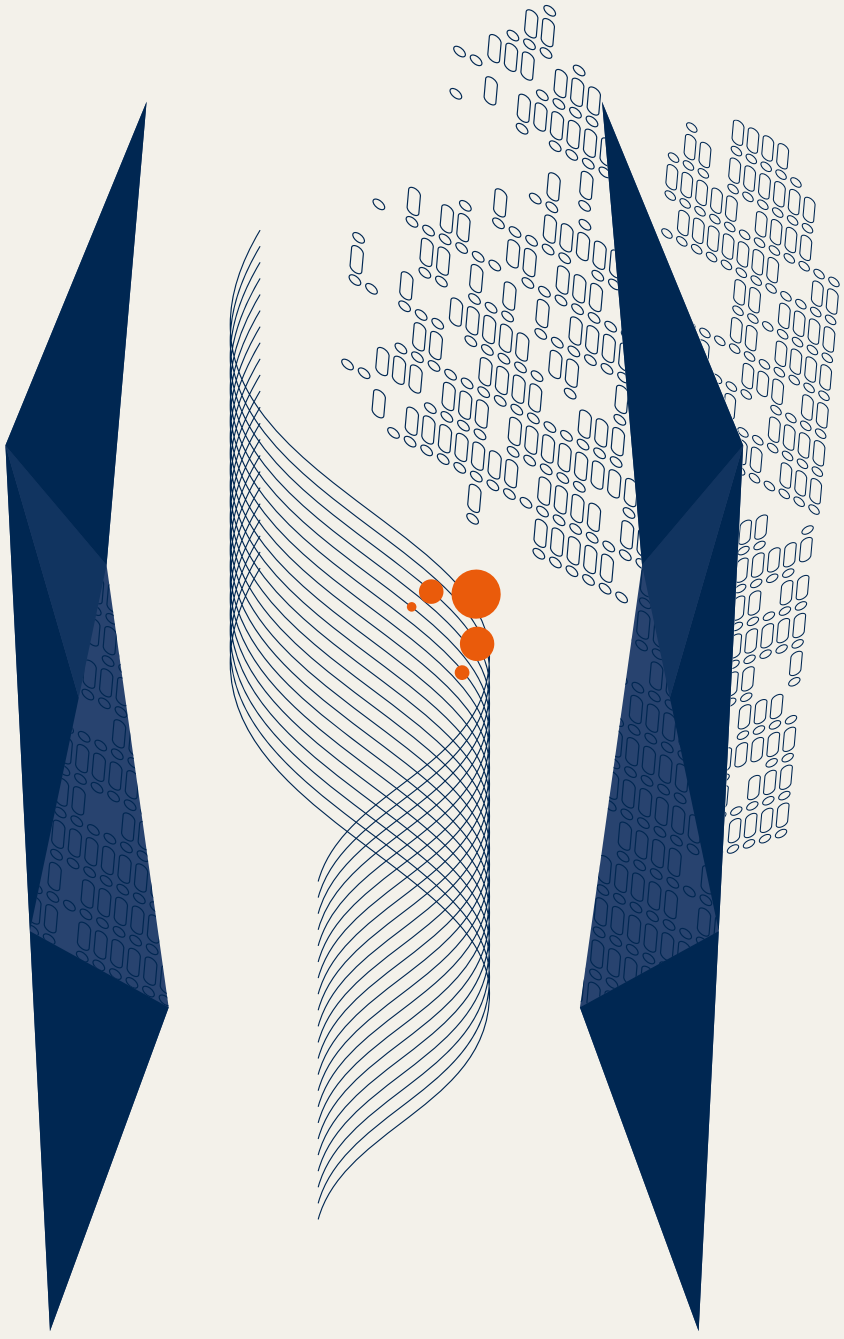
Digitalisierung & Compliance

Compliance-Studie 2021



In Kooperation mit:

Technische Universität München

Noerr

Vorwort

Zwar hat der Bundestag den bereits 2020 verabschiedeten Gesetzentwurf des Bundeskabinetts zum Unternehmenssanktionsrecht auf der Zielgeraden noch gestoppt. Doch auch so sind die Anforderungen an Unternehmer und Compliance-Verantwortliche in den vergangenen Monaten gestiegen. Zahlreiche neue Gesetze und Vorschriften auf Bundes- und Europa-Ebene sind in Kraft getreten und bedeuten für die Verantwortlichen zusätzliche Arbeit.

Vor diesem Hintergrund freuen wir uns, dass wir Ihnen unsere aktuelle Compliance-Studie präsentieren können. Wir haben dazu erneut 300 Interviews mit Führungskräften von privatwirtschaftlichen Unternehmen der ersten und zweiten Entscheidungsebene geführt und die Ergebnisse für Sie kompakt zusammengefasst – sicherlich werden Sie beim Lesen auf viele interessante Details stoßen.

Wenn Sie Anmerkungen zu unserer Studie haben oder Ideen und Anstöße für künftige Untersuchungen geben möchten, kommen Sie gerne auf uns zu. Wir freuen uns auf Ihr Feedback!

Prof. Dr. Peter Bräutigam

Dr. Julia Sophia Habbe

Prof. Dr. Dirk Heckmann

Inhalt

Executive Summary

Die fortschreitende Digitalisierung stellt Unternehmen auch unter Compliance-Gesichtspunkten vor organisatorische Herausforderungen. Neue Technologien schaffen neue Compliance-Risiken. Die Geschäftsleitung ist dabei verantwortlich, diese Risiken zu ermitteln und innerhalb des Unternehmens richtig zu allokieren.

Oftmals sehen sich die befragten Unternehmen jedoch nicht hinreichend digital aufgestellt, wobei insbesondere im Bereich Compliance dringender Handlungsbedarf zu bestehen scheint. Dies gilt umso mehr in kleineren Unternehmen, die ihr Digitalisierungsniveau eher niedriger einschätzen als große. Weiterhin fehlen vielen spezielle Positionen zur Überwachung digitaler Compliance-Risiken und oftmals entsprechende technische Expertise.

Der weit überwiegende Teil hat sich zwar mit den rechtlichen Risiken der Digitalisierung auseinandergesetzt. Bei vielen haben sich diese dennoch realisiert. Gerade beim Einsatz neuer Technologien werden rechtliche Risiken unterschätzt. Auch beim Einsatz von Compliance-Tools scheint es oft an Risikobewusstsein zu fehlen.

Die Covid-19-Pandemie hat den Einsatz digitaler Arbeitsmittel weiter befördert. Die Befragung zeigt, dass viele Unternehmen deren Einsatz unter Compliance-Gesichtspunkten für bedenklich halten. Demgegenüber scheint die Covid-19-Pandemie kaum zu Lockerungen von Compliance-Richtlinien geführt zu haben.

Die Organisation der digitalen Compliance ist eine Managementaufgabe

Das Management ist dafür verantwortlich, digitale Compliance-Risiken zu erkennen und innerhalb des Unternehmens richtig zu allokieren. Die Antworten unserer Befragung legen indes nahe, dass nur wenige Unternehmen die Geschäftsleitung für digitale Risiken verantwortlich sehen.

Hier besteht dringender Handlungsbedarf. Die Geschäftsleitung hat geeignete Maßnahmen zur Schaffung und Erhaltung der Cybersicherheit des Unternehmens zu ergreifen. Die Zuständigkeit für die digitale Infrastruktur wird nach den Rückmeldungen der befragten Unternehmen indes oftmals verkannt.

Viele Unternehmen sehen sich nicht als ausreichend digital aufgestellt

Damit Unternehmen die wachsenden Herausforderungen der Digitalisierung meistern können, müssen sie über entsprechende Strukturen und Prozesse verfügen. Der Großteil der befragten Führungskräfte sieht insofern Nachholbedarf und bewertet den digitalen Reifegrad des eigenen Unternehmens als gering bis mittel. In den einzelnen Unternehmensbereichen schneidet die Compliance-Abteilung am schlechtesten ab. Hier sieht lediglich ein Drittel einen hohen bis sehr hohen digitalen Reifegrad.

Spezielle Positionen für digitale Compliance-Risiken fehlen oft; jedenfalls technische Expertise unterrepräsentiert

Diese Eigeneinschätzung eines begrenzten digitalen Reifegrads spiegelt sich auch in organisatorischer Hinsicht wider. Spezielle Positionen zur Behandlung digitaler Compliance-Risiken sind in vielen Unternehmen nicht etabliert. Rund **70 %** geben an, dass es keine besondere Position für digitale Compliance Risiken gibt.

Beim beruflichen Hintergrund der Compliance-Beauftragten zeigt sich zudem ein uneinheitliches Bild. Dies mag auch daran liegen, dass es keine belastbaren Daten zu der Frage gibt, welche Kompetenzen in diesem Feld notwendig sind. Nach wie vor verfügt der überwiegende Teil der mit Compliance-Aufgaben betrauten Mitarbeiter über ein wirtschafts-

oder rechtswissenschaftliches Studium. Spezifische technische Expertise scheint hingegen unterrepräsentiert zu sein. Nur etwas mehr als ein Viertel der Compliance-Beauftragten hat einen Technik- oder Informatik-Hintergrund.

In rund der Hälfte der Unternehmen haben sich digitale Rechtsrisiken bereits realisiert

Digitale Rechtsrisiken haben in den vergangenen Jahren zugenommen. Dieser Befund steht in Einklang mit den Rückmeldungen der befragten Entscheidungsträger.

Zwar hat sich der weit überwiegende Teil der befragten Unternehmen mit den rechtlichen Risiken der Digitalisierung auseinandergesetzt. So haben viele beispielsweise ihre Risikoexposition in SWOT-Analysen ermittelt. Dennoch haben sich in rund der Hälfte der Studienteilnehmer bereits rechtliche Risiken realisiert, zum Beispiel in Form von Hacking-Angriffen oder Datenschutzrechtsverstößen.

Gerade bei neueren Technologien werden die rechtlichen Risiken unterschätzt

Besonders bei neueren Technologien zeigt sich, dass Unternehmen die damit zusammenhängenden rechtlichen Risiken vielfach unterschätzten. Im Bereich Cloud-Computing, künstlicher Intelligenz und Big-Data-Analysen bewertet etwa die Hälfte die rechtlichen Risiken als gering. Dies steht in einem Spannungsfeld zu den stetig wachsenden regulatorischen Anforderungen, etwa beim Datenschutz oder in der IT-Sicherheit.

In seiner Schrems-II-Entscheidung vom 16. Juli 2020 hatte der EuGH den „EU-US Privacy Shield" für ungültig erklärt und damit rechtskonforme Datentransfers in die USA erheblich erschwert. Allerdings werden viele Cloud-Services gerade von US-amerikanischen Providern bereitgestellt oder gehostet. Da die datenschutzkonforme Übermittlung personenbezogener Daten in Drittstaaten im besonderen Fokus der Aufsichtsbehörden steht, drohen hier hohe Bußgelder und Schadensersatzforderungen betroffener Dritter.

Auch im IT-Sicherheitsrecht steigen die Anforderungen. Mit dem am 23. April 2021 beschlossenen „IT-Sicherheitsgesetz 2.0" hat sich der Deutsche Bundestag vom sektorspezifischen Ansatz verabschiedet und die IT-sicherheitsrechtlichen Pflichten auf „Unternehmen im besonderen öffentlichen Interesse" ausgeweitet. Zudem müssen „Betreiber kritischer Infrastrukturen" ab dem 01. Mai 2023 „Systeme zur Angriffserkennung" verwenden. Bei Verstößen drohen Bußgelder in Höhe von bis zu 20 Millionen Euro.

Die regulatorischen Anforderungen steigen auch im Hinblick auf künstliche Intelligenz und Big-Data-Analysen. Am 21. April 2021 hat die Europäische Kommission den Entwurf einer „KI-Verordnung" vorgelegt. Der Vorschlag folgt einem risikobasierten Ansatz und stellt teilweise hohe Anforderungen an den technischen Aufbau und Einsatz von KI. Bei Verstößen gegen die Verbotstatbestände sieht der Verordnungsentwurf Bußgelder von bis zu 30 Millionen Euro beziehungsweise **6 %** des weltweiten Jahresumsatzes vor.

Informations- und Prozesstools weit verbreitet, Risikobewusstsein gering

Vor allem Informations- und Prozesstools bilden nach den erhaltenen Rückmeldungen den Großteil der vorhandenen Compliance-Tools. Hierzu zählen beispielsweise Analyse- und Monitoring-Tools sowie E-Learning-Plattformen. Dabei setzt rund ein Drittel der Unternehmen eigens entwickelte Tools ein.

Der Umstand, dass der Einsatz solcher Tools selbst mit Compliance-Risiken einhergehen kann, scheint dem Großteil der Befragten hingegen nicht bewusst zu sein. Nur **32 %** der Unternehmen mit Sitz im Ausland und **16 %** der Unternehmen mit Sitz im Inland sehen im Einsatz von Compliance-Tools Risiken.

