STRÖER

DATENSCHUTZ

INHALTSVERZEICHNIS

01

Einleitung

Das Datenschutz-Management-System (DSMS) wurde für den Ströer 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 und dem Bundesdatenschutzgesetz) 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 – DS-GVO)“ ergriffen werden.

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

02

DATENSCHUTZ-REGELKREIS

Bei Kund:innen, Geschäftspartner:innen 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 Ströer SE & Co. KGaA und alle verbundenen Mehrheitsbeteiligungen, die dem räumlichen Anwendungsbereich der DS-GVO unterliegen. Sein Zweck ist es, die aus der DS-GVO abgeleiteten Prinzipien umzusetzen, wie sie in der Datenschutzrichtlinie von Ströer definiert sind und in Anlehnung an den Datenschutz-Regelkreis festgelegt sind:

2.1 Kultur

Ströer bekennt sich zum Grundrecht auf Datenschutz. Dieses Recht schützt den Einzelnen/die Einzelne vor Eingriffen in seine/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 Ströer 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 in geeigneter Weise zu schützen.

Der Ströer 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 Ströer sich auch im Rahmen der unternehmerischen Tätigkeit ausdrücklich zu seiner Datenverantwortung bekennt. Der verantwortungsvolle Umgang mit Daten im Interesse unserer Kund:innen, Beschäftigten und anderen Stakeholdern, wird daher auch in Zukunft zu unseren Zielen gehören und das Vertrauen in Ströer 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, Kund:innen, Geschäftspartner:innen, Lieferant:innen, Anteilseigner:innen usw.). Jeder Verstoß gegen Datenschutzgesetze birgt die Gefahr, unseren Ruf dauerhaft zu schädigen, und kann zu erheblichen Schäden und schwerwiegenden Folgen für den Ströer Konzern führen. Darüber hinaus können derartige Verstöße, ebenso wie für die beteiligten Beschäftigten, zu zivil- oder strafrechtlichen Sanktionen führen.

Bei Ströer ist ethisches und juristisch korrektes Handeln ein Kernprinzip, das bereits im „Code of Conduct“ zum Ausdruck kommt und selbstverständlich die Einhaltung des Datenschutzrechts umfasst. Dies wird unterstützt durch das grundlegende bei Ströer bestehende 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 Beschäftigten sowie unserer Kunden:innen und Geschäftspartner:innen zu respektieren.“

Stephan Schnitzler
Leiter Governance, Risk & Compliance

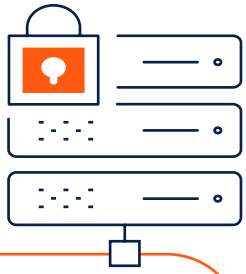
Darüber hinaus basiert die „Allgemeine Richtlinie zum Datenschutz“ von Ströer auf dem grundlegenden Verständnis, dass jede Verarbeitung personenbezogener Daten in Übereinstimmung mit den geltenden Datenschutzgesetzen, insbesondere der Datenschutz-Grundverordnung (DS-GVO) erfolgen muss.

Unsere Datenschutzkultur wird durch die folgende Erklärung des Konzernvorstandes zum Datenschutz veranschaulicht:

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

Henning Gieseke
Vorstand

DATENSCHUTZ IST FÜR STRÖER AUS DREI GRÜNDEN BESONDERS WICHTIG:



ZUKUNFT

Die Nutzung von Daten ist für viele Bereiche unserer Aktivitäten essenziell. Hier wollen wir weitere Entwicklungen positiv begleiten und die Chancen, die aus einem wachsenden Datenangebot entstehen, auch weiterhin positiv nutzen. Das ist nur möglich, wenn wir „Daten“ auch angemessen schützen.

VERTRAUEN

Sowohl unsere Kund:innen, Nutzer:innen wie unsere Partner:innen und natürlich unsere Beschäftigten müssen darauf vertrauen können, dass ihre Daten und ggf. die Daten ihrer Kund:innen, Nutzer:innen und Partner:innen bei uns sicher sind, um diese mit uns zu teilen und mit uns zusammen zu arbeiten.

