Datenschutz-Management-System (DMS)
Henkel AG & Co. KGaA („Henkel Deutschland“)

Vorbemerkung

Das Datenschutz-Management-System (DMS) von Henkel wurde unter Berücksichtigung allgemein anerkannter Standards und des geltenden Rechts aufgestellt. Nachfolgend beschreiben wir die Grundelemente des Henkel-DMS zum 03.09.2019 gemäß IDW PS 980 und unter Berücksichtigung des IDW PH 9.860.1. Henkels DMS umfasst dabei alle Managementmaßnahmen, die in den Unternehmen der Henkel-Gruppe zur Einhaltung der geltenden Datenschutzgesetze im materiellen und räumlichen Geltungsbereich der Verordnung (EU) 2016/679 (Datenschutzgrundverordnung – DSGVO) ergriffen werden.

Der Vorstand trägt die Gesamtverantwortung für die Datenschutzorganisation, die als Teil der Compliance-Organisation von Henkel organisiert ist und unter der Leitung des weltweit verantwortlichen General Counsel & Chief Compliance Officer (CCO) mit der Sicherstellung der weltweiten Einhaltung von Gesetzen und internen Standards beauftragt ist.

1. Datenschutzkultur

In einer zunehmend digitalisierten und datengetriebenen Wirtschaft bringen neue Technologien zur Datenverarbeitung immer wieder die Herausforderung mit sich, die Privatsphäre der Menschen in geeigneter Weise zu schützen. Dabei führt Henkels Strategie, in unseren internen Prozessen und unseren Aktivitäten gegenüber den Kunden kundenorientierter, innovativer, agiler und umfassend digital zu werden, naturgemäß zu einer größeren Menge an persönlichen Daten bei Henkel und deren vielfältigerer Nutzung.

Die Fähigkeit von Henkel, seine strategischen Ziele zu erreichen, beruht auf einem guten Verhältnis zu sämtlichen Akteuren, z.B. Mitarbeiter, Kunden, Geschäftspartner, Lieferanten, Anteilseigner usw. Jeder Verstoß gegen Datenschutzgesetze birgt dabei die Gefahr, Henkels Ruf dauerhaft zu schädigen, und kann für Henkel zu erheblichen Schäden und schwerwiegenden Folgen führen. Darüber hinaus können derartige Verstöße für Henkel, ebenso wie für die beteiligten Mitarbeiter, zu zivil- oder strafrechtlichen Sanktionen führen.

Bei Henkel ist ethisches und juristisch korrektes Handeln ein Kernprinzip, das bereits in Henkels *Code of Conduct* zum Ausdruck kommt. Dies umfasst selbstverständlich die Einhaltung des Datenschutzrechts. Dies wird unterstützt durch das grundlegende bei Henkel geltende Verständnis, dass die Einhaltung der geltenden Gesetze im Konfliktfall stets Vorrang vor den Geschäftszielen hat.

> ***„Wir sind uns unserer Verpflichtung bewusst, die persönliche Würde, die Privatsphäre und die Persönlichkeitsrechte aller Mitarbeiterinnen und Mitarbeiter sowie unserer Kunden, Dienstleister und Lieferanten zu respektieren.“***
>
> *Code of Conduct*

Darüber hinaus basiert die Henkel-interne EU-Datenschutzrichtlinie (*EU Data Protection Policy*) auf dem grundlegenden Verständnis, dass jede Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen, insbesondere der DSGVO erfolgen muss.

Die Datenschutzkultur von Henkel wird durch die folgende Erklärung des Henkel-Vorstandsvorsitzenden im globalen Compliance eLearning zum Datenschutz veranschaulicht:

> ***„In einer zunehmend digitalisierten Welt ist Datenschutz ein kritischer Faktor und der Schutz personenbezogener Daten ist und bleibt eine der Top-Prioritäten in der Compliance-Management-Strategie von Henkel. Es liegt in unser aller Verantwortung, dass die Einhaltung der DSGVO sichergestellt wird.“***

Das Verständnis, dass Datenschutz in der Verantwortung aller liegt, wurde durch die „Verpflichtungserklärung für die Verarbeitung personenbezogener Daten“ gestärkt, die allen Mitarbeitern weltweit zugegangen ist.