Einsatz digitaler Arbeitsmittel trotz Compliance-Bedenken verbreitet

Auch wenn Unternehmen dazu tendieren, die rechtlichen Gefahren neuerer Technologien generell zu unterschätzen, ist zumindest hinsichtlich der im Unternehmen eingesetzten digitalen Arbeitsmittel

ein gewisses Bewusstsein für Compliance-Risiken vorhanden. So gibt etwa ein Fünftel der befragten Entscheidungsträger an, dass Videokonferenzen, Sharepoint-Systeme oder Collaboration-Tools mit hohen bis sehr hohen Compliance- und Datenschutzrisiken einhergehen. Dennoch sind digitale Arbeitsmittel aus dem heutigen Arbeitsalltag nicht mehr wegzudenken. Die Covid-19-Pandemie hat ihren Einsatz in der Breite weiter befördert.

Kaum Lockerungen von Compliance-Richtlinien während der Covid-19-Pandemie

Während der Covid-19-Pandemie scheinen nur wenige Unternehmen ihre Compliance-Richtlinien gelockert zu haben. Rund zwei Drittel der Befragten befinden, dass im Branchenumfeld Compliance-Richtlinien weder ausgesetzt noch gelockert worden seien. Dies mag verwundern, müssen doch viele Unternehmen flexible Lösungen finden, um den Auswirkungen der Covid-19-Pandemie zu begegnen, beispielsweise durch Homeoffice. Die Dunkelziffer der internen Lockerungen dürfte daher weitaus höher sein.

1. Compliance-Organisation im digitalen Unternehmensumfeld

Compliance in Unternehmen befindet sich im Wandel. Sie wird insbesondere durch digitale Technologien und die zunehmende Digitalisierung von Unternehmensprozessen vor neue Herausforderungen gestellt.

Neue Technologien verändern den Arbeitsalltag der Beschäftigten und zwingen Unternehmen, damit verbundene digitale Risiken zu erkennen, zu bewerten und zu managen. Gleichzeitig sind viele Unternehmen digitalen Risiken stärker exponiert; dies zeigt sich etwa an der zunehmenden Bedrohung durch Cyberangriffe. Um den digitalen Herausforderungen angemessen zu begegnen, müssen Unternehmen entsprechende präventive und reaktive Compliance-Maßnahmen ergreifen. Dabei ist es Aufgabe des Managements, diese Maßnahmen zu organisieren und zu überwachen.

Viele der befragten Entscheidungsträger[1] sehen ihr Unternehmen als nicht ausreichend digital aufgestellt. Zudem scheinen oftmals spezielle Positionen zum Umgang mit digitalen Compliance-Risiken zu fehlen oder aber die notwendige technische Expertise unterrepräsentiert zu sein.

1.1 Digitale Compliance als Managementaufgabe

Die Organisation der digitalen Compliance ist eine Managementaufgabe.

Die Geschäftsleitung ist dafür zuständig, durch geeignete Maßnahmen die digitale Compliance ihres Unternehmens zu organisieren und aufrechtzuerhalten. So haben Vorstandsmitglieder die Sorgfalt eines ordentlichen und gewissenhaften Geschäftsleiters anzuwenden (§ 93 Abs. 1 S. 1 AktG). Der Geschäftsführer einer GmbH ist gleichermaßen verpflichtet (§ 43 Abs. 1 GmbHG). Die konkrete Ausgestaltung der Compliance-Organisation liegt dabei im Ermessen der Geschäftsleitung und hat sich insbesondere an Art, Größe, wirtschaftlicher und finanzieller Lage des Unternehmens sowie der personellen Aufstellung der Geschäftsleitung zu orientieren. Auch wenn eine Pflichtendelegation grundsätzlich möglich und oftmals sinnvoll ist, verbleibt die letztendliche Verantwortung bei der Geschäftsleitung. Diese sollte zumindest über entsprechende Berichte in der Lage sein, sich ein Bild über die Situation in ihrem Unternehmen zu machen.

Im Falle einer konkreten Gefährdung, wie beispielsweise eines Cyberangriffs, verdichten sich die Überwachungspflichten der Geschäftsleitung. Bei Verdachtsmomenten sind unverzüglich alle erforderlichen Maßnahmen zu ergreifen, um das Schadensrisiko für das Unternehmen zu begrenzen. Anschließend sind sichtbar gewordene Schwachstellen im Compliance-System zu schließen.

Die Befragten verorten die Verantwortung für digitale Risiken sehr unterschiedlich.[2] Sofern keine spezielle Position für digitale Compliance-Risiken existiert, ist die **IT-Abteilung** in den weit überwiegenden Fällen in die Verantwortung für digitale Risiken eingebunden (74 %). In Unternehmen mit Stammsitz in Deutschland ist dies sogar noch etwas häufiger der Fall als in Unternehmen mit ausländischem Mutterkonzern (75 % versus 67 %). Gleiches gilt für kleinere Unternehmen mit weniger als 1.000 Beschäftigten. Hier ist die IT-Abteilung in fast vier von fünf der betreffenden Unternehmen involviert (78 %).

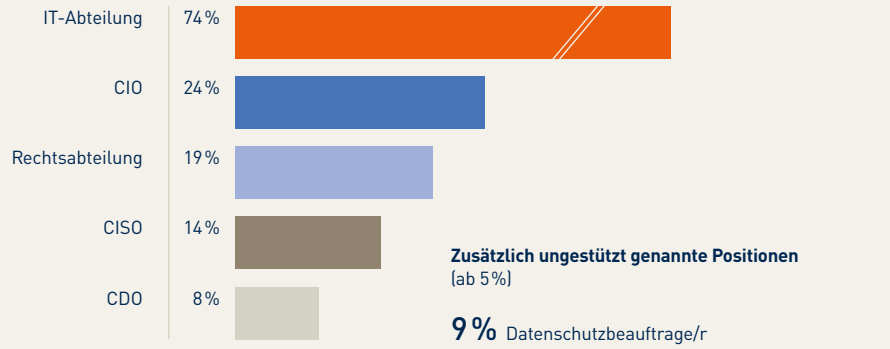
---

[1] Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

[2] Methodischer Hinweis: Da die dargestellten Anteilswerte auf ganze Zahlen gerundet sind, kann es vorkommen, dass sie sich nicht zu 100 % aufsummieren. Aus demselben Grund können durch Addition zusammengefasste Kategorien (zum Beispiel „Top-Two-Werte" wie „sehr zufrieden" und „eher zufrieden") von der Summe der dargestellten Einzelkategorien abweichen. Bei Fragen mit mehreren möglichen Antwortoptionen können die aufaddierten Nennungen 100 % überschreiten. Die Prozentsätze im Text beziehen sich auf die Ergebnisse der Umfrage. Besonders wichtige Resultate der Studie sind zudem grafisch dargestellt.

Unternehmenspositionen mit Verantwortung für digitale Risiken

Auch wenn die Verantwortlichkeiten teils sehr unterschiedlich aufgehängt sind, ist die IT-Abteilung in der Regel involviert



Zusätzlich ungestützt genannte Positionen
(ab 5 %)

9 % Datenschutzbeauftrage/r
8 % Positionen in Finance/Controlling
6 % Geschäftsführung, Vorstand
5 % Positionen innerhalb der Compliance-Abteilung

Frage: Auf welche Positionen ist der Bereich digitale Risiken in Ihrem Unternehmen verteilt?

Basis: Unternehmen ohne spezielle Position für digitale Compliance-Risiken; Mehrfachnennungen möglich; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Die Rechtsabteilung spielt vor allem in größeren Unternehmen sowie in Unternehmen, deren Mutterkonzern im Ausland sitzt, im Bereich digitaler Risiken eine wichtige Rolle. Während die Rechtsabteilung in mehr als jedem vierten befragten Unternehmen mit mindestens 1.000 Beschäftigten (27 %) oder mit Sitz im Ausland (28 %) für digitale Risiken zuständig ist, binden nur **12 %** der kleineren Unternehmen beziehungsweise nur **17 %** der Unternehmen mit Stammsitz in Deutschland bei diesem Thema die Rechtsabteilung ein.

Auch im Übrigen zeigt sich bei speziellen Stellen für digitale Compliance-Risiken ein sehr unterschiedliches Bild. Neben den oben genannten Positionen nennen die befragten Entscheidungsträger den **Chief Information Officer** (CIO) am häufigsten.

Auf dem vierten Platz folgt der **Chief Information Security Officer** (CISO), der für die Informationssicherheit im Unternehmen gesamtverantwortlich ist. In **14 %** der befragten Unternehmen ohne eigene Digital-Compliance-Position ist die Verantwortung für digitale Risiken hier verortet. Diese Position richten große Unternehmen doppelt so häufig ein wie kleinere mit weniger als 1.000 Beschäftigten (18 % versus 9 %).

Den **Chief Digital Officer** (CDO) nennen weniger als **10 %** der Befragten. Weitere Positionen, wie etwa die des **Datenschutzbeauftragten**, Positionen in den Bereichen Finance und Controlling beziehungsweise in der **Compliance-Abteilung** werden ebenfalls vergleichsweise selten genannt.

1.2 Digitaler Reifegrad aus Unternehmenssicht

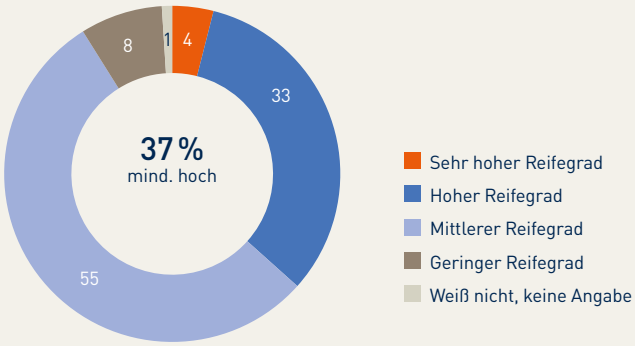
Viele Unternehmen erachten sich als nicht ausreichend digital aufgestellt.

Der digitale Reifegrad ist ein wichtiger Indikator für die Frage, inwiefern Unternehmen sich der fortschreitenden Digitalisierung anpassen und wie exponiert sie sich im Hinblick auf digitale Risiken sehen.

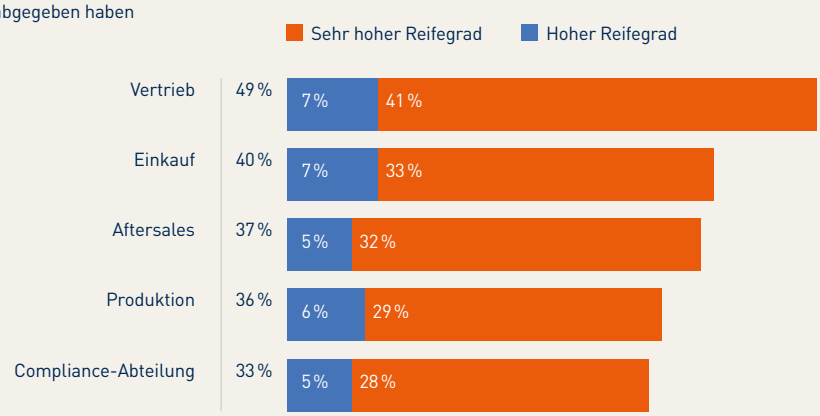
Digitaler Reifegrad

Nur gut ein Drittel der Fachleute bescheinigt dem eigenen Unternehmen einen hohen Reifegrad – Compliance-Abteilung mit Nachholbedarf

Globaleinschätzung



Digitaler Reifegrad verschiedener Unternehmensbereiche
Basis: Befragte, die eine Einschätzung abgegeben haben



Frage: Wie stufen Sie den digitalen Reifegrad Ihres Unternehmens ein? Und wie stufen Sie den digitalen Reifegrad der folgenden Bereiche Ihres Unternehmens ein?

Basis: Alle Unternehmen; Befragte, die eine Einschätzung zum digitalen Reifegrad einzelner Unternehmensbereiche abgegeben haben; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Viele Studienteilnehmer erachten ihr Unternehmen als nicht ausreichend digital aufgestellt. Dabei schätzten die Befragten mit Geschäftsleitungsfunktion den digitalen Reifegrad des Unternehmens im Vergleich zu Befragten aus Fachabteilungen zurückhaltender ein. Wenig verwunderlich ist, dass börsennotierte Unternehmen ihren Digitalisierungsgrad deutlich höher einschätzen als der Gesamtschnitt. Mit Blick auf einzelne Unternehmensbereiche sieht gerade die Compliance-Abteilung den größten Nachholbedarf.

Geschäftsleitung, Leitungsebene und Fachabteilungen

Bemerkenswert ist, dass die Einschätzung des digitalen Reifegrads innerhalb der Unternehmensebenen zu variieren scheint. Besonders unterscheiden sich die Einschätzungen zwischen Geschäftsleitung und Fachabteilung.

Die **Geschäftsleitung** bewertet den digitalen Reifegrad des eigenen Unternehmens eher zurückhaltend. Nur etwas mehr als ein Viertel von ihnen geht von einem hohen oder sehr hohen Reifegrad des eigenen Unternehmens aus (27 %). Die überwiegende Mehrheit sieht den Digitalisierungsgrad indes höchstens auf mittlerem Niveau.