COMPLIANCE

Unternehmenserfolg und persönlicher Erfolg können nur in einem Umfeld der Rechtstreue erreicht und gesichert werden. Die Einhaltung der rechtlichen Vorgaben ist für uns eine nicht verhandelbare Grundvoraussetzung unserer Aktivitäten. Die Basis hierfür ist unser „Code of Conduct“.

2.2 Ziele

Die Rechtspflichten aus den jeweiligen Datenschutzbestimmungen – insbesondere aus der Datenschutz-Grundverordnung (DS-GVO) 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.

Jede/r Einzelne bei Ströer 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 Ströer werden mit personenbezogenen Daten unserer Kund:innen, Geschäftspartner:innen und ihren Kolleg:innen sorgfältig und vertraulich umgehen und das geltende Recht beachten.

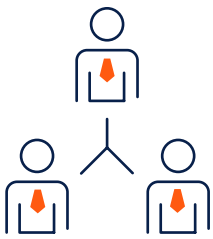
Jede/r, die/der im Ströer Konzern für eine Aktivität, die personenbezogene Daten betrifft, verantwortlich ist, organisiert die Verarbeitung (Erhebung, Nutzung, Speicherung, Löschung etc.) personenbezogener Daten so, dass die Einhaltung geltenden Rechts gewährleistet wird.

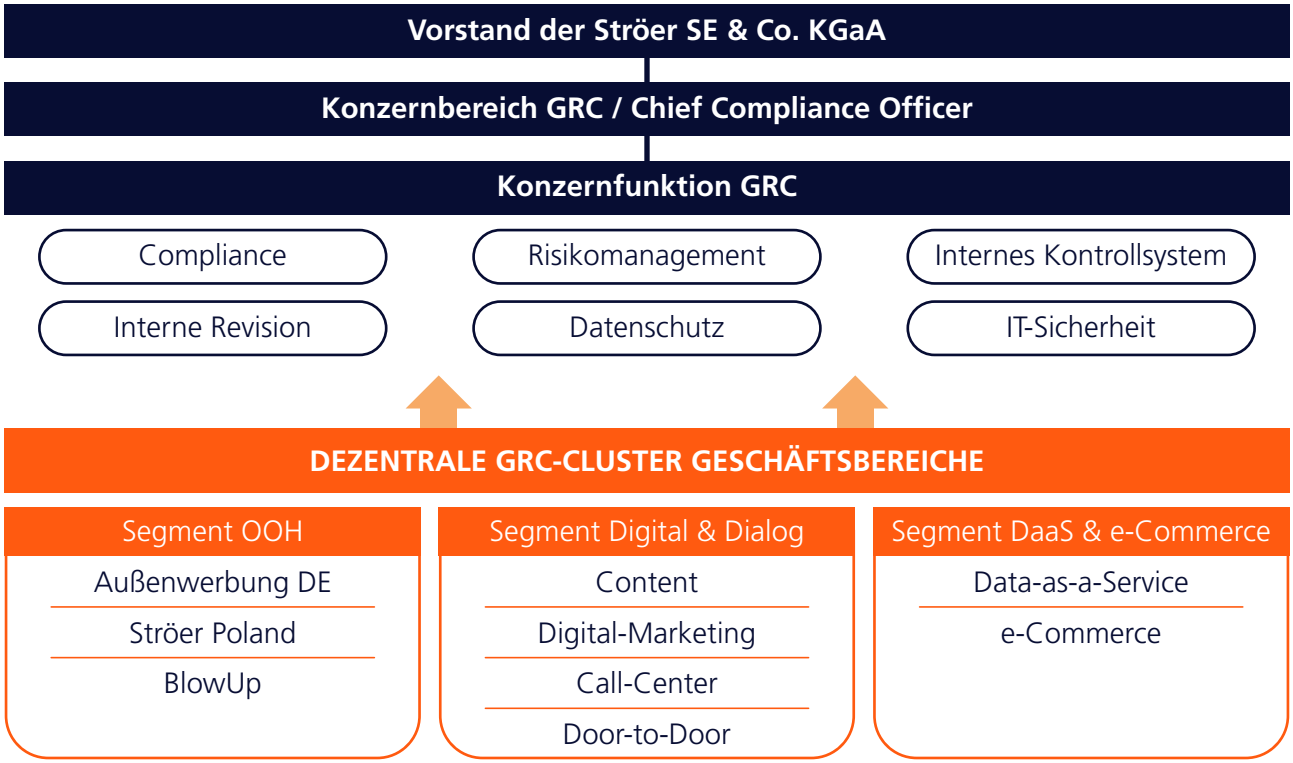
Diese Erwartungen übertragen wir über unseren Verhaltenscodex für Lieferant:innen und Geschäftspartner:innen auch auf unsere Lieferant:innen und Geschäftspartner:innen.