2. Datenschutz-Ziele

Henkel betreibt seine Geschäfte in Ländern mit strengen und weniger strengen Datenschutzbestimmungen. Überall besteht jedoch bei Kunden, Partnern und Mitarbeitern die berechtigte Erwartung, dass die Henkel anvertrauten Daten sicher aufbewahrt und nur für die vorgesehenen Zwecke verarbeitet werden. Allerdings verlangen nicht alle Rechtsordnungen Datenschutz nach einem einheitlichen globalen Standard, noch ist es möglich, so allen Rechtsordnungen gleichermaßen gerecht zu werden. Das DMS von Henkel konzentriert sich daher auf Datenverarbeitungen im Anwendungsbereich der DSGVO.

Dieses DMS gilt für Henkel Deutschland und die verbundenen Unternehmen, die dem räumlichen Anwendungsbereich der DSGVO unterliegen. Sein Zweck ist es, die aus der DSGVO abgeleiteten Leitprinzipien umzusetzen, wie sie in der EU-Datenschutzrichtlinie von Henkel definiert sind, mit den Zielen:

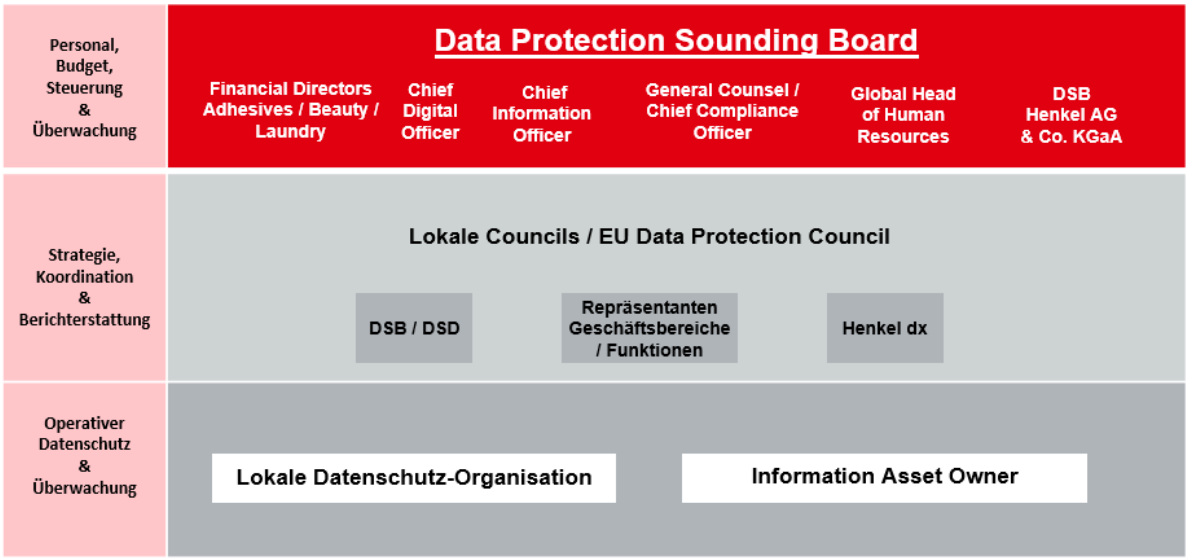
1. Errichtung einer ordnungsgemäßen Datenschutzorganisation;
2. rechtmäßige Verarbeitung personenbezogener Daten;
3. erforderliche Richtlinien und Standards;
4. praxisgerechte Prozesse und Verfahrensanweisungen zur Compliance;
5. geeignete Maßnahmen zur Datensicherheit; und
6. zuverlässige Mechanismen, um die Compliance nachzuweisen (Rechenschaftspflicht).

3. Datenschutz-Organisation

Innerhalb des Geltungsbereiches dieses DMS muss die Einhaltung der Datenschutzbestimmungen hinsichtlich jeder einzelnen Verarbeitung von personenbezogenen Daten, sei es als Verantwortlicher oder als Auftragsverarbeiter (jeweils ein „Information Asset“), auf Unternehmensebene sichergestellt sein.