Die Sicht der **Leitungsebene** ist durchaus optimistischer. Hier sehen bereits **37 %** der befragten Führungskräfte ihr Unternehmen als hoch oder sehr hoch digitalisiert an. Eine deutliche Mehrheit der Führungskräfte bewertet den digitalen Reifegrad hingegen im Mittelfeld (55 %) oder sieht Nachholbedarf (geringer Reifegrad 8 %). Im Branchenvergleich sticht insbesondere der **Banken- und Versicherungssektor** hervor. Hier sieht ein Großteil der befragten Führungskräfte den digitalen Reifegrad ihres Unternehmens als hoch an (63 %).

Deutlich höher ist der Anteil der Beschäftigten in den **Fachabteilungen**, wie beispielsweise IT, Compliance und Legal, die von einem hohen bis sehr hohen digitalen Reifegrad ausgehen. Hier sind es zwischen **39 %** und **46 %**.

Börsennotierte Unternehmen

Es mag nicht verwundern, dass vergleichsweise viele **börsennotierte Unternehmen** ihren Digitalisierungsgrad als hoch oder sehr hoch bewerten (42 %). Ihr Anteil liegt damit deutlich über dem **Gesamtschnitt** (37 % mit hohem oder sehr hohem digitalen Reifegrad). Selbst im Banken- und Versicherungssektor bescheinigen sich die befragten Unternehmen weniger oft einen hohen bis sehr hohen digitalen Reifegrad (40 %).

Einzelne Unternehmensbereiche

Auch beim Blick auf einzelne Unternehmensbereiche bewerten die Befragten den digitalen Reifegrad sehr unterschiedlich.[3]

Im Bereich **Compliance** sehen die Befragten den **größten Nachholbedarf**. Nur jedes dritte Unternehmen, das eine Einschätzung abgegeben hat, attestiert der Compliance-Abteilung einen mindestens hohen digitalen Reifegrad (33 %). Bei Unternehmen mit mindestens hohem digitalem Reifegrad schätzen die Compliance-Verantwortlichen selbst den eigenen Bereich zwar besser ein (41 %), bei Unternehmen mit niedrigerem Reifegrad allerdings fällt auch in dieser Gruppe das Urteil allenfalls mittelmäßig aus.

Anders sieht dies beispielsweise in den Bereichen **Einkauf, Aftersales und Produktion** aus. Hier bewerten immerhin zwischen **36 %** und **40 %** das Digitalisierungsniveau mindestens hoch. Der **Vertrieb** schneidet **am besten** ab. Hier sieht knapp die Hälfte der Befragten einen mindestens hohen digitalen Reifegrad (49 %). Allerdings wird der digitale Reifegrad jedoch auch in den anderen Unternehmensbereichen mehrheitlich höchstens im mittleren Niveau angesiedelt.

Insgesamt scheint es in den einzelnen Unternehmensbereichen und insbesondere in der Compliance-Abteilung der Befragten ein erhebliches Aufholpotenzial zu geben.

[3] Anmerkung: Um Verzerrungen der Ergebnisse vorzubeugen, werden nur jene Fachleute herangezogen, deren Fachexpertise eine Bewertung jeweils zuließ. Je nach abgefragtem Unternehmensbereich konnten oder wollten zwischen 8 % und 31 % der Befragten keine Einschätzung vornehmen.

1.3 Positionen für digitale Compliance im Unternehmen

Oft fehlen spezielle Positionen zum Umgang mit digitalen Compliance-Risiken; die technische Expertise ist jedenfalls unterrepräsentiert.

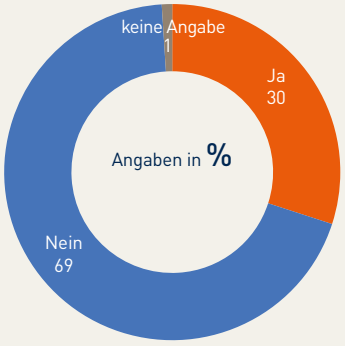
Die Geschäftsleitung kann die Aufgabe der digitalen Compliance innerhalb des Unternehmens delegieren. Regelmäßig wird es sinnvoll sein, wenn die Geschäftsleitung Beschäftigte mit der notwendigen speziellen Expertise mit dieser Aufgabe betraut. Damit wird die Geschäftsleitung zwar nicht von ihrer Gesamtverantwortung befreit, sondern ihre Handlungspflicht wandelt sich zu einer Auswahl- und Überwachungspflicht.

Trotz dieser Delegationsmöglichkeit zeigt die Studie, dass oftmals spezielle Positionen zum Umgang mit digitalen Compliance-Risiken fehlen. Zudem deuten die Rückmeldungen darauf hin, dass die technische Expertise in den jeweiligen Positionen vergleichsweise unterrepräsentiert ist.

Unternehmensposition für digitale Compliance-Risiken

In 3 von 10 Fällen ist eine dedizierte Position vorhanden

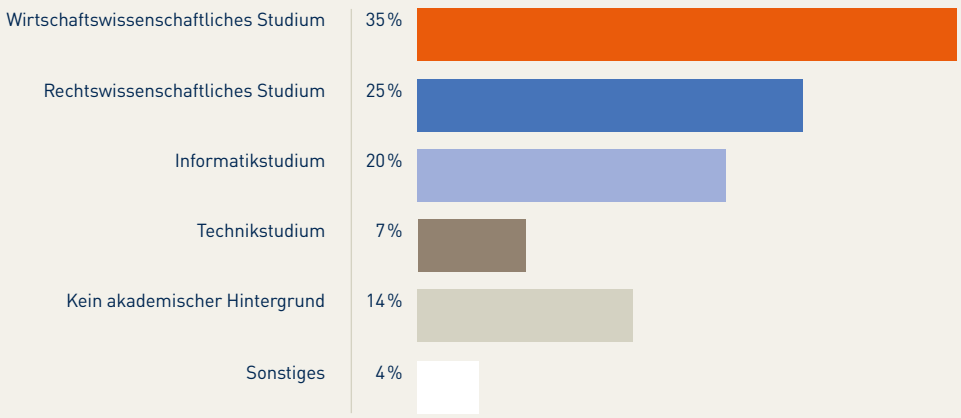
Spezielle Unternehmensposition für digitale Compliance-Risiken vorhanden?



Falls vorhanden:
Häufigste Bezeichnung der Position (Top 3)

26 % (Digital) Compliance-Beauftrage/r
20 % IT-Security Officer, IT-Governance Officer o.Ä.
12 % Datenschutzbeauftragte/r

Falls vorhanden: Ausbildungshintergrund des bzw. der zuständigen Compliance-Beauftragten



Frage: Gibt es in Ihrem Unternehmen eine Position, die speziell für digitale Compliance-Risiken zuständig ist? Wie ist die Bezeichnung dieser Position? Und können Sie uns sagen, über welchen Ausbildungshintergrund der oder die zuständige Compliance-Beauftragte verfügt?

Basis: Alle Unternehmen; Unternehmen mit einer speziellen Position für digitale Compliance-Risiken; Mehrfachnennungen teilw. möglich; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Ausdrückliche Zuständigkeit für digitale Compliance-Risiken

Lediglich drei von zehn der befragten Unternehmen haben eine Position geschaffen, die speziell für digitale Compliance-Risiken zuständig ist. Vor allem Unternehmen, die sich einen weniger hohen digitalen Reifegrad bescheinigen, haben auch seltener spezielle Positionen zum Umgang mit digitalen Compliance-Risiken eingerichtet (26 %).

Auch in den einzelnen Branchen ergeben sich große Unterschiede. Während mehr als jedes Zweite der befragten Unternehmen aus der **Finanzbranche** eine digitale Compliance-Position besetzt hat (53 %), ist der Anteil im verarbeitenden Gewerbe deutlich geringer (höchstens 27 %).

Die befragten **börsennotierten und nicht börsennotierten Unternehmen** unterscheiden sich ebenfalls, wobei der Unterschied im Vergleich geringer ausfällt. So hat mehr als ein Drittel der börsennotierten Unternehmen eine spezielle Position für digitale Compliance-Risiken etabliert (35 % versus 30 %).

Die **Unternehmensgröße** alleine spielt offenbar **nicht die entscheidende Rolle**, auch wenn es sich bei den allermeisten der befragten börsennotierten Unternehmen um größere mit über 1.000 Beschäftigten handelt. Sie geben an, etwas seltener eine Digital-Compliance-Position zu unterhalten, als kleinere Unternehmen mit weniger als 1.000 Beschäftigten (29 % versus 32 %). In den größeren befragten Unternehmen ab 1.000 Beschäftigten hat diese Position überdurchschnittlich häufig der Compliance-Beauftragte oder ein IT-Security Officer inne (33 % beziehungsweise 23 %).

Die genauen Positionsbezeichnungen lassen erkennen, dass die im Rahmen dieser Position für digitale Compliance-Risiken Verantwortlichen sehr oft **direkt aus dem Bereich Compliance oder der IT** stammen. So sind die häufigsten Bezeichnungen für diese Position etwa „Digital Compliance-Beauftragte/r" (26 %) oder „IT-Security/Governance Officer" (20 %). In **12 %** der befragten Unternehmen wird die Position von dem oder der Datenschutzbeauftragten bekleidet. Darüber hinaus existiert bei den Studienteilnehmern eine Vielzahl unterschiedlicher Positionsbezeichnungen für diese Rolle, von nicht näher spezifizierten IT-Positionen über den Risk-Manager bis hin zum Digital Transformation Manager.

Interessanterweise deuten die Rückmeldungen darauf hin, dass Unternehmen mit zunehmendem digitalem Reifegrad auch öfter der Compliance-Abteilung den Umgang mit digitalen Compliance-Risiken anvertrauen (38 % mindestens hoher versus 16 % höchstens mittlerer digitaler Reifegrad). Im Gegensatz dazu ist in den befragten Unternehmen mit geringem oder mittlerem Reifegrad die IT-Abteilung, der Datenschutz oder das Risk-Management öfter zuständig (IT-Security/Governance Officer: 22 % bei geringem oder mittlerem versus 17 % bei hohem Reifegrad; Datenschutzbeauftragter: 17 % versus 7 %; Risk-Manager: 8 % versus 2 %).

Eine Compliance-Abteilung muss nicht zwingend existieren. Allerdings gibt der weit überwiegende Anteil der Befragten mit einer Digital-Compliance-Position an, über eine Compliance-Abteilung zu verfügen (85 %).

Technische Expertise

In den speziellen Compliance-Positionen, die sich mit digitalen Risiken befassen, ist die technische Expertise oft unterrepräsentiert.

Nur ein Fünftel der befragten Unternehmen gibt an, dass die Beschäftigten in dieser Position über ein **Informatikstudium** verfügen. Ein abgeschlossenes **Technikstudium** ist äußert selten anzutreffen (7 %). Am häufigsten managen studierte **Wirtschaftswissenschaftler** digitale Compliance-Risiken in den befragten Unternehmen (35 %), gefolgt von **Juristen** (25 %).

Gerade **größere Unternehmen** mit 1.000 oder mehr Mitarbeitern beschäftigen laut eigenen Angaben etwa doppelt so häufig Juristen als kleinere Unternehmen (35 % versus 18 %). Auch in den befragten Unternehmen mit einem hohen digitalen Reifegrad sind häufiger Juristen in der Position des Digital-Compliance-Beauftragten anzutreffen als in Unternehmen mit niedrigerer digitaler Reife (31 % versus 20 %).

Dementsprechend verfügt der weit überwiegende Teil der Mitarbeiter, die mit dem Umgang digitaler Compliance-Risiken beauftragt sind, über einen akademischen Hintergrund. Nur **14 %** der speziell hierfür zuständigen Mitarbeiter haben kein Studium absolviert. Auffällig ist, dass der Anteil in kleineren Unternehmen fast doppelt so hoch ist wie in größeren Unternehmen mit mehr als 1.000 Beschäftigten (18 % versus 10 %).

2. Digitale Rechtsrisiken

Die digitalen Rechtsrisiken, denen Unternehmen ausgesetzt sein können, nehmen kontinuierlich zu und werden gleichzeitig komplexer.

Es verwundert daher nicht, dass sich bereits bei rund der Hälfte der Befragten digitale Risiken realisiert haben. Bei denjenigen Unternehmen, die noch nicht betroffen waren, scheint es vor allem Nachholbedarf beim Compliance-Management von Ransomware-Angriffen und Urheberrechtsverletzungen zu geben. Der weit überwiegende Teil der Studienteilnehmer hat aber bereits Compliance-Maßnahmen zur Reduzierung digitaler Rechtsrisiken ergriffen. Gerade bei neueren Technologien werden die rechtlichen Risiken derzeit oftmals noch unterschätzt.