DIE PFLICHTEN BETREFFEN ALSO JEDEN BEI STRÖER!

2.3 Organisation

Der Ströer Konzern besteht aus der Ströer SE & Co. KGaA als Konzernmutter und zahlreichen Tochtergesellschaften. Diese Konzerngesellschaften sind in der „Governance, Risk & Compliance“-Organisation in „Cluster“ gegliedert.



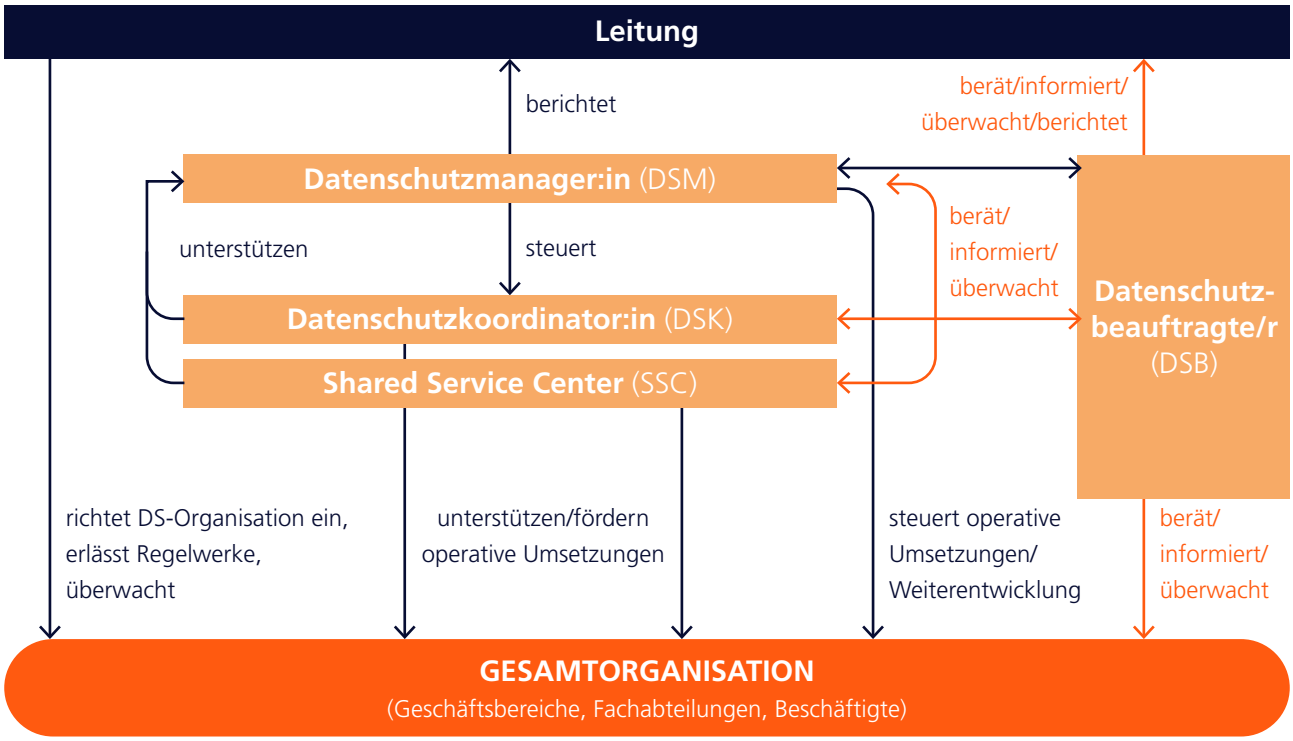


Innerhalb der dezentralen Cluster muss die Einhaltung der Datenschutzanforderungen hinsichtlich jeder einzelnen Verarbeitung von personenbezogenen Daten („Verarbeitungstätigkeit“), auf Gesellschaftsebene sichergestellt sein.