Der **Vorstand** trägt die Gesamtverantwortung für die weltweite Einhaltung der geltenden Gesetze und internen Standards. Henkel hat ein interdisziplinäres **Data Protection Sounding Board** unter dem Vorsitz des Datenschutzbeauftragten von Henkel Deutschland eingerichtet, das für die personelle und finanzielle Ausstattung sowie für die Steuerung und Überwachung der Datenschutzorganisation im Geltungsbereich dieses DMS zuständig ist.

Henkels Datenschutz-Organisation



Jedes Henkel-Unternehmen im Geltungsbereichs des DMS, das Verantwortlicher oder Auftragsverarbeiter von Information Assets ist, ernennt einen **Datenschutzbeauftragten (DSB)** oder **Datenschutzdelegierten (DSD)**, der die in der DSGVO definierten Aufgaben eines Data Protection Officers wahrnimmt, insbesondere das Führen eines Verfahrensverzeichnisses aller gemäß den eingerichteten Prozessen gemeldeten Information Assets, die personenbezogene Informationen enthalten, und seine Funktion als Ansprechpartner für Anfragen Dritter.

Jeder DSB / DSD hat darüber hinaus den Vorsitz des für das jeweilige Unternehmen eingerichteten **Data Protection Councils** (DPC) inne, das aus den ernannten Delegierten der jeweiligen Geschäftsbereiche, von HR, der IT sowie anderen geeigneten, vom DSB / DSD ernannten Personen besteht. Das Data Protection Council ist mit Aufgaben hinsichtlich Strategie, Koordination und Berichterstattung betraut. Es evaluiert datenschutzrelevante Prozesse und Richtlinien, überwacht die Umsetzung datenschutzrelevanter Maßnahmen und berichtet den Status des Unternehmens an das lokale Management, das im Falle von Henkel Deutschland durch das Sounding Board vertreten wird.

Das **EU Data Protection Council** (EU-DPC) setzt sich aus allen DSBs / DSDs unter dem Vorsitz des DSB von Henkel Deutschland zusammen und wurde für den halbjährlichen Austausch zwischen den Henkel-Unternehmen eingerichtet, insbesondere in Bezug auf Fragen des unternehmensinternen Datentransfers, Verantwortlicher-Auftragsverarbeiter-Verhältnisse und andere Themen, die mehr als ein Unternehmen oder Gruppen von Ländern mit gemeinsamen Management-Funktionen betreffen.

Der operative Datenschutz (z.B. Sicherstellung der Rechtmäßigkeit von Datenverarbeitungen, Management von Auftragsverarbeitern, Einhaltung der internen Datenschutzmanagementprozesse, Überwachung (1st line of defense), Erstellung geeigneter Dokumentation zum Nachweis der Einhaltung der DSGVO etc.) ist Aufgabe der **Information Asset Owner**. Sie müssen über ausreichendes Wissen und die erforderlichen Ressourcen zur Erfüllung ihrer Aufgaben sowie über die Befugnis verfügen, Datenverarbeitungen zu ändern oder zu stoppen.

Die Konzern-IT ist dafür zuständig, 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 eines Information Assets die Prinzipien des Datenschutzes durch Technikgestaltung und der datenschutzfreundlichen Voreinstellungen berücksichtigt werden. Außerdem ist die Konzern-IT für die regelmäßige Überwachung der Übereinstimmung mit diesen Richtlinien verantwortlich. Darüber hinaus leistet sie in allen Ländern im Anwendungsbereich des DMS Unterstützung im Datenschutz.