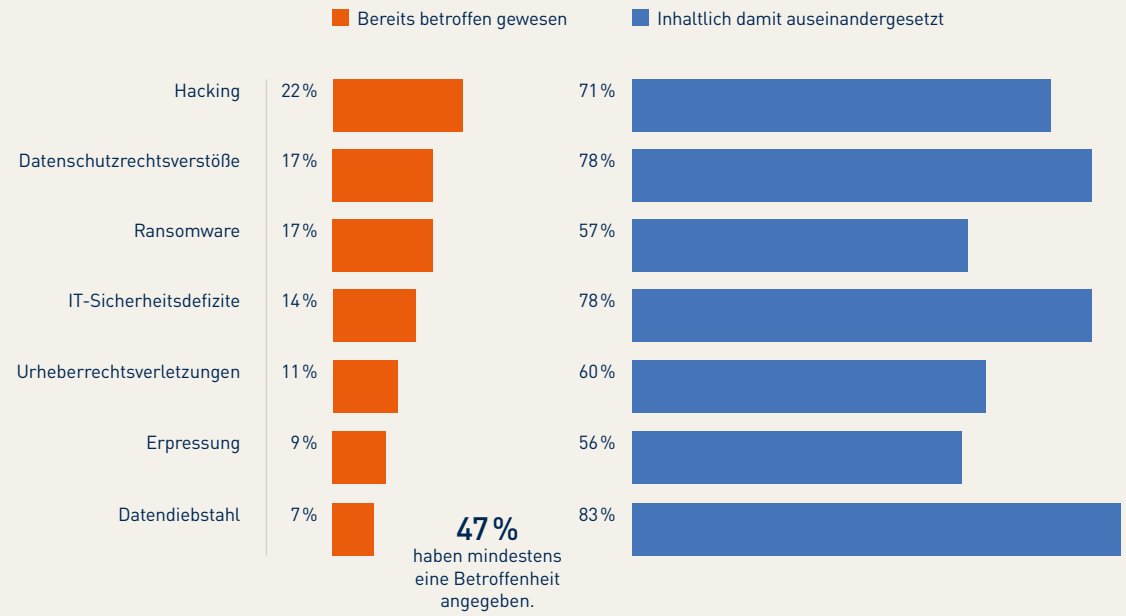
2.1 Betroffenheit

In rund der Hälfte der Unternehmen haben sich digitale Rechtsrisiken bereits realisiert.

Mehr als jedes Fünfte der befragten Unternehmen wurde schon einmal Opfer eines Hacking-Angriffs (22 %). Von den größeren oder börsennotierten Unternehmen oder solchen mit Mutterkonzern im Ausland waren sogar jeweils fast drei von zehn betroffen (27 % bis 28 %).

Rechtliche Risiken durch Digitalisierung

Fast jedes zweite Unternehmen war insgesamt bereits betroffen – Nachholbedarf in Sachen Erpressung, Ransomware und Urheberrecht



Frage: Inwieweit hat sich Ihr Unternehmen mit den folgenden rechtlichen Risiken bezogen auf Digitalisierung befasst?

Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Diese Angaben korrespondieren mit den seit Jahren **steigenden rechtlichen Anforderungen** an digitale Technologien und der **wachsenden Bedrohungslage** durch Cyberangriffe. So stellt das Bundesamt für Sicherheit in der Informationstechnik in seinem aktuellen Lagebericht zur IT-Sicherheit in Deutschland fest, dass alleine im Jahr 2020 rund 117 Millionen neue Schadprogramm-Varianten in Umlauf gebracht wurden. Das Bundeskriminalamt gibt in seinem aktuellen Bundeslagebild zur Cyberkriminalität an, dass die Anzahl der Cyberstraftaten stetig steigt (allein um knapp 8 % von 2019 auf 2020). In den letzten Jahren stellen vor allem Ransomware-Attacken Unternehmen weltweit vor enorme Herausforderungen. Vereinfacht dargestellt verschlüsselt der Angreifer im Rahmen dieser Attacken oftmals existenzielle Unternehmensdaten und erpresst für deren Freigabe ein digitales Lösegeld.

Etwa jedes sechste Unternehmen berichtet davon, bereits Opfer einer **Ransomware-Attacke** gewesen zu sein (17 %). Der Anteil der **börsennotierten Unternehmen** ist dabei auffallend hoch (37 %). Etwas geringer, aber dennoch vergleichsweise hoch, ist der Anteil der befragten **größeren Unternehmen** mit mindestens 1.000 Beschäftigten oder Unternehmen mit **ausländischem Mutterkonzern**, von denen jeweils ein Viertel bereits Ziel von Ransomware-Attacken wurde (jeweils 25 %).

IT-Sicherheitsdefizite und **Urheberrechtsverletzungen** scheinen nach den Rückmeldungen einen geringeren Anteil zu bilden (14 % beziehungsweise 11 %). Speziell der **Datendiebstahl** scheint noch seltener stattzufinden, wobei diese vergleichsweise geringe Zahl vor dem Hintergrund der hohen Anzahl an Hacking- und Ransomware-Angriffen etwas verwundert (7 %). Auch in diesen Bereichen werden die befragten **börsennotierten Unternehmen** häufiger attackiert als nicht börsennotierte Unternehmen. So gaben rund dreimal so viele börsennotierte Unternehmen an, zum Ziel unbefugten Ausspähens geheimer oder personenbezogener Daten geworden zu sein (21 % versus 7 %).

2.2 Risikoeinschätzung nicht betroffener Unternehmen

Die Unternehmen, bei denen sich noch keine digitalen Risiken realisiert hatten, fragten wir danach, ob sie sich mit den jeweiligen Risiken bereits inhaltlich auseinandergesetzt haben.

Hier scheint es gerade bei den weiter zunehmenden **Ransomware-Angriffen**, aber auch bei **Urheberrechtsverletzungen größeren Nachholbedarf** zu geben. Lediglich etwa drei von fünf der Befragten berichten, sich mit diesen Risiken befasst zu haben (zwischen 56 % und 60 %). Rechnet man jeweils die Unternehmen hinzu, in denen bereits entsprechende Rechtsverletzungen stattgefunden haben, fehlt es jeweils zwischen einem Drittel und einem Viertel der Befragten zu diesen Themen an Erfahrung oder sie haben sich hiermit noch gar nicht befasst (26 % bis 35 %). Demgegenüber haben sich bereits mehr als zwei Drittel der Entscheidungsträger nach eigenen Angaben mit den Themenfeldern Hacking, Datenschutzrechtsverstöße, IT-Sicherheitsdefizite und Datendiebstahl auseinandergesetzt (jeweils über 70 %).

2.3 Maßnahmen zur Risikoreduzierung

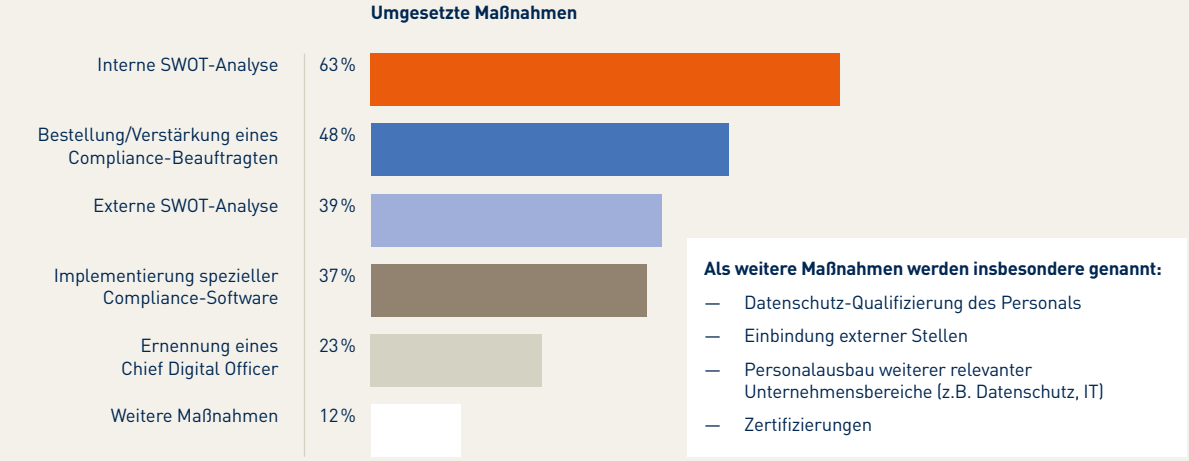
Der weit überwiegende Teil der befragten Unternehmen hat bereits Compliance-Maßnahmen zur Reduzierung digitaler Rechtsrisken ergriffen.

Begrüßenswert ist, dass der weit überwiegende Teil der befragten Unternehmen bereits in der einen oder anderen Weise Compliance-Maßnahmen ergriffen hat, um digitale Rechtsrisiken zu mindern.

89 % der befragten Entscheidungsträger nennen mindestens eine der fünf nachfolgenden Einzelmaßnahmen oder verweisen auf weitere Maßnahmen.

Maßnahmen gegen Compliance-Risiken

9 von 10 Unternehmen haben Maßnahmen umgesetzt, meist interne SWOT-Analysen



Frage: Welche der folgenden Maßnahmen haben Sie ergriffen, um Compliance-Risiken aus der Digitalisierung zu begegnen?

Basis: Alle Unternehmen; Mehrfachnennungen möglich; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Am verbreitetsten sind **interne SWOT-Analysen**, die in **63 %** der befragten Unternehmen als Element der strategischen Risikoabwehr zum Einsatz kommen. Diese Untersuchungen von Stärken, Schwächen, Chancen und Risiken des eigenen Unternehmens sind am meisten in der **Finanz- und Versicherungsbranche** verbreitet (84 %).

Ebenfalls erfreulich ist, dass fast jedes zweite Unternehmen angibt, einen **Compliance-Beauftragten bestellt** oder das **Compliance-Team verstärkt** zu haben (48 %). Die Rückmeldungen legen nahe, dass Unternehmen Maßnahmen vermehrt implementieren, wenn ein Compliance-Beauftragter oder eine dezidierte Compliance-Abteilung existiert. So führen die Studienteilnehmer mit einer eingerichteten Compliance-Abteilung deutlich häufiger unter anderem interne SWOT-Analysen durch (68 %) oder implementieren spezielle Compliance-Software (41 %) als die befragten Unternehmen ohne Compliance-Abteilung (51 % beziehungsweise 27 %). Dieser Umstand mag aber nicht darüber hinwegtäuschen, dass in nur drei von zehn der befragten Unternehmen eine Position existiert, die speziell für digitale Compliance-Risiken zuständig ist (siehe hierzu oben S. 13).

Auffällig ist, dass **größere Unternehmen mit mindestens 1.000 Beschäftigten, börsennotierte Unternehmen und solche mit ausländischer Konzernmutter** offensichtlich sehr viel häufiger Maßnahmen gegen digitale Risiken umsetzen als kleinere, nicht börsennotierte Unternehmen mit Stammsitz im Inland. So haben beispielsweise **77 %** der befragten börsennotierten Unternehmen interne SWOT-Analysen vorgenommen, während dies lediglich bei **61 %** der nicht börsennotierten Unternehmen der Fall ist.

Ein ähnlicher Befund ergibt sich im Vergleich zwischen den befragten **Unternehmen mit hohem oder sehr hohem digitalem Reifegrad**, die weniger zögerlich Compliance-sichernde Maßnahmen implementieren (durchschnittlich 2,5 ergriffene Maßnahmen) als Unternehmen mit geringerem digitalem Reifegrad (durchschnittlich 2,0 ergriffene Maßnahmen).

Compliance-Maßnahmen werden vergleichsweise oft als **reaktives Mittel** auf Compliance-Verstöße vorgenommen. So führen Unternehmen, die bereits betroffen waren, öfter interne SWOT-Analysen durch oder schaffen spezielle Compliance-Software an als Unternehmen, die bisher noch keine Compliance-Vorfälle zu beklagen hatten (Abstand jeweils zwischen 8 und 14 Prozentpunkten). Insofern wäre es zu begrüßen, wenn Unternehmen noch stärker einen präventiven Ansatz verfolgen, um Compliance-Vorfälle bereits bestmöglich zu verhindern, anstatt später darauf reagieren zu müssen.

2.4 Technologien

Gerade bei neueren Technologien werden die rechtlichen Risiken oftmals unterschätzt.

Die digitalen Compliance-Risiken eines Unternehmens hängen maßgeblich von den eingesetzten Technologien ab. Die Rückmeldungen der Studie zeigen, dass das allgemeine Risikobewusstsein bei den Unternehmen noch geschärft werden muss. Denn die Befragten bewerten die rechtlichen Risiken in fast allen abgefragten Technologiebereichen weit überwiegend als gering oder mittelmäßig. Die rechtlichen Risiken neuerer Technologien werden oftmals unterschätzt. Dabei wird die Komplexität der Compliance-Anforderungen gerade in diesem Feld weiter steigen.

Übergreifende Risikoeinschätzung

Die befragten Unternehmen bewerten in **fast allen Technologiebereichen** die hiermit verbundenen Rechtsrisiken weit überwiegend als **gering oder mittelmäßig** (71 % bis 88 %).