Der Vorstand trägt die Gesamtverantwortung für die Einhaltung der geltenden Gesetze und internen Standards. Ströer hat ein interdisziplinäres „GRC-Komitee“ unter dem Vorsitz des CFO der Ströer SE & Co. KGaA eingerichtet, das für die Mittelausstattung sowie für die Steuerung und Überwachung der Datenschutzorganisation zuständig ist.

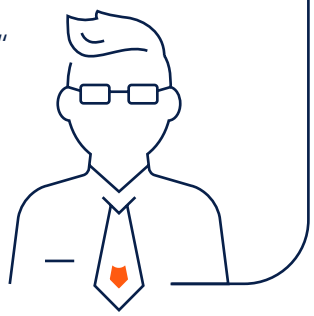
Soweit gesetzlich vorgesehen, ernennt jede Konzerngesellschaft eine/n fachkundige/n Datenschutzbeauftragte/n (DSB), die/der die in der DS-GVO definierten Aufgaben wahrnimmt, insbesondere ihre/seine Funktion als Ansprechpartner:in für Betroffene.

Für jedes Cluster ist zudem ein/e Datenschutzmanager/in (DSM) ernannt. Die/der DSM ist über die gesetzlichen Pflichten eines DSB hinaus für die Einhaltung datenschutzrechtlicher Vorgaben zuständig. Die Leitung delegiert an die/den DSM die Wahrnehmung ihrer datenschutzrechtlichen Pflichten. Die/der DSM wird durch Datenschutzkoordinatoren (DSK) bei der Umsetzung ihrer/seiner Aufgaben unterstützt und kann diese soweit erforderlich fachlich anweisen.



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 geeigneter Dokumentation zum Nachweis der Einhaltung der DS-GVO etc.) ist Aufgabe der „Prozess-/Verarbeitungsverantwortlichen", „Product- und Contract-Ownern". Sie verfügen über ausreichendes Wissen und die erforderlichen Ressourcen zur Erfüllung ihrer Aufgaben sowie über die Befugnis, Datenverarbeitungen zu ändern oder auszusetzen.

Die Group IT und das Group Information Security Office (GISO) unterstützen dabei, technische und organisatorische Maßnahmen in Übereinstimmung mit der DS-GVO 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.