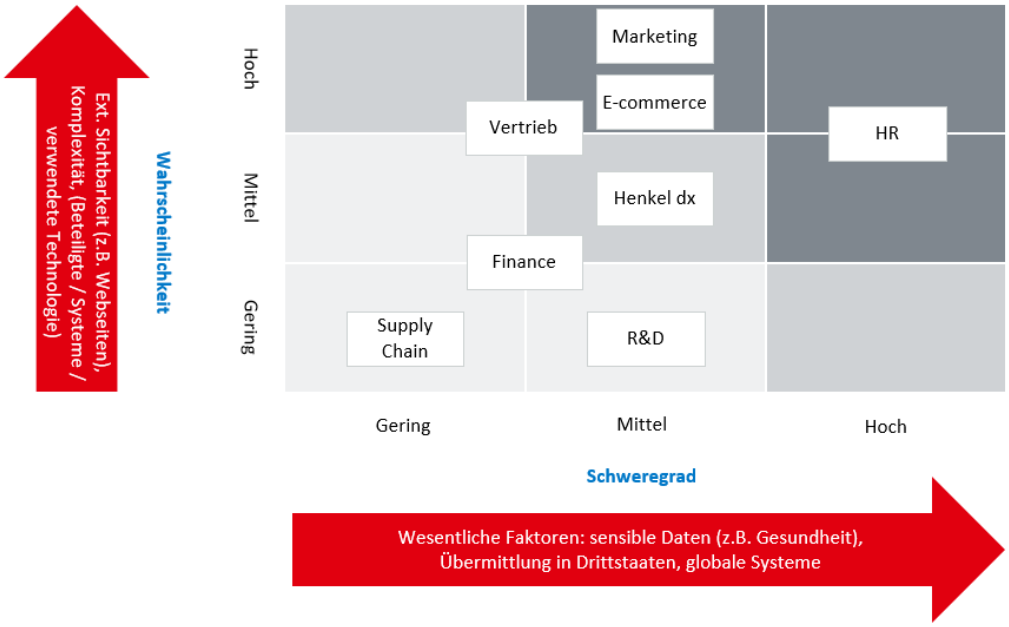
Rollen in Henkels Datenschutz-Organisation

Information Asset Owner	DSB	Henkel dx
Rechtmäßigkeit der Verarbeitung	Information & Beratung	Definition der TOMs
Erfüllung interner Vorgaben	Template-Verwaltung	IT Demand-Prozess
Überwachung & Dokumentation	Compliance-Überwachung	Datenschutz durch Technikgestaltung
	Anlaufstelle für Externe	Unterstützung DSB + Asset Owner

4. Datenschutz-Risiken

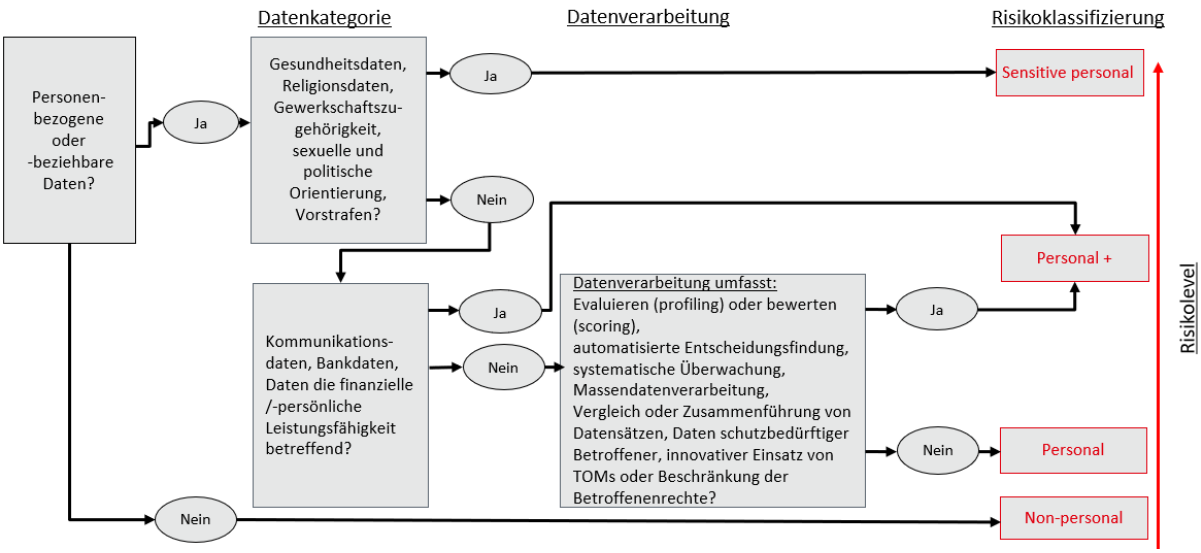
Datenschutz-Risiken müssen aus der Sicht der von der Datenverarbeitung betroffenen Personen („Dritte“) beurteilt werden. Der Schweregrad eines Risikos resultiert danach hauptsächlich aus der Kategorie der verarbeiteten Daten und den dabei eingesetzten Mitteln, während die Eintrittswahrscheinlichkeit eines Risikos im Wesentlichen durch das Gefahrpotential und die Komplexität der Verarbeitung bestimmt wird. Aus dieser Sichtweise ergibt sich bei abstrakter Betrachtung für Henkel eine Risikomatrix, die das Vorhandensein von Konsumenten- oder HR-Daten sowie den Grad der Digitalisierung eines bestimmten Bereichs als Hauptrisikofaktoren identifiziert (**Top-Down-Ansatz**).

Risikomatrix für die Verarbeitung personenbezogener Daten @Henkel



Das Risiko jedes einzelnen Information Assets (**Bottom-Up-Ansatz**) wird nach einer eigenen Methodik bewertet, die sowohl die verarbeiteten Datentypen als auch die konkrete Art der Verarbeitung berücksichtigt. Diese Methodik wird auch für Zwecke der Risikoklassifizierung gemäß Henkels IT-Sicherheitssystem verwendet. Damit kann festgestellt werden, ob die Verarbeitung personenbezogener Daten allein aufgrund des Umstands ein Risiko darstellt, dass überhaupt personenbezogene Daten verarbeitet werden ("*personal*"), ob spezielle Kategorien personenbezogener Daten nach DSGVO verarbeitet werden ("*sensitive personal*") oder ob bestimmte Datenkategorien und Risikofaktoren auf ein erhöhtes Risiko eines Information Assets bei der Datenverarbeitung ("*personal +*") hinweisen. **Datenschutz-Folgenabschätzungen** dienen der Beurteilung und Bewältigung eines als „hoch“ klassifizierten Risikos bei der Verarbeitung personenbezogener Daten durch Henkel.

Risikoklassifizierung



5. Datenschutz-Programm

Henkels DMS basiert auf **weltweit verbindlichen Corporate Standards** und, wo nötig, ergänzenden Richtlinien. Das Kernstück des DMS ist die EU-Datenschutzrichtlinie, in der alle Maßnahmen zur Einhaltung der DSGVO bei Henkel im Einzelnen dargelegt sind. Sie stützt sich auf eine starke IT-Sicherheits-Governance, wie sie im Corporate Standard Information Security (CSIS) festgeschrieben ist. Der CSIS wurde eigens an die zusätzlichen Anforderungen der DSGVO angepasst. EU-Datenschutzrichtlinie und CSIS können durch zusätzliche Richtlinien mit Geltung für bestimmte Länder oder Geschäftsbereiche ergänzt werden, um die Einhaltung der DSGVO umfassend sicherzustellen. So gibt beispielsweise die Richtlinie zu Datenschutzverstößen (Data Breach Policy) einen Rahmen für die effektive Identifizierung, das interne Management und die externe Meldung von **Datenschutzverstößen** vor.

Für jedes Henkel-Unternehmen, das entweder Verantwortlicher oder Auftragsverarbeiter von Information Assets ist, führt der jeweilige DSB / DSD ein Verzeichnis der relevanten Information Assets (Verzeichnis von Verarbeitungstätigkeiten) und implementiert einen Prozess, um Änderungen widerzuspiegeln und die Richtigkeit der Verfahrenseinträge sicherzustellen. Henkel setzt modernste **IT-Hilfsmittel** für die Verwaltung datenschutzrelevanter Managementaufgaben ein.

Für jedes einzelne Information Asset muss sichergestellt sein, dass die Verarbeitung unter Einhaltung aller geltenden Vorschriften geschieht. Information Asset Owner gewährleisten die **rechtmäßige Verarbeitung**, d.h. sie stellen sicher, dass entweder eine geltende gesetzliche Bestimmung oder die nachweisliche 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 (TOMs) 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 (einschließlich ständiger Änderungen und Projekte) 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. Der Standard der bei Henkel geltenden technischen und organisatorischen Datenschutz-Maßnahmen wird im Corporate Standard Information Security (CSIS) beschrieben und durch spezifische Vorgaben ergänzt, die sich z.B. aus Datenschutz-Folgenabschätzungen (DPIAs) ergeben.

Darüber hinaus stellen die Information Asset Owner den **betroffenen Personen transparente** Informationen über die Datenverarbeitung zur Verfügung, die es ihnen ermöglichen, ihre gesetzlich gewährten Rechte wirksam geltend zu machen. Der DSB / DSD als ausgewiesene Anlaufstelle für Externe hilft bei der Einrichtung eines wirksamen internen Beschwerdeverfahrens.

Information Asset Owner melden dem DSB / DSD die Einführung und Ersetzung von **Auftragsverarbeitern**. Auftragsverarbeiter werden regelmäßig auf ihre Fähigkeit zur Erbringung von Leistungen nach den Henkel-Standards und auf ihre Einhaltung geeigneter technischer und organisatorischer Maßnahmen hin überprüft; die Kontrolle erfolgt durch Befragungen, Untersuchungen oder andere geeignete Maßnahmen. Der DSB / DSD führt eine Übersicht über alle von dem jeweiligen Unternehmen beauftragten Auftragsverarbeiter.

Falls eine Verarbeitung **Datenübermittlungen an ein Drittland** mit sich bringt, melden Information Asset Owner solche Datentransfers; angemessene Schutzmaßnahmen sowie die Gewährleistung der Rechte Dritter, ihrer Durchsetzbarkeit und effektiver Rechtsmittel werden regelmäßig überprüft.

Als hochgradig internationaler Konzern ist Henkel auf interne internationale Datenübermittlungen angewiesen, um die Daten den entsprechenden Führungskräften in der Matrixorganisation des Konzerns zur Verfügung zu stellen. Henkel hat dazu ein System für Datenübermittlungen innerhalb des Unternehmens (Corporate Data Transfer Governance) für Information Assets definiert, die personenbezogene Daten an Henkel-Gesellschaften in Drittländern übertragen; zwischen den betreffenden Henkel-Gesellschaften bestehen Standardvertragsklauseln, die angemessene Schutzmaßnahmen, durchsetzbare Rechte der Betroffenen und wirksame Rechtsmittel für die Betroffenen vorsehen.

Datenschutzverstöße, die im Rahmen einer Untersuchung, allgemeiner Überwachungsprozesse oder auf andere Weise festgestellt werden, müssen dem jeweiligen DSB / DSD entsprechend den Vorgaben aus der Richtlinie zu Datenschutzverstößen und in der dort festgelegten Form unverzüglich gemeldet werden; eine 24-Stunden-Hotline ist eingerichtet, um Meldungen außerhalb der regulären Geschäftszeiten zu sammeln. Der DSB / DSD entscheidet, ob eine Meldung an die Datenschutzbehörden und/oder die von der Datenverletzung betroffenen Personen erforderlich ist, und gibt gegebenenfalls die Meldung heraus.

6. Datenschutz-Kommunikation

Datenschutz-Kommunikation erfolgt breit gestreut und reicht von allgemeinen Informationen im Intranet, auf Sharepoints, in Massen-E-Mails oder anderen Kanälen, die für alle Mitarbeitern

zugänglich oder an bestimmte Teile des Unternehmens adressiert sind, über zielorientierte Detailinformationen, die sich an einzelne Interessengruppenrichten bis hin zu Diskussionen mit Unternehmensorganen.

Datenschutzprozesse und -standards werden den Henkel-Mitarbeitern auf mehreren Ebenen vermittelt. **Schulungs**- und Kommunikationsmaßnahmen sind auf das Risikoprofil der Henkel-Geschäfte und die konkreten Aktivitäten der Adressaten zugeschnitten. Dazu gehören freiwillige und obligatorische e-Learnings ebenso wie persönliche Schulungen für Henkel-Mitarbeiter, aber auch die Einweisung neuer Mitarbeiter im Rahmen des Mitarbeiter-Onboardingprozesses. Die Weiterentwicklung des Datenschutz-Schulungsprogramms, insbesondere im Hinblick auf Schulungen für Information Asset Owner und andere interne Akteure auf Basis eines risikobasierten Ansatzes (z.B. HR, Konzern-IT und Marketing im Zusammenhang mit Konsumentendaten), ist oberste Priorität der Datenschutz-Organisation von Henkel.

Alle Mitarbeiter können sich in Datenschutzfragen angemessen beraten lassen. Sie sind aufgefordert, sich dazu jederzeit mit dem jeweiligen DSB / DSD, der Henkel-Rechtsabteilung oder dem jeweiligen Information Asset Owner in Verbindung zu setzen.

Die **Berichterstattung** zu Datenschutzthemen erfolgt regelmäßig durch den DSB / DSD an die Führungsgremien des jeweiligen Unternehmens sowie, bei wesentlichen Fragestellungen, in Budgetfragen oder zur Herbeiführung von Beschlüssen an das Data Protection Sounding Board. Alle DSBs / DSDs tragen zu der jährlichen Datenschutzberichterstattung bei, die von den lokalen Presidents an Henkels Compliance-Organisation übermittelt und dort für den Vorstand von Henkel aufbereitet wird. Darüber hinaus erstellt der Datenschutzbeauftragte von Henkel Deutschland einen jährlichen DSB-Bericht für die Führungsgremien von Henkel Deutschland.

7. Datenschutz-Überwachung und Verbesserung

Henkels Datenschutzbemühungen werden von Henkels Management ständig **überwacht**: von den verantwortlichen Führungsgremien und dem Data Protection Sounding Board, von den Information Asset Ownern hinsichtlich der Angemessenheit und Wirksamkeit der Datenschutzmaßnahmen ihres jeweiligen Information Asset sowie durch regelmäßige interne Kontrollen und Untersuchungen seitens Corporate Audit und des DSB / DSD, die die Wirksamkeit des DMS überprüfen. Die Datenschutzorganisation arbeitet eng mit Corporate Audit zusammen, das den überwiegenden Teil der internen Prüfungen bei Henkel auf Basis eines aus einem risikobasierten Prüfungsansatz abgeleiteten Untersuchungsplans vorbereitet und durchführt. Länder-Untersuchungen werden von der Datenschutzorganisation regelmäßig in ausgewählten Ländern durchgeführt, häufig mit Unterstützung externer Rechtsanwaltskanzleien.

Rechtliche Datenschutzangelegenheiten werden regelmäßig mit externen Rechtsberatern erörtert und abgestimmt sowie zu weiteren **Verbesserungen** und neuen regulatorischen Anforderungen beraten.

Henkels Datenschutzorganisation ist aktiv in externen Compliance-Foren vernetzt, was einen Austausch von Wissen und **Benchmarking von Prozessen** mit Fachkollegen ermöglicht. **Best Practices** werden identifiziert, umgesetzt und führen zu Verbesserungen der Datenschutzprozesse bei Henkel. Die **Identifizierung von Kontrolldefiziten** und die Umsetzung geeigneter Abhilfemaßnahmen (z.B. bei

der Behebung eines Datenschutzverstoßes) ist Teil der Datenschutzberichterstattung von Henkel, einschließlich der Entwicklung wichtiger Compliance-Initiativen, die über mehrere betroffene Unternehmen der Henkel-Gruppe hinweg umgesetzt werden.

Die kontinuierliche Verbesserung der Compliance-Organisation belegt Henkels Bestreben, die höchsten Standards bei der Durchführung von Datenverarbeitungen in ethisch und rechtlich einwandfreier Weise zu erfüllen.

Düsseldorf, 29. Oktober 2019

Henkel AG & Co. KGaA