Die Unternehmen mit hohem digitalem Reifegrad schätzen auch die Compliance-Risiken von Technologien höher ein als Unternehmen mit einem geringeren digitalen Reifegrad. So nehmen **Unternehmen mit hohem digitalem Reifegrad** Compliance-Risiken etwa von Webservices und Big-Data-Analysen als bedeutend höher wahr (17 % beziehungsweise 13 % versus 8 % beziehungsweise 5 %).

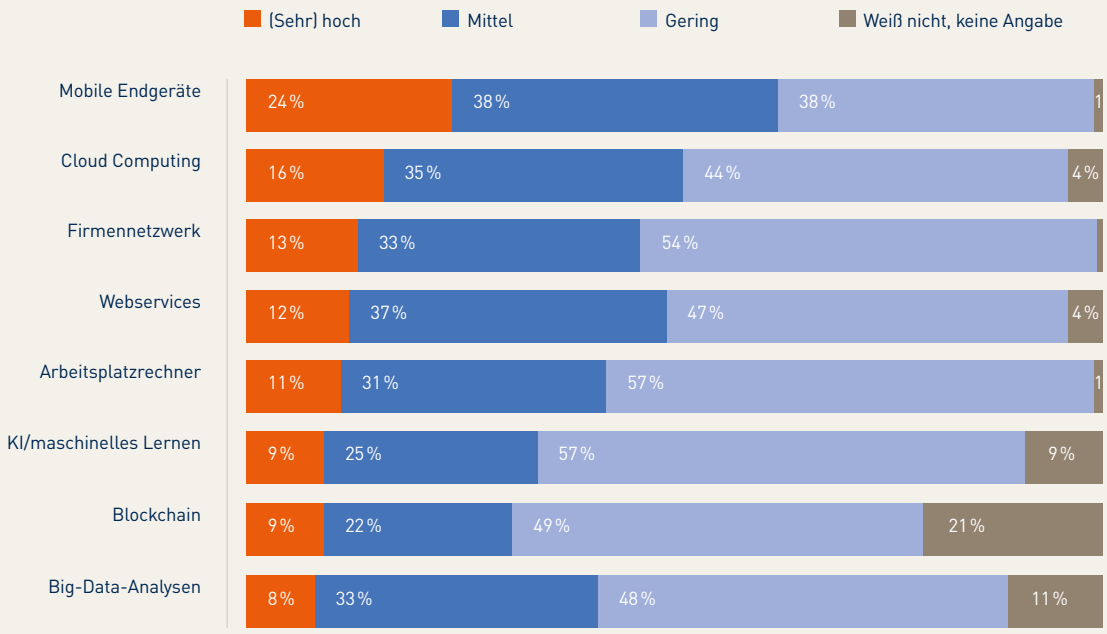
Dies deutet darauf hin, dass Unternehmen, die sich intensiver mit dem Thema digitale Compliance auseinandersetzen, digitale Rechtsrisiken von Technologien häufiger erkennen und damit adressieren können.

Technologiespezifische Risikoeinschätzung

Gerade bei **neueren Technologien** wie etwa Blockchain, Einsatz von künstlicher Intelligenz („**KI**") oder Big-Data-Analysen zeigt sich, dass die befragten Unternehmen die hiermit zusammenhängenden Risiken oftmals unterschätzen.

Laptops, Smartphones und Tablets am ehesten risikobehaftet

Risikograd von Rechtsverletzungen im Bereich digitaler Technologien



Frage: Wenn Sie an die in Ihrem Unternehmen eingesetzten digitalen Technologien denken: Wie schätzen Sie diesbezüglich das Risiko von Rechtsverletzungen ein?

Basis: Unternehmen, die die jeweilige Technologie einsetzen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Dabei sieht die **Geschäftsleitung** mit diesen Technologien vergleichsweise öfter höhere Rechtsrisiken einhergehen als Führungskräfte aus den Fachabteilungen, denn deren Anteil ist mindestens doppelt so groß wie im Durchschnitt. Dennoch ist die absolute Anzahl vergleichsweise gering, da jeweils etwa ein Fünftel der befragten Geschäftsführer und Vorstände und etwa ein Zehntel der Befragten insgesamt in diesen Technologien hohe Rechtsrisiken sehen.

Für die befragten Entscheidungsträger sind **mobile Endgeräte**, wie beispielsweise Laptops oder Smartphones, noch am ehesten risikobehaftet. **24 %** der Studienteilnehmer, deren Beschäftigte derartige Geräte beruflich nutzen, gehen hier von einem hohen bis sehr hohen Compliance-Risiko aus. Bei den Befragten aus dem IT-Bereich ist der Anteil noch größer (29 %).

Für das **Cloud-Computing** ist das Risikobewusstsein übergreifend eher gering ausgeprägt (24 % bei den befragten Führungskräften aus dem IT-Bereich versus 16 % aus anderen Abteilungen). Im Mittelfeld der Risikowahrnehmung liegen **Firmennetzwerke**, **Webservices** und der **klassische Arbeitsplatzrechner**. Jedes achte bis neunte Unternehmen sieht hier jeweils ein hohes oder sehr hohes Risiko von Rechtsverletzungen.

Noch seltener gelten **KI- oder Blockchain-Anwendungen sowie Big-Data-Analysen** als riskant. Jeweils weniger als jedes zehnte der befragten Unternehmen sieht in diesen Technologien hohe Compliance-Risiken. Dies dürfte wohl vor allem daran liegen, dass diese Technologien noch vergleichsweise jung sind und viele Unternehmen diese noch nicht stark einsetzen. Hierfür spricht auch, dass bis zu einem Fünftel der Befragten zu den Rechtsrisiken dieser Technologien keine Angaben machen können oder wollen (21 % bis 9 %).

Zunehmende Komplexität der Compliance bei neueren Technologien

In den letzten Jahren sind der europäische sowie der deutsche Gesetzgeber auf dem Gebiet digitaler Regulierung deutlich aktiver geworden. Auch die Rechtsprechung des Europäischen Gerichtshofs erhöht die Komplexität der Situation weiter.

Ein Treiber dieser gesteigerten Aktivität ist zum einen die tatsächliche Bedrohungslage, die der Vulnerabilität der eingesetzten Technologien geschuldet ist. Aufgrund der fortschreitenden Digitalisierung und Automatisierung von Prozessen besteht für die Unternehmen die ständige Gefahr eines Angriffs von außen, insbesondere in Form von Hackerattacken, die im schlimmsten Fall durch die Verschlüsselung kritischer Daten die wirtschaftliche Tätigkeit des Unternehmens zum Erliegen bringen können.

Zum anderen bringt der rasante technische Fortschritt die Gefahr eines Kontrollverlusts mit sich. Zum Beispiel führt die Weiterentwicklung der KI dazu, dass deren Ergebnisse und Reaktionen vom Menschen nicht mehr vollständig kontrolliert werden können.

Die oben skizierten Aussagen bestätigen sich vor allem durch einen kurzen Blick auf das IT-Sicherheitsrecht, das Datenschutzrecht sowie die neuen regulatorischen Ansätze für die Regulierung von KI-Anwendungen.

IT-Sicherheitsrecht

Das „Gesetz über das Bundesamt für Sicherheit in der Informationstechnik" („**BSIG**") bestimmt für einen gewissen Unternehmenskreis konkrete Anforderungen an die Organisation und Überwachung ihrer IT-Systeme. Ebenso haben diese Unternehmen die Pflicht, Störungen ihrer IT an das Bundesamt für Sicherheit in der Informationstechnik („**BSI**") zu melden. Bei Verstößen drohen Bußgelder in Höhe von bis zu 20 Millionen Euro (§ 14 Abs. 5 S. 1 BSIG, § 30 Abs. 2 S. 3 OWiG). Mit dem kürzlich verabschiedeten „IT-Sicherheitsgesetz 2.0" wurden der Adressatenkreis sowie das inhaltliche Pflichtenspektrum noch einmal erheblich erweitert. Angesprochen sind nun nicht nur Unternehmen bestimmter Sektoren, sondern auch „Unternehmen im besonderen öffentlichen Interesse", die von „erheblicher volkswirtschaftlicher Bedeutung für die Bundesrepublik Deutschland oder die für solche Unternehmen als Zulieferer [...] von wesentlicher Bedeutung sind" (vgl. § 2 Abs. 14 S. 1 Nr. 2 BSIG). Durch die Referenz dieser Definition auf Zulieferer dürfte sich der persönliche Anwendungsbereich des Gesetzes deutlich erweitert haben. Jedenfalls müssen diese Unternehmen dem BSI detailliert darlegen, welche Zertifizierungen und Sicherheitsaudits sie in den letzten zwei Jahren durchgeführt haben, und etwaige Störungen ihrer IT-Systeme unverzüglich melden (§ 8f Abs. 1, 7, 8 BSIG). Die Betreiber kritischer Infrastrukturen, also Unternehmen bestimmter Sektoren, die von hoher Bedeutung für das Funktionieren

des Gemeinwesens sind, müssen noch strengere Anforderungen erfüllen. Dazu zählen unter anderem die Pflichten, die IT-Systeme durch organisatorische und technische Vorkehrungen proaktiv zu schützen (§ 8a Abs. 1 BSIG), den Einsatz bestimmter IT-Produkte anzuzeigen (§ 9b Abs. 1 BSIG) oder künftig auch „intelligente" Systeme zur Angriffserkennung (§ 8a Abs. 1a BSIG) zu verwenden.

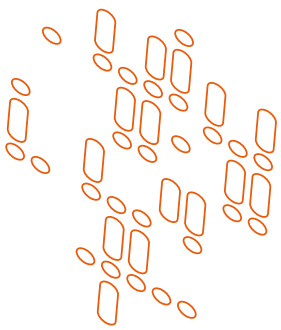
Datenschutzrecht

Hackerangriffe führen nicht selten auch zur Kompromittierung personenbezogener Daten. Jüngstes Beispiel dafür ist der Angriff der Hackergruppe „Hafnium", die sich durch eine kritische Sicherheitslücke in „On-premise"-Versionen des Programms „Microsoft Exchange" Zugriff auf eine Vielzahl an E-Mail-Accounts verschaffen und Malware in die Systeme einschleusen konnte. Dabei sind Unternehmen auch datenschutzrechtlich dazu verpflichtet, Sicherheitslücken in ihren IT-Systemen unverzüglich zu schließen. Bei Verlust oder Offenlegung personenbezogener Daten müssen die zuständigen Datenschutzaufsichtsbehörden (Art. 33 Abs. 1 DSGVO) sowie gegebenenfalls auch die Betroffenen (Art. 34 Abs. 1 DSGVO) benachrichtigt werden.

Datenschutzrechtliche Herausforderungen stellen sich jedoch nicht nur beim Schutz der IT-Infrastruktur vor Hackerangriffen, sondern auch beim Einsatz digitaler Arbeitsmittel, insbesondere bei der Nutzung cloudbasierter Software-as-a-Service-Lösungen, in denen personenbezogene Daten verarbeitet werden. Mit Urteil vom 16. Juli 2020 hat der Europäische Gerichtshof (Rs. C 311/18 – Schrems II) den „EU-US Privacy Shield", ein Rechtsinstrument für sichere Datenübermittlungen in die USA, für ungültig erklärt. Da viele Cloudlösungen für Unternehmen vor allem von US-Anbietern stammen, hat die Frage der datenschutzrechtskonformen Nutzbarkeit dieser Angebote entscheidende Bedeutung. Nach den Empfehlungen des Europäischen Datenschutzausschusses (Recommendations 01/2020) sollten Unternehmen die Rechtslage und Behördenpraxis im Zielland der Datenübermittlung genau prüfen und gegebenenfalls ergänzende Maßnahmen wie die Verschlüsselung der Daten implementieren, um ein angemessenes Datenschutzniveau sicherzustellen.

Regulierung von KI

Der oben beschriebene drohende Kontrollverlust, insbesondere bei der Anwendung von KI, hat mittlerweile auch den Gesetzgeber auf den Plan gerufen. So hat beispielsweise die Europäische Kommission einen Entwurf einer KI-Verordnung (COM(2021) 206 final) vorgelegt, in dem sie den Umgang mit KI-Systemen zu regeln beabsichtigt. Der Vorschlag folgt einem risikobasierten Ansatz, der die Zulässigkeit der Verwendung der KI von den damit verbundenen Gefahren abhängig macht. Bei Verstößen sieht der Entwurf deutliche Bußgelder in Höhe von bis zu 30 Millionen Euro bzw. **6 %** des weltweiten Jahresumsatzes vor. Die Schwelle der Anwendbarkeit dieser Regeln ist dabei denkbar niedrig. Denn der Vorschlag der Europäischen Kommission folgt einem sehr weiten Verständnis von „künstlicher Intelligenz", die bereits dann vorliegen soll, wenn Software nach bestimmten Techniken und Konzepten entwickelt worden ist und das Umfeld, mit dem sie interagiert, durch „Empfehlungen oder Entscheidungen" beeinflussen kann (Art. 3 Nr. 1 KI-Verordnung-Entwurf). Damit dürften unter die Verordnung auch Anwendungen fallen, die bis dato noch als „normale" Software eingeordnet worden sind. Zwar wird der Entwurf der Kommission im weiteren Verfahren wohl noch erhebliche Änderungen erfahren, bevor er tatsächlich in Kraft tritt. Allerdings ist bereits jetzt erkennbar, dass der von der Europäischen Kommission verfolgte Regulierungsansatz die Unternehmen vor große (Compliance-)Herausforderungen stellen wird.