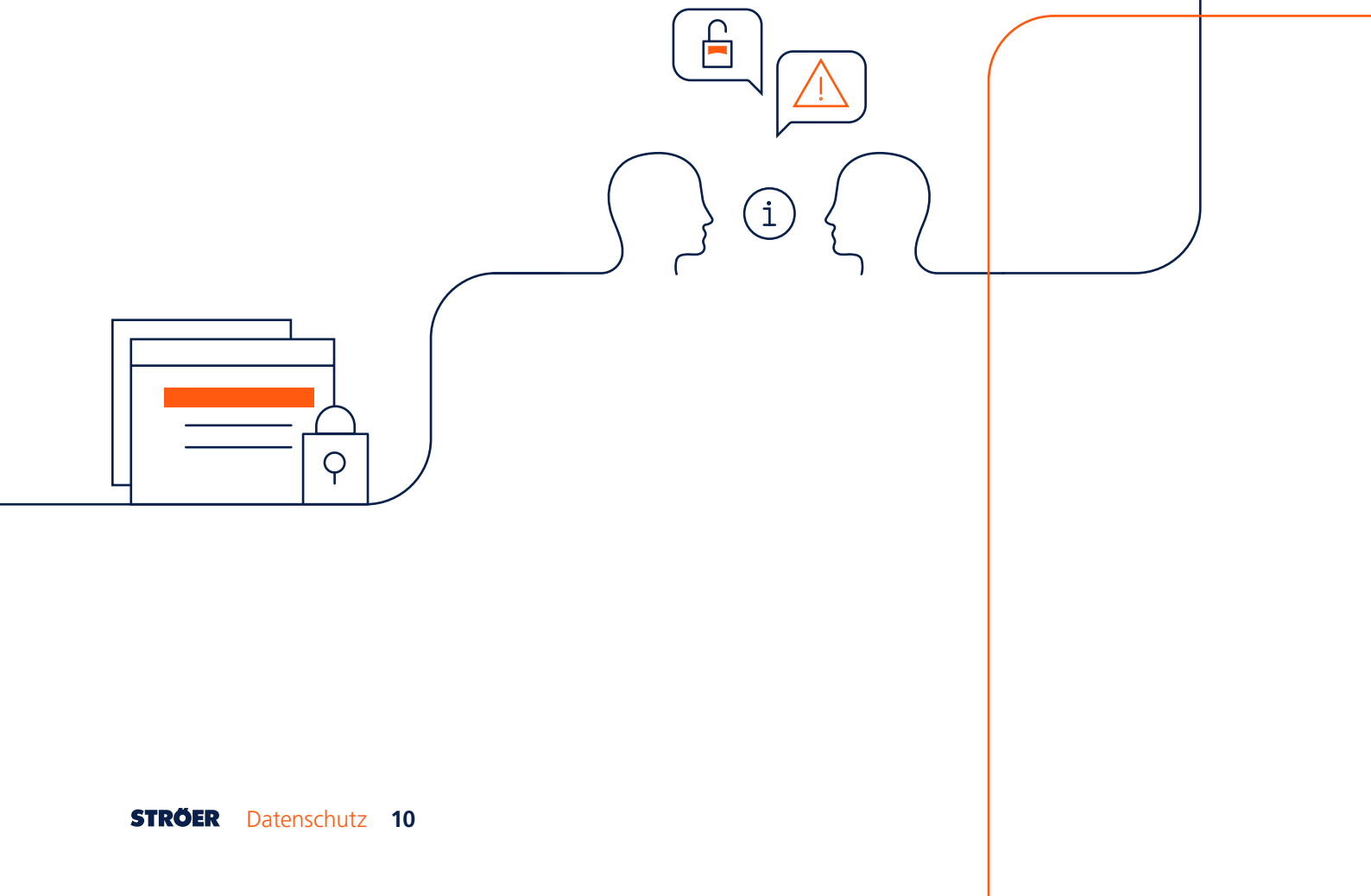


2.4 Risiken

Im Rahmen eines integrierten Corporate-Governance-Ansatzes betreibt der Ströer 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/r“) 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 verarbeitet werden oder ob bestimmte Datenkategorien und Risikofaktoren auf ein erhöhtes Risiko einer Verarbeitungstätigkeit bei der Datenverarbeitung hinweisen.



2.5 Programm

Das DSMS basiert auf weltweit verbindlichen Konzerngrundsätzen und ergänzenden Richtlinien. Das Kernstück des DSMS sind die „Corporate Privacy Principles“ (CPP). Ziel dieser CPP ist es, im Konzern organisatorische Mindeststandards und einen einheitlichen Rahmen für die Verarbeitung und den Schutz personenbezogener Daten zu schaffen und Schäden von Ströer abzuwenden. Die CPP können durch zusätzliche Richtlinien mit Geltung für bestimmte Länder oder Geschäftsbereiche ergänzt werden, um die Einhaltung der gesetzlichen Datenschutzanforderungen umfassend sicherzustellen. Unser Datenschutz-Programm umfasst insbesondere:

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

So gibt beispielsweise die Richtlinie zu Datenschutzverstößen („Incident Response Plan“) einen 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 der/m jeweiligen DSM entsprechend den Vorgaben aus der Richtlinie und in der dort festgelegten Form unverzüglich gemeldet werden. Die/der DSB berät die/den Verantwortliche/n bei der Entscheidung, ob eine Meldung an die Datenschutzbehörden und/oder die von der Datenverletzung betroffenen Personen erforderlich ist, und gibt gegebenenfalls die Meldung heraus.

Unsere „Allgemeine Richtlinie zum Datenschutz“ verpflichtet jede Gesellschaft im Konzern ein Verarbeitungsverzeichnis der relevanten Verarbeitungstätigkeiten zu führen und einen Prozess zu implementieren, um Änderungen zu berücksichtigen und die Richtigkeit und Vollständigkeit der Verarbeitungstätigkeiten sicherzustellen. Wir setzen dabei eine marktführende Datenschutz-Management-Software für die Verwaltung solcher datenschutzrelevanten Aufgaben ein. Für jede einzelne Verarbeitungstätigkeit muss zudem sichergestellt sein, dass die Verarbeitung unter Einhaltung aller geltenden Vorschriften geschieht. Sogenannte „Prozess-/Verarbeitungsverantwortliche“ 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 (TOM) 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.

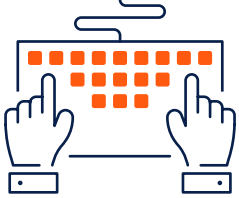
Darüber hinaus stellen die „Prozess-/Verarbeitungsverantwortlichen“ den betroffenen Personen transparente Informationen (sog. „Datenschutzhinweise“) über die Datenverarbeitung zur Verfügung, die es ihnen ermöglichen, ihre gesetzlich gewährten Betroffenenrechte wirksam geltend zu machen.

Die Einführung und Ersetzung von Auftragsverarbeitern werden durch „Contract-Owner“ an die/den DSK gemeldet. Die Auftragsverarbeiter werden regelmäßig auf ihre Zuverlässigkeit zur

Erbringung von Leistungen auf die Einhaltung geeigneter technischer und organisatorischer Maßnahmen hin überprüft; die Kontrolle erfolgt z. B. durch Interviews, Dokumenten-Reviews, Untersuchungen vor Ort oder andere geeignete Maßnahmen. Die/der DSM führt eine Übersicht über alle von der jeweiligen Gesellschaft in seinem Cluster beauftragten Auftragsverarbeiter:innen.

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

Als Konzern ist Ströer auf interne internationale Datenübermittlungen angewiesen, um die Daten den entsprechenden Verarbeiter:innen zur Verfügung zu stellen. Wir haben dazu Anforderungen für Datenübermittlungen innerhalb des Konzerns definiert. Zwischen den betreffenden Tochtergesellschaften bestehen z. B. Standardvertragsklauseln, die angemessene Schutzmaßnahmen, durchsetzbare Rechte der Betroffenen und wirksame Rechtsmittel für die Betroffenen vorsehen.



2.6 Kommunikation

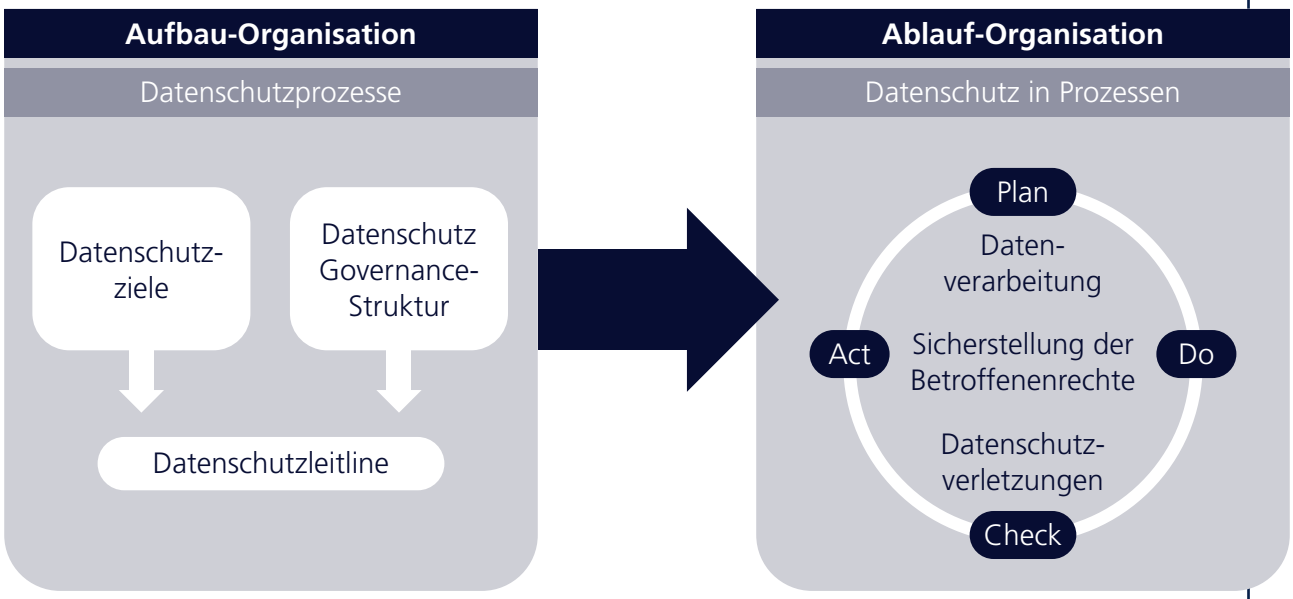
Kommunikation bzw. Sensibilisierung im Datenschutz erfolgt breit gestreut und reicht von allgemeinen Informationen im internen Ströernetz, auf Sharepoints, in Newslettern oder anderen (Teams-)Community-Kanälen, die für alle Beschäftigten zugänglich oder an bestimmte Fachbereiche adressiert sind, über zielorientierte Detailinformationen im „Datenschutzkoffer“, die sich an einzelne Interessengruppen richten bis hin zu Diskussionen im Kreis der Datenschutz-Akteure. Jährlich berichtet Ströer über seine Fortschritte im Datenschutz zudem im Rahmen des Nachhaltigkeitsberichts des Konzerns.

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 DS-GVO als „eLearning“, die für alle Beschäftigten im Ströer Konzern verpflichtend ist. Darüber hinaus werden freiwillige eLearnings ebenso wie z. B. persönliche Schulungen für „Entscheider:innen im Datenschutz“, aber auch die Unterrichtung neuer Beschäftigter im Rahmen des Onboardings angeboten. Das Verständnis, dass Datenschutz in der Verantwortung aller liegt, wurde auch durch die „Vertraulichkeitsverpflichtung im Datenschutz“ gestärkt, über die alle Beschäftigten vor Beginn ihrer Tätigkeit unterrichtet werden. Alle Beschäftigten können sich in Datenschutzfragen angemessen beraten lassen. Ihnen steht es frei, sich dazu jederzeit mit den jeweiligen Datenschutz-Akteuren:innen 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 DSM fest vorgesehen.

2.7 Überwachung und Verbesserung

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



Das DSMS unterstützt Ströer dabei, Maßnahmen zur Einhaltung der Datenschutzbestimmungen strukturiert zu planen, umzusetzen und regelmäßig zu überprüfen. Die in der Datenschutzorganisation tätigen Datenschutz-Akteur:innen 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 Wirksamkeit überprüft. Die Datenschutzorganisation arbeitet eng mit der internen Revision zusammen, die den überwiegenden Teil der internen Prüfungen im Ströer Konzern auf Basis eines aus einem risikobasierten Prüfungsansatz abgeleiteten Prüfungsplans vorbereitet und durchführt.

Rechtliche Datenschutzangelegenheiten werden mit internen und externen Rechtsberater:innen 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 Benchmarking von Prozessen mit Fachkolleg:innen ermöglicht. Best Practices werden identifiziert, umgesetzt und führen zu Verbesserungen der Datenschutzprozesse bei Ströer. Die Identifizierung von Kontrolldefiziten und die Umsetzung geeigneter Maßnahmen ist Teil der Datenschutzberichterstattung von Ströer, einschließlich der Entwicklung wichtiger Compliance-Aktivitäten, die über mehrere Gesellschaften im Konzern hinweg umgesetzt werden.

Ströer SE & Co. KGaA
Ströer-Allee 1
50999 Köln

ANSPRECHPARTNER

Stephan Schnitzler
Governance, Risk & Compliance

Stephan Kuchenbuch
Konzerndatenschutz

Stand: November 2022