisen.

PROGRAMM

Das DSMS basiert auf weltweit verbindlichen Konzerngrundsätzen und ergänzenden Richtlinien. Das Kernstück des DSMS sind die „Verarbeitungsgrundsätze“. Diese verfolgen das Ziel, im Konzern sowohl organisatorische Mindeststandards sowie einen einheitlichen Rahmen für die Verarbeitung und den Schutz personenbezogener Daten zu schaffen als auch Schäden von DEUTZ abzuwenden. Sie können durch zusätzliche Richtlinien mit Geltung für bestimmte Länder oder Geschäftsbereiche ergänzt werden, um die Einhaltung der datenschutzrechtlichen Anforderungen vollumfänglich sicherzustellen.

Unser Datenschutz-Programm umfasst insbesondere:

- Auftragsverarbeitung
- Betroffenenrechte
- Drittstaatenübermittlung
- Löschkonzepte
- Melde- und Benachrichtigungspflichten
- Technisch und organisatorische Maßnahmen
- Verarbeitungsverzeichnis

Ein sogenannter „Incident Response Plan“ gibt beispielsweise den Rahmen für die effektive Identifizierung, das interne Management und die externe Meldung von Datenschutzverstößen vor. Datenschutzverstöße, die im Rahmen einer Untersuchung, allgemeiner Überwachungsprozesse oder auf andere Weise festgestellt werden, müssen dem jeweiligen DPM entsprechend den Vorgaben der Richtlinie und in der dort festgelegten Form unverzüglich gemeldet werden. Der DPO berät den Verantwortlichen bei der Entscheidung, ob eine Meldung an die Datenschutzbehörden oder / und die von der Schutzverletzung betroffenen Personen erforderlich ist und gibt gegebenenfalls die Meldung heraus.

Unsere „Datenschutzrichtlinie“ verpflichtet jede Gesellschaft im Konzernverbund ein Verzeichnis der relevanten Verarbeitungstätigkeiten zu führen (Verarbeitungsverzeichnis) sowie einen Prozess zu implementieren, um Änderungen zu berücksichtigen und die Richtigkeit wie Vollständigkeit der Verarbeitungstätigkeiten sicherzustellen. Für die Verwaltung solcher datenschutzrelevanten Aufgaben setzt DEUTZ eine Datenschutz-Management-Software ein.

Für jede einzelne Verarbeitungstätigkeit muss sichergestellt sein, dass die Verarbeitung unter Einhaltung aller geltenden Vorschriften geschieht. Die „Prozess-/ Projektverantwortlichen“ gewährleisten die rechtmäßige Verarbeitung, d. h. sie stellen sicher, dass entweder eine geltende gesetzliche Regelung oder Einwilligung der betroffenen Person die Verwendung von personenbezogenen Daten erlaubt und dass alle anderen Grundsätze einer rechtmäßigen Datenverarbeitung jederzeit eingehalten werden.

Dies umfasst die Sicherstellung der Implementierung geeigneter technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten, einschließlich des Schutzes vor unbefugter, unrechtmäßiger Verarbeitung oder Änderung des

Zwecks und vor versehentlichem Verlust, Zerstörung oder Beschädigung, ebenso wie Maßnahmen zur ordnungsgemäßen und rechtzeitigen Löschung, wobei der Stand der Technik sowie die Art, der Umfang, der Kontext und die Zwecke der Verarbeitung sowie das Risiko unterschiedlicher Wahrscheinlichkeit und Schwere für die Rechte und Freiheiten der betroffenen Personen zu berücksichtigen sind. Darüber hinaus stellen die „Prozess-/Projektverantwortlichen“ den betroffenen Personen transparente Informationen (sog. „Datenschutzhinweise“) über die Datenverarbeitung zur Verfügung, die es ihnen ermöglichen, die ihnen nach den Datenschutzgesetzen zustehenden Rechte wirksam geltend zu machen.

Beauftragung oder Änderung von Auftragsverarbeitern werden durch die „Prozess-/ Projektverantwortlichen“ an die Datenschutzorganisation gemeldet. Alle Auftragsverarbeiter werden regelmäßig auf ihre Zuverlässigkeit zur Erbringung von Leistungen und die Einhaltung geeigneter technischer wie organisatorischer Maßnahmen hin überprüft; die Kontrolle erfolgt z. B. durch Interviews, Self-Assessments, Dokumenten-Reviews, Untersuchungen vor Ort oder andere geeignete Maßnahmen. Die DPM führen eine Übersicht aller von dem jeweiligen Geschäftsbereich beauftragten Auftragsverarbeitern. Bringt eine Verarbeitung Datenübermittlungen an Empfänger in einem Land außerhalb der Europäischen Union (Drittland) mit sich, melden Prozess-/ Projektverantwortliche solche Datentransfers; angemessene Schutzmaßnahmen sowie die Gewährleistung der Rechte Dritter an die jeweiligen DPM; Durchsetzbarkeit und effektiver Rechtsmittel werden regelmäßig überprüft.

Als weltweit agierender Konzern ist DEUTZ auf interne internationale Datenübermittlungen angewiesen, um die Daten den entsprechenden Verarbeitern zur Verfügung zu stellen. Diesbezüglich haben wir Anforderungen für Datenübermittlungen innerhalb des Konzerns definiert. Zwischen den betreffenden Beteiligungsgesellschaften bestehen. bspw. Standardvertragsklauseln. Diese sehen angemessene Schutzmaßnahmen, durchsetzbare Rechte der Betroffenen und wirksame Rechtsmittel für die betroffenen Personen vor.

KOMMUNIKATION

Kommunikation bzw. Sensibilisierung im Datenschutz erfolgt breit gestreut und reicht von allgemeinen Informationen, auf Sharepoints oder anderen Kanälen, die für alle Beschäftigten zugänglich oder an bestimmte Fachbereiche adressiert sind, über zielorientierte Detailinformationen im DEUTZ-Intranet (Bereiche „Datenschutz“), die sich an einzelne Interessengruppen richten bis hin zu Diskussionen im Kreis der Datenschutz-Akteure.

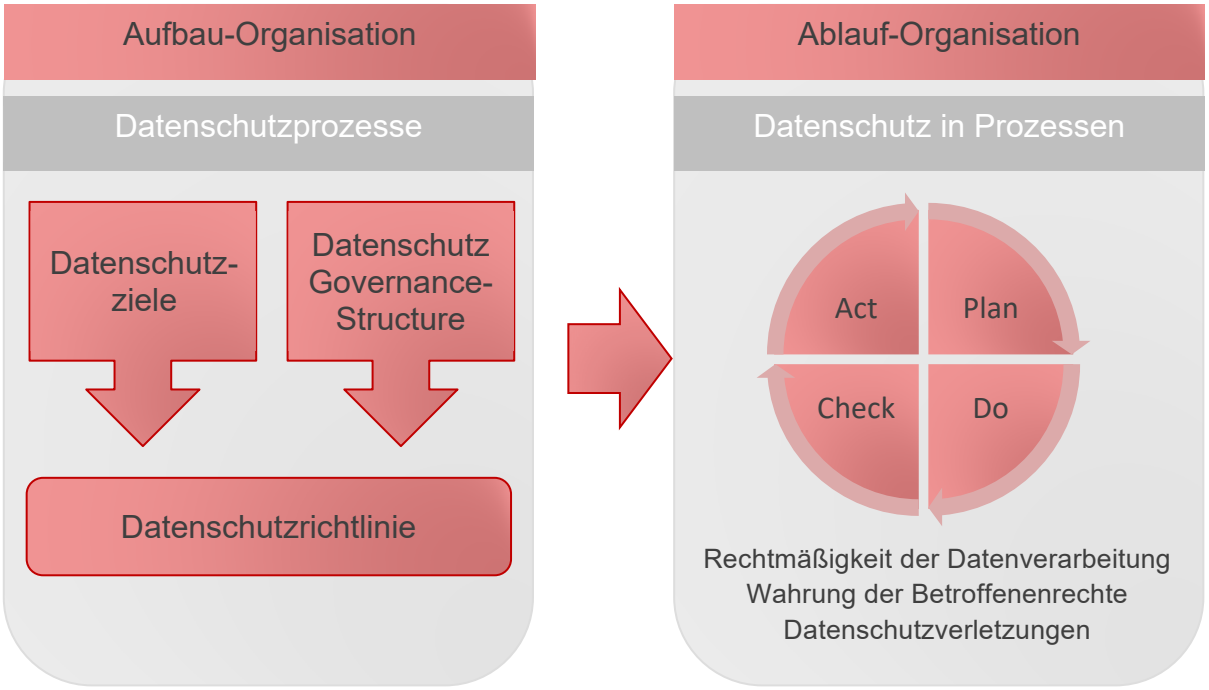
DEUTZ berichtet jährlich im Rahmen seines Geschäftsberichts über die eigenen Fortschritte im Datenschutz. Datenschutzprozesse und -standards werden unseren Beschäftigten auf mehreren Ebenen vermittelt. Schulungs- und Sensibilisierungsmaßnahmen sind auf das Risikoprofil der Geschäftsfelder und die konkreten Aktivitäten der Adressaten zugeschnitten. Dazu gehört eine Grundlagenschulung zur DSGVO als „eLearning“, die für alle Beschäftigten im DEUTZ-Konzern verpflichtend ist. Darüber hinaus werden sowohl freiwillige eLearnings wie auch persönliche Schulungen für Fachbereiche und „Entscheider im Datenschutz“ angeboten.

Das Verständnis, dass Datenschutz in der Verantwortung aller liegt, ist gestärkt durch die „Verpflichtung auf das Daten- und Fernmeldegeheimnis“, über die alle Beschäftigten vor Beginn ihrer Tätigkeit unterrichtet werden. Die Beschäftigten können sich in Datenschutzfragen angemessen beraten lassen. Ihnen steht es frei, sich dazu jederzeit mit den jeweiligen Datenschutz-Akteuren aus der Datenschutzorganisation in Verbindung zu setzen. Die Weiterentwicklung des Datenschutz-Schulungskonzeptes, insbesondere im Hinblick auf Schulungen für Datenschutz-Akteure und andere interne Beschäftigte auf Basis eines risikobasierten Ansatzes (z. B. HR, Group-IT und Marketing im Zusammenhang mit Kundendaten), ist im DSMS fest vorgesehen.

ÜBERWACHUNG

Die fortlaufende Weiterentwicklung unserer Konzepte, Inhalte und Instrumente zur Gewährleistung eines angemessenen Datenschutzes, konnte die Wirksamkeit des bestehenden Datenschutzmanagementsystems (DSMS) weiter verbessern.

Das DSMS unterstützt DEUTZ dabei, Maßnahmen zur Einhaltung der Datenschutzbestimmungen strukturiert zu planen, umzusetzen und regelmäßig zu überprüfen. Die in der Datenschutzorganisation tätigen Datenschutz-Akteure analysieren und nutzen die Ergebnisse der Prüfungen, um Datenschutzrisiken kontinuierlich zu reduzieren. Die Datenschutzmaßnahmen werden zudem durch interne Kontrollen und Untersuchungen der internen Revision auf ihre Wirksamkeit überprüft.



Die Datenschutzorganisation arbeitet mit der internen Revision zusammen, die den überwiegenden Teil der internen Prüfungen innerhalb der DEUTZ-Gruppe auf Basis eines risikobasierten Prüfungsplans vorbereitet und durchführt.

Rechtliche Datenschutzangelegenheiten werden mit interner und externer Rechtsberatung erörtert und abgestimmt sowie zu weiteren Verbesserungen und neuen regulatorischen Anforderungen beraten. Die Datenschutzorganisation ist aktiv in externen Foren vernetzt, was einen Austausch von Wissen und Benchmark von Prozessen mit Fachkollegen ermöglicht.

Best Practices werden identifiziert, umgesetzt und führen zu Verbesserungen der Datenschutzprozesse bei DEUTZ. Die Identifizierung von Kontrolldefiziten sowie die Umsetzung geeigneter Maßnahmen ist Teil der Datenschutzberichterstattung, einschließlich der Entwicklung wichtiger Compliance-Aktivitäten, die über mehrere Gesellschaften im Konzern hinweg umgesetzt werden.

DEUTZ AG
Ottostr. 1
51149 Köln
Telefon: +49 (0) 221 822-0
Fax: +49 (0) 221 822-3525
E-Mail: ir@deutz.com
www.deutz.com