3. Digitalisierung der Compliance-Prozesse

Unternehmen müssen nicht nur trotz der voranschreitenden Digitalisierung ihre Compliance sicherstellen. Die Digitalisierung eröffnet vielmehr auch neue Möglichkeiten, potenziellen Compliance-Risiken zu begegnen.

Die fortschreitende Digitalisierung wird daher für Compliance-Prozesse vieler Unternehmen immer wichtiger. Die enorme Relevanz zeigt sich auch daran, dass viele befragte Entscheidungsträger in den kommenden Jahren verstärkt in digitale Compliance-Tools investieren möchten.

Zwar setzen die Studienteilnehmer bereits überwiegend Compliance-Tools, vor allem Informations- und Prozesstools, ein. Es scheint aber noch an flexiblen Lösungen zu fehlen, da ein signifikanter Teil der Befragten Compliance-Tools selbst entwickelt. Dass die eingesetzten Tools ihrerseits wiederum mit Compliance-Risiken einhergehen können, scheint vielen der befragten Unternehmen nicht bewusst zu sein.

3.1 Relevanz der fortschreitenden Digitalisierung im Bereich Compliance

Die fortschreitende Digitalisierung wird für Compliance-Prozesse vieler Unternehmen immer wichtiger.

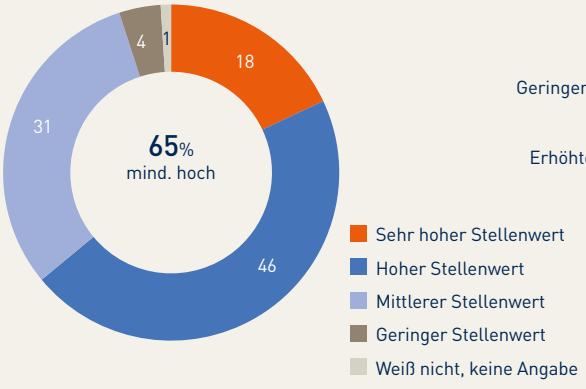
Wenn es um die Verbesserung der Compliance geht, messen **zwei von drei der Studienteilnehmer** der Digitalisierung einen **hohen bis sehr hohen Stellenwert** bei.

Immerhin rund ein Drittel der befragten **Führungskräfte** geht von einer mittleren Bedeutung aus (31 %). Kaum jemand gibt an, dass die fortschreitende Digitalisierung für die Compliance nur von geringer Relevanz ist (4 %).

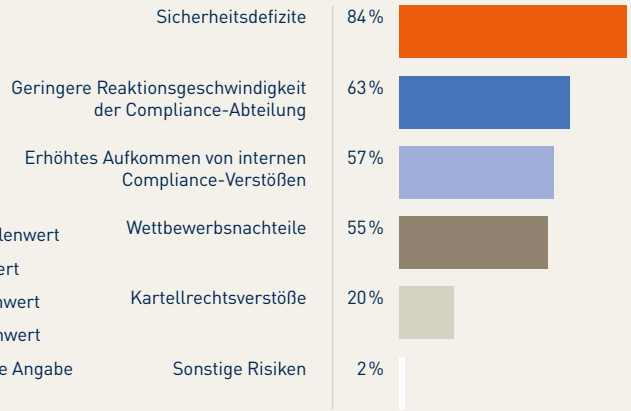
Relevanz einer fortschreitenden Digitalisierung im Bereich Compliance

Für zwei Drittel hat das Thema einen hohen Stellenwert – insbesondere um Sicherheitsdefiziten vorzubeugen

Stellenwert der Möglichkeiten einer verbesserten Compliance durch Digitalisierung



Risiken durch verschleppte Digitalisierung von Compliance-Prozessen



Frage: Welchen Stellenwert messen Sie den Möglichkeiten der Digitalisierung zu, um Compliance besser als bisher zu gewährleisten? Welche der folgenden Risiken sehen Sie, wenn die Compliance-Prozesse nicht mit der Digitalisierung im Unternehmen Schritt halten?

Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Vor allem die Befragten in den **Compliance-Abteilungen** gehen davon aus, dass die Digitalisierung für die Compliance äußert relevant ist. Fast drei Viertel der befragten **Führungskräfte** aus Compliance-Abteilungen messen den digitalen Tools und Verfahren eine hohe bis sehr hohe Bedeutung zu (73 %). Die Anzahl der Kollegen aus den **IT-Abteilungen**, die diese Einschätzung teilt, ist jedoch geringer (56 %).

Unternehmen, die bereits von Compliance-Verstößen **betroffen** waren, erachten die Digitalisierung für die Verbesserung der Compliance öfter als bedeutend als Unternehmen ohne solche Vorfälle (72 % versus 58 %). Dieser Auffassung sind auch befragte größere und börsennotierte Unternehmen. Diese messen der Digitalisierung ebenfalls einen größeren Stellenwert bei als kleinere Unternehmen (69 % versus 61 %) und nicht börsennotierte Unternehmen (77 % versus 63 %).

Dabei sehen die Befragten durch eine **verschleppte Digitalisierung** vor allem die Gefahr von Sicherheitsdefiziten in ihren Compliance-Prozessen. Mehr als vier von fünf Studienteilnehmern gehen von **erhöhten Sicherheitsrisiken** aus, wenn die Compliance-Prozesse nicht mit der Digitalisierung im Unternehmen Schritt halten (84 %). Ein großer Anteil sorgt sich auch darum, dass die Compliance-Abteilung nur langsamer auf potenzielle Vorfälle reagieren könnte (74 %). Vor allem die Compliance-Abteilungen selbst beunruhigt dieser Aspekt. Drei von vier Führungskräften aus den Compliance-Abteilungen der befragten Unternehmen sehen hier ein bedeutendes Risiko (76 %).

Weiterhin befürchtet jeweils eine Mehrheit der Befragten bei einer unzureichenden Digitalisierung von Compliance-Prozessen ein erhöhtes Aufkommen von **internen Compliance-Verstößen** und **Wettbewerbsnachteile** (57 % beziehungsweise 55 %). Unternehmen mit ausländischem Mutterkonzern schätzen diese Risiken noch höher ein als Unternehmen mit Stammsitz in Deutschland (jeweils 67 % versus 54 % bzw. 67 % versus 52 %). Dass ein Verzicht auf Digitalisierung auch **kartellrechtliche Compliance-Verstöße** wahrscheinlicher macht, glaubt in **börsennotierten Unternehmen** jede dritte Führungskraft (35 %).

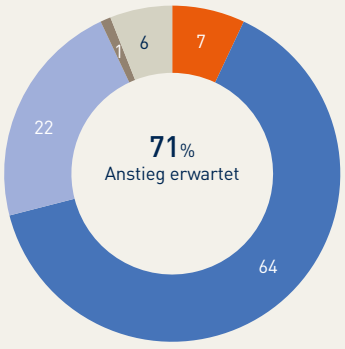
3.2 Budget für digitale Compliance-Prozesse

In den kommenden Jahren möchten viele Unternehmen verstärkt in digitale Compliance-Tools investieren. Nur wenige Informationen zum derzeitigen Budget für digitale Compliance-Tools.

Budgetentwicklung

Die Rückmeldungen legen nahe, dass in den kommenden drei Jahren von zunehmenden Investitionen in digitale Compliance-Tools auszugehen ist. Digitale Tools werden damit von einer großen Mehrheit der befragten Fachleute als **wichtiges Zukunftsthema** gesehen.

Künftige Entwicklung des Compliance-Budgets für digitale Tools



Gesamtergebnis

- Stark ansteigen
- Ansteigen
- In etwa gleichbleiben
- Sinken
- Weiß nicht, keine Angabe

Digitale Tools werden definitiv als investitionswürdiges Zukunftsthema gesehen – unter Unternehmen mit Nachholbedarf sogar verstärkt

Ergebnisse nach digitalem Reifegrad der Unternehmen
Dargestellt: Anstieg erwartet

65 %
(Sehr) hoher digitaler Reifegrad

75 %
Mittlerer/geringer digitaler Reifegrad

Frage: Würden Sie sagen, Ihr Compliance-Budget wird in den nächsten drei Jahren sinken, in etwa gleich bleiben, ansteigen oder stark ansteigen?

Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Sieben von zehn befragten Entscheidungsträgern gehen in den kommenden drei Jahren von einem **Anstieg des Compliance-Budgets für digitale Tools** in ihren Unternehmen aus (71 %). Vor allem solche, die ihren digitalen Reifegrad in der Studie als gering oder mittel einschätzen, beabsichtigen, zukünftig mehr in digitale Tools zu investieren (75 %), während dies Teilnehmer mit bereits hohem digitalem Reifegrad weniger häufig erwarten (65 %). Kaum eines der befragten Unternehmen plant dagegen zukünftig, das Budget für digitale Tools zu kürzen (1 %).

Auffällig ist, dass insbesondere **börsennotierte Unternehmen** ihre Digital-Tool-Budgets deutlich häufiger **aufstocken** wollen als nicht börsennotierte (84 % versus 69 %).

Aktuelles Budget

Obwohl fast jedes Zweite der befragten Unternehmen bereits von rechtlichen Risiken der Digitalisierung betroffen war, können oder wollen nur die wenigsten sich zur Budgetierung digitaler Tools innerhalb der Compliance äußern. Insgesamt scheint der Anteil am Gesamtbudget der Compliance noch vergleichsweise gering zu sein.

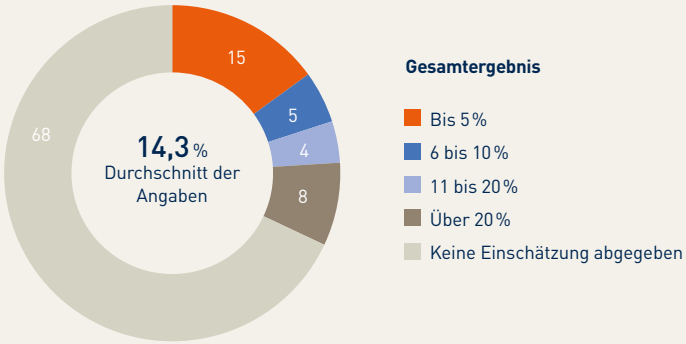
Nur knapp ein Drittel der befragten Führungskräfte äußert sich zum aktuellen Anteil des Compliance-Budgets, der für **digitale Compliance-Tools** eingesetzt wird (32 %). Dies gilt in ähnlicher Weise für die Befragten in Compliance-Positionen (38 %) oder in der Geschäftsführung (40 %). Dieser vergleichsweise große blinde Fleck ist bei den folgenden Ausführungen zu beachten.

Wenn man die Angaben derjenigen zugrunde legt, die eine Einschätzung vorgenommen haben, wird im Schnitt **jeder siebte Euro** des Compliance-Budgets der befragten Unternehmen (14,3 %) für digitale Tools eingesetzt. In größeren Unternehmen ist dieser Budgetanteil höher (17,2 %). Gleiches gilt für die Studienteilnehmer, die sich einen hohen digitalen Reifegrad zuschreiben (16,9 %).

Besonders Unternehmen, die bereits über eine **spezielle Position** für digitale Compliance-Risiken verfügen, investieren vergleichsweise mehr Geld in digitale Compliance-Tools. Hier wird **jeder fünfte Euro** (20 %) des Budgets für die Digitalisierung der Compliance-Prozesse ausgegeben.

Gut zwei Drittel können oder wollen keine Einschätzung abgeben

Compliance-Budget für digitale Tools



Frage: Welcher Teil des Compliance-Budgets Ihres Unternehmens wird für digitale Tools eingesetzt?

Basis: Alle Unternehmen; Angaben in Prozent Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

3.3 Einsatz von digitalen Compliance-Tools

Digitale Compliance-Tools: Übersicht und Systematik

Durch die fortschreitende digitale Transformation ergeben sich für Unternehmen neue Möglichkeiten, Compliance auch durch den Einsatz von digitalen Tools sicherzustellen bzw. zu erhöhen. Die Einsatzmöglichkeiten solcher digitalen Compliance-Tools sind vielfältig, die Palette der auf dem Markt verfügbaren Tools ist breit und wächst stetig. Deshalb soll hier ein **strukturierter Überblick** über die Möglichkeiten der Compliance-Sicherung durch digitale Compliance-Tools gegeben werden.

Nähert man sich der digitalen Compliance auf einer systematischen Ebene, lassen sich zwei methodische Ansätze identifizieren, die eine Grobunterteilung ermöglichen. So kann zwischen **Compliance by Design** und **Compliance by Detection** unterschieden werden. Das wesentliche Unterscheidungsmerkmal zwischen den beiden Ansätzen besteht darin, dass Compliance by Design die Compliance **proaktiv** sichern soll und Compliance by Detection **reaktiv** für Compliance sorgt.

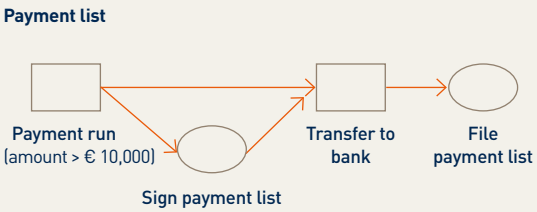
Diese Unterteilung findet sich ursprünglich insbesondere im Rahmen der automatisierten Compliance. Damit sind digitale Anwendungen beschrieben, die nicht nur manuelle Maßnahmen digitalisieren, sondern sie im besten Falle so abbilden, dass sie eine menschliche Aktivität nur noch zur Überwachung benötigen. Damit lassen sich jedoch nicht alle am Markt angebotenen digitalen Compliance-Tools abbilden. Zum Zweck der Systematisierung wird hier deshalb ein erweiterter Begriff von Compliance by Design und Compliance by Detection verwendet. Dadurch können auch diejenigen digitalen Tools, die nicht oder nur zu einem gewissen Grad automatisierbar sind, wie zum Beispiel das Richtlinienmanagement, mit diesen Begriffen abgebildet werden.

Compliance by Design

Compliance by Design ist als proaktives Konzept darauf ausgerichtet, es gar nicht erst zu Compliance-Verstößen kommen zu lassen. In einem (hypothetischen) perfekten Compliance-by-Design-System ist ein **Compliance-Verstoß von vorneherein ausgeschlossen**. Das System wäre dabei so geschaffen, dass es das Verhalten der Mitarbeiter derart überwacht und beschränkt, dass ein nicht rechtskonformes Verhalten nicht möglich ist. Dazu muss gerade beim Grundfall des automatisierten Compliance-by-Design-Systems **im Vorhinein klar definiert** sein, wie das jeweils erwünschte regelkonforme Verhalten auszusehen hat. Die Implementierung in das automatisierte Compliance-System kann dann auf zwei Arten erfolgen. Zum einen kann definiert werden, welches Verhalten erlaubt sein soll: Dann wäre durch das System kein abweichendes Verhalten möglich. Oder es kann definiert werden, welches Verhalten nicht gestattet ist, und entsprechendes Verhalten würde dann blockiert. Das bedeutet jedoch in beiden Fällen, dass alle denkbaren Szenarien schon erfasst und in das Programm gegossen sein müssen. Damit geht der **Nachteil** einher, dass das System keine Flexibilität zulässt und stetig an veränderte Anforderungen angepasst werden muss. In dem hier verwendeten weiteren Begriff von Compliance by Design sind jedoch wie oben beschrieben auch nicht automatisierte Compliance-Tools erfasst, die auch flexibler ausgestaltet sein können.

Die folgende Grafik zeigt beispielhaft den Freigabeprozess einer Bank bei Überweisungen in Höhe von über 10.000 Euro. Ein Programm überprüft Überweisungen darauf, ob sie einen Betrag von mehr als 10.000 Euro umfassen. Ist dies der Fall, wird die Transaktion zunächst gestoppt und einem Mitarbeiter vorgelegt. Erst nachdem dieser den Vorgang akzeptiert hat, kann die Transaktion abgeschlossen werden. Anschließend archiviert das Programm die Freigabe für spätere Überprüfungen.

Compliance Rule Graph Example



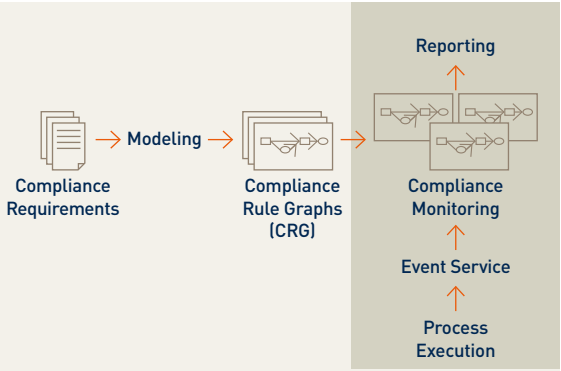
Before a payment list with amount beyond €10,000 is transferred to the bank, the payment list has to be signed by an officer. After being transferred to the bank, the payment list has to be filed for later audits.

Quelle: *Ly/Rinderle-Ma/Knuplesch/Dadam*, Monitoring Business Process Compliance Using Compliance Rule Graph

Compliance by Detection

Compliance by Detection hat als reaktives Konzept zum Ziel, Compliance-Verstöße nachträglich zuverlässig **aufzuspüren** und im besten Fall den Vorgang noch zu **unterbrechen**. Zudem sollten die Prozesse anschließend so umgestaltet werden, dass es nicht erneut zu dem gleichen Verstoß kommt. Hierin besteht zugleich ein **großer Vorteil** des Compliance-by-Detection-Ansatzes. Er ermöglicht umfassenden Handlungsspielraum und Flexibilität, da anders als bei Compliance by Design der erlaubte Verhaltenskorridor nicht bereits im Vorfeld klar festgelegt sein muss. Um alle verfüg- und denkbaren Möglichkeiten der reaktiven, nachträglichen Compliance zu erfassen, werden im Folgenden wie bei Compliance by Design von Compliance by Detection auch nicht automatisierte Tools erfasst. Ein Beispiel für ein solches nicht komplett automatisches Tool bildet ein digitales Hinweisgebersystem.

Die folgende Grafik zeigt auf der linken Seite, wie das Tool zur Compliance-Sicherung geschaffen wird, und auf der rechten Seite dessen Einsatz. Dieser beginnt bei der „Process Execution". In deren Rahmen kommt es zu Ereignissen („Event Services"), die im Punkt „Compliance Monitoring" durch das auf der rechten Seite geschaffene Modell automatisiert überprüft werden. Nach der Überprüfung erstellt das Programm einen Bericht und macht diesen den verantwortlichen Personen zugänglich. In diesem Bericht kann einerseits festgehalten sein, dass das Ereignis als rechtskonform eingestuft wird, oder dass andererseits eine Regelverletzung identifiziert wurde. Entsprechend können die verantwortlichen Personen auf das Ereignis reagieren und zum Beispiel den Ausgangsprozess anpassen.



Quelle: https://www.uni-ulm.de/in/iui-dbis/forschung/abgeschlossene-projekte/seaflows/ (zuletzt abgerufen am 02. August 2021).

Bei der Konzeption und Implementierung eines digitalen Compliance-Systems wird es in der **Praxis** kaum möglich sein, ausschließlich auf eines der beiden Konzepte zu setzen. Ziel muss stets sein, durch eine **Kombination von beiden Ansätzen** einen möglichst umfassenden Schutz vor Compliance-Verstößen zu erreichen. So dürfte es in manchen Geschäftsprozessen durchaus Sinn ergeben, einen Compliance-by-Design-Ansatz zu verfolgen, da aufgrund klarer Anforderungen keine Flexibilität erforderlich ist. Gleichzeitig kann es in anderen Bereichen vorteilhaft sein, den Prozessen im ersten Moment freien Lauf zu lassen, um sie anschließend „einzufangen", damit Regelkonformität hergestellt werden kann.

Compliance by Mapping

Neben den vorgestellten Konzepten von Compliance by Design und Compliance by Detection hat sich durch die Möglichkeiten der Digitalisierung die **Methode der Compliance by Mapping** herausgebildet. Diese kann einerseits zur **Konzeption** und andererseits zur **Überwachung** der Einhaltung der internen und gesetzlichen Regelungen eingesetzt werden. Compliance kann so mittels Mapping **ressourcenschonender, zeitsparender und allgemein effizienter** verwirklicht werden. Verbreitet ist dieses bereits auf dem Gebiet der Antikorruptions-Compliance und im Datenschutzrecht. Auch im Hinblick auf die IT-Sicherheit kann Mapping von Vorteil sein.

Zum einen wird mit Compliance by Mapping umschrieben, dass Bedrohungen identifiziert werden, die dann bestimmten Festsetzungen zugeordnet werden, um diesen in der Folge konkrete Compliance-Maßnahmen zuordnen zu können. Dies wurde vonseiten der Wissenschaft insbesondere für das Cloud-Computing vorgenommen. Die Autoren ordneten dort den verschiedenen Compliance-Maßnahmekatalogen einen Vorschlag für eine bestimmte Bedrohung sowie das betroffene Gebiet zu. Ein Beispiel aus der **Praxis** wäre hier das Unternehmen *exeon*. Dieses will seine Kunden bei der Sicherstellung der Compliance im Rahmen der Cyber-Security unterstützen. Dazu kann die Software zunächst auch komplexe Netzwerke visualisieren und Datenströme sichtbarer machen. So wird es erleichtert, die Compliance sicherzustellen, da unerwünschte Datenströme leicht erkannt werden können.

Soweit zum anderen ein Unternehmen vielen verschiedenen Regularien und Standards unterfällt, die zunächst zu identifizieren sind, bietet sich für dieses an, mittels Mapping eine einheitliche geordnete Liste an Voraussetzungen zu generieren, die nötig sind, um Compliance insgesamt zu erreichen. Denn Mapping erleichtert insbesondere, die verschiedenen Standards, Frameworks etc. einander gegenüberzustellen und Überschneidungen bzw. Überlappungen zu identifizieren. Hierauf haben sich bereits Anbieter spezialisiert, sodass ein Unternehmen dieses Mapping nicht selbst vornehmen muss, sondern auf Dienstleister zurückgreifen kann. Zu nennen sind für die IT-Sicherheit insbesondere die CIS Controls und CIS Benchmarks.

RegTechs

Im letzten Jahrzehnt hat sich eine **eigenständige Branche** entwickelt, die darauf ausgerichtet ist, Compliance-Prozesse digitaler zu gestalten. Gerade im Finanzsektor hat die Regulierungsdichte in den letzten Jahren, nicht zuletzt im Nachgang der globalen Banken- und Finanzkrise, stark zugenommen. Damit einhergehend ist auch der Bedarf nach entsprechenden digitalen Compliance-Tools besonders angestiegen. Unter dem Schlagwort „RegTech" hat sich eine Vielzahl von Start-ups darauf spezialisiert, Softwarelösungen zu entwickeln, die die Einhaltung der umfangreichen Gesetze und Regularien in der **Finanzbranche** erleichtern sollen. Aufgrund dieser Vorreiterrolle wird der Fokus in den ausgewählten Praxisbeispielen insbesondere auf Compliance-Tools für die Finanzbranche gelegt. Allerdings ist erkennbar, dass sich viele Angebote der RegTech-Unternehmen auch auf andere Branchen erweitern lassen.

Beispiele aus der Praxis

Die folgenden Praxisbeispiele illustrieren die Bandbreite der vielfältigen am Markt angebotenen digitalen Compliance-Tools. Untergliedert nach den verschiedenen Aufgaben, die die Tools wahrnehmen können, soll so ein Überblick über die Möglichkeiten für die digitale Compliance-Sicherstellung aufgezeigt werden.

Risikoanalyse: Risikoanalysen sind unerlässliche Bestandteile für die Sicherstellung von Compliance. Zum einen muss bereits im Ausgangspunkt geklärt werden, welche Compliance-Maßnahmen erforderlich sind. Zudem muss fortlaufend überprüft werden, ob die bisherige Risikoeinschätzung weiterhin gilt oder angepasst werden muss. Auf Basis der Risikoanalyse kann auch eingeschätzt werden, für welche Bereiche des Unternehmens ein Compliance-by-Design- bzw. Compliance-by-Detection-Ansatz sinnvoll ist.

So bietet beispielsweise das Unternehmen *risklytics* umfassende Datenanalysen zu Einschätzung der Risiken an. Dazu können verschiedene Daten live analysiert und so ein umfassendes Bild der Risikotragfähigkeit zur Verfügung gestellt werden.

Code of Conduct: Bei der Erstellung und vor allem Aktualisierung eines Code of Conduct können ebenfalls digitale Tools eingesetzt werden. So kann hier insbesondere das Überprüfen der gesetzlichen Vorgaben auf Neuerungen durch Software übernommen werden. Dadurch bleiben die Regelungen immer auf dem neuesten Stand.

Die Firma *APIAX* zum Beispiel geht hier noch einen Schritt weiter und stellt ihren Kunden maschinenlesbare Datenbanken zur Verfügung. So können die in Programmen implementierten Regeln ebenfalls automatisiert aktuell gehalten werden. Bei dieser Maßnahme handelt es sich um ein sehr gutes Beispiel für Compliance by Design im weiteren Sinne. Durch die Erstellung und Aktualisierung des Code of Conduct können zwar Compliance-Verstöße nicht absolut vermieden werden, aber es handelt sich um eine klassische präventive Maßnahme.

Unterrichtung der Mitarbeiter über den Kodex durch Schulungsmaßnahmen: Neben der fortlaufenden Aktualisierung der internen Regelungen müssen diese als weitere präventive Maßnahme an die Mitarbeiter kommuniziert werden. Auch zu diesem Zweck werden digitale Tools angeboten.

So werben die Macher der Software *Otris Compliance* damit, dass ihre GRC-Software nicht nur erlaubt, die internen Regelungen an die richtigen Stellen im Unternehmen zu verteilen, sondern auch zu überprüfen, ob diese von den Mitarbeitern tatsächlich gelesen wurden.

Zudem kann in diesem Bereich der Einsatz von E-Learning-Methoden gefasst werden. Im Rahmen von derartigen Unterrichtungen können die Mitarbeiter zu allen möglichen Themen der Compliance geschult werden.

Hinweisgebersystem: Eine Maßnahme zur reaktiven Sicherstellung der Compliance ist das Einrichten eines Hinweisgebersystems („Whistleblower-System"). Ein solches kann rein analog dadurch erstellt werden, dass eine Ombudsperson berufen wird, an die sich Whistleblower wenden könnten. Doch auch digital lässt sich ein entsprechendes System einrichten. Dieses könnte dabei insbesondere den Vorteil haben, dass die Schwelle für die hinweisgebende Person deutlich niedriger ist, zumal wenn der Hinweis anonym gegeben werden kann.

Ein webbasiertes Hinweisgebersystem bietet beispielsweise die Lösung *Trusty*. Ein weiterer Schritt könnte in diesem Bereich auch der Einsatz von Whistleblower-Chatbots sein.

Reportingsystem: Auch im Bereich des Reportings, also des Zusammenstellens von Berichten für die Unternehmensleitung, gibt es vermehrt digitale Tools. Damit soll den Entscheidungsträgern ermöglicht werden, jederzeit einen bestmöglichen Überblick über die Situation des Unternehmens zu haben. Digitale Reportingsysteme sind dabei darauf ausgerichtet, Daten automatisiert sichtbar zu machen und zugleich besonders übersichtlich darzustellen. Hierzu werden häufig Dashboards eingesetzt, die einen schnellen und möglichst intuitiven Überblick über eine Vielzahl an Kennzahlen ermöglichen.

Eine weitere Unterkategorie des Reportings ist das sogenannte Regulatory Reporting. Hierbei geht es nicht nur um die Meldung der Kennzahlen an die Unternehmensleitung, sondern zudem um die gesetzeskonforme Meldung an die zuständigen Aufsichtsbehörden. Entsprechende Dienste bietet beispielsweise die Firma *Cleversoft* an.

System zur Überwachung des Zahlungssystems: Ein Bereich, in dem Compliance-by-Design- und Compliance-by-Detection-Ansätze zugleich zum Einsatz kommen können, ist die Überwachung von Transaktionen. Dabei soll sichergestellt werden, dass weder die gesetzlichen Bestimmungen zur Geldwäsche noch zur Terrorismusfinanzierung unterlaufen werden.

In diesem Bereich ist beispielsweise das RegTech-Unternehmen *Clarus* tätig. Dieses erlaubt es Finanzinstituten, die Transaktionen ihrer Kunden überprüfen zu lassen. Dazu übermittelt das Institut die Daten der Transaktionen. Clarus analysiert die Daten automatisiert und sortiert verdächtige Vorgänge heraus. Diese können anschließend mithilfe von Clarus´ „Investigation Platform" weiter überprüft werden.

System zur Korruptionsverhinderung: Ein System zur Korruptionsverhinderung kann sowohl präventiv als auch reaktiv ausgelegt sein. Zum einen kann hier präventiv durch Schulungsmaßnahmen gerade auch per E-Learning gearbeitet werden, zum anderen lassen sich hier sehr gut automatisierte Compliance-by-Design-Tools einsetzen. So könnte in einem digitalen Prozess von den Mitarbeitern verlangt werden, dass sie jede Zuwendung, die sie von Geschäftspartnern erhalten, in einem System hinterlegen. Dieses prüft, ob die Zuwendung im Einklang mit dem Code of Conduct angenommen werden kann, und gibt der entsprechenden Person anschließend Rückmeldung.

So erklärt beispielsweise *BMW* im Jahresbericht 2020: „Die Mitarbeiterinnen und Mitarbeiter der BMW Group werden bei der Bewertung, Genehmigung und Dokumentation von Compliance-relevanten Vorgängen durch verschiedene IT-Systeme unterstützt. So müssen beispielsweise alle Austauschaktivitäten mit Wettbewerbern in einem speziellen Compliance-IT-System dokumentiert und genehmigt werden. Das Gleiche gilt für die Prüfung der rechtlichen Zulässigkeit von Zuwendungen und deren Dokumentation, insbesondere im Rahmen von Corporate Hospitality."

Know-Your-Costumer-System: Ein solches System (KYC) soll sicherstellen, dass Unternehmen keine Geschäfte mit Personen oder Firmen eingehen, die ein Compliance-Risiko darstellen, etwa weil sie auf einer Sanktionsliste stehen. Gleichzeitig ist das Ziel von KYC gerade auch die eindeutige Identifikation des Geschäftspartners. Das ist insbesondere im Finanzsektor relevant, wo die Verhinderung von Geldwäsche eine besondere Rolle spielt.

Das RegTech Unternehmen *GlobalPass* hat sich etwa auf den Bereich KYC spezialisiert. Eines der angebotenen Tools, „Name Search", erstellt dabei automatisiert eine Art Dossier zu einer gesuchten Person. Zu diesem Zweck werden nicht nur Fahndungslisten von Europol und Interpol überprüft, sondern auch Sanktionslisten und sogar Medien und soziale Netzwerke. So soll jede mögliche negative Berichterstattung sichtbar gemacht werden. Diese Dossiers können täglich aktualisiert werden. Ein weiteres Tool von *GlobalPass*„Real Time Screening", soll die Verifikation der Identität von Kunden und Geschäftspartnern sicherstellen.

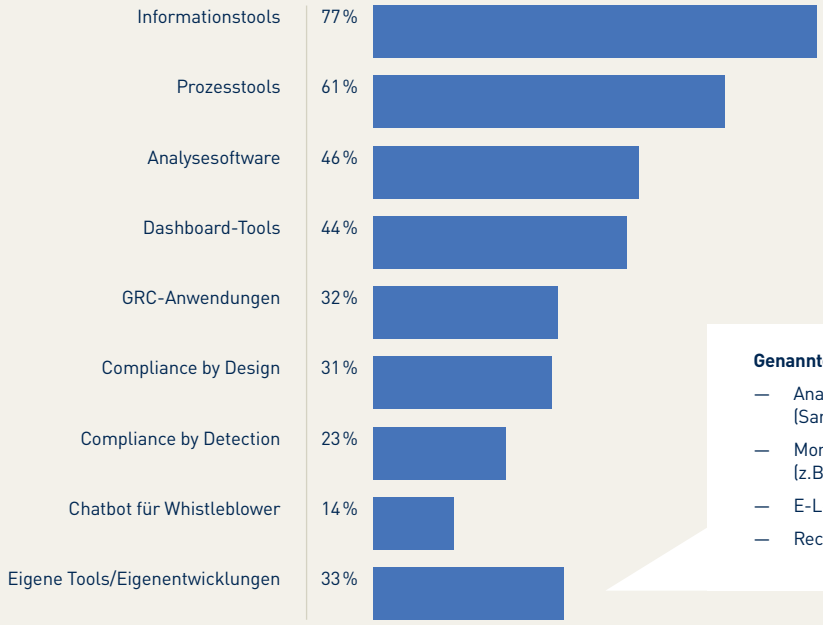
Weite Verbreitung von Informations- und Prozesstools

Informations- und Prozesstools sind weit verbreitet.

Die befragten Unternehmen setzen eine beachtliche Breite an Compliance-Tools ein.

Informationstools am weitesten verbreitet – ein Drittel verweist auf Eigenentwicklungen

Einsatz von Compliance-Tools und Vorgehensweisen im Unternehmen



Genannte Eigenentwicklungen:

- Analyse-, Detection-, Dokumentationstools (Sanktionslistenabgleich, Risikoanalysen)
- Monitoring-Tools (z.B. Dashboards, Prozessanalyse)
- E-Learning-Plattformen, Prävention
- Rechte- und Freigabeverwaltung

Frage: Welche Compliance-Tools und Vorgehensweisen setzen Sie ein?
Basis: Alle Unternehmen; Mehrfachnennungen möglich; Angaben in Prozent
Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Mit Abstand am häufigsten setzen die Befragten **Informationstools** ein, also beispielsweise Schulungssoftware oder E-Learning-Angebote für die Mitarbeiter. So schulen mehr als drei Viertel der Studienteilnehmer (77 %) ihre Beschäftigten mithilfe solcher Tools hinsichtlich wesentlicher Compliance-Anforderungen. Besonders in **börsennotierten und größeren Unternehmen sowie in Unternehmen mit ausländischem Mutterkonzern** gehören Compliance-Informationstools mit jeweils über **80 %** praktisch zum **Standardrepertoire** (86 % der börsennotierten Unternehmen, 82 % der größeren Unternehmen mit über 1.000 Beschäftigten, 85 % der Unternehmen mit ausländischem Mutterkonzern).

Auch **Prozesstools**, die etwa mittels Checklisten die Einhaltung rechtlicher Vorgaben abfragen, setzen die befragten Entscheidungsträger vergleichsweise oft ein (61 %), um möglichen Rechtsverstößen bereits im laufenden Produktions- oder Vertriebsprozess vorzubeugen.

Bei den **börsennotierten Unternehmen** und solchen mit ausländischer Konzernmutter geben sogar **mindestens zwei Drittel** der Entscheider an, in ihrem Unternehmen Prozesstools einzusetzen (67 % beziehungsweise 71 %).

Analysesoftware zum Aufzeigen von Compliance-Verstößen und **Dashboard-Tools**, die Prozessdaten aus unterschiedlichen Quellen zusammenfassen und optisch aufbereiten, setzen die befragten Unternehmen dagegen mehrheitlich nicht ein (lediglich 46% beziehungsweise 44% nutzen diese Tools). Ausnahmen bilden Unternehmen, deren **Mutterkonzern im Ausland** sitzt, die überwiegend auf solche Anwendungen setzen, um Compliance-Risiken zu reduzieren. So verwenden **54 %** Analysesoftware und **58 %** Dashboard-Tools.

Zurückhaltender ist der Einsatz von komplexeren GRC-Anwendungen oder speziellen IT-Systemen. **GRC-Anwendungen**, die über die Identifizierung, Analyse und Aufnahme von regulatorischen Anforderungen neben der Compliance auch Governance und Risk-Management unterstützen, sowie IT-Systeme, die qua Design so strukturiert sind, dass Compliance-Verstöße zumindest unwahrscheinlicher werden (**Compliance by Design**), nutzt knapp jedes dritte befragte Unternehmen. Die eher retrospektiv angelegten IT-Systeme, die Unternehmensprozesse und Mitarbeiterverhalten umfassend aufzeichnen, um dann rückwirkend Verstöße feststellen zu können (**Compliance by Detection**), wendet dagegen nur knapp jedes Vierte der befragten Unternehmen an (23 %).

Eine eher untergeordnete Rolle im Rahmen der Compliance-Tools spielen **Whistleblower-Chatbots**. Hintergrund dieser Anwendungen ist die „EU-Whistleblowing-Richtlinie" ((EU) 2019/1937), die seit Ende 2019 in Kraft ist und die es Whistleblowern ermöglichen soll, Missstände im Unternehmen ohne Furcht vor Repressalien zu melden. Nach den Vorgaben der Richtlinie müssen Unternehmen mit mindestens 50 Beschäftigten interne Meldekanäle einrichten, über die Personen mit Bezug zum jeweiligen Unternehmen auf Verstöße gegen Unionsrecht hinweisen können (Art. 8). Diese internen Meldekanäle müssen so konzipiert sein, dass die Identität des Hinweisgebers geschützt bleibt (Art. 16). Zur fristgerechten Umsetzung der EU-Whistleblowing-Richtlinie zum 17. Dezember 2021 (für Unternehmen von 50 bis 249 Beschäftigten bis zum 17. Dezember 2023) hat das Bundesministerium für Justiz bereits einen Entwurf für ein nationales Hinweisgeberschutzgesetz (HinSchG) vorgelegt. Auch wenn die Unternehmen nach der EU-Whistleblowing-Richtlinie die Art des Meldekanals (analog oder digital) frei auswählen können (vgl. Erwägungsgrund 53), haben sich digitale Hinweisgebersysteme wie Chatbots bislang noch nicht durchgesetzt. Sie werden derzeit nur in jedem siebten befragten Unternehmen eingesetzt (14 %). **Börsennotierte Unternehmen** verwenden sie allerdings doppelt so häufig (28 %). Auch knapp jedes fünfte größere Unternehmen mit mindestens 1.000 Beschäftigten (19 %) gibt an, bereits solche KI-gestützten Hinweisgebersysteme einzusetzen, während nur knapp jedes zehnte kleinere Unternehmen solche Systeme nutzt (9 %).

Jedes dritte Unternehmen gibt zudem an, **eigens entwickelte Compliance-Tools** einzusetzen. Dabei handelt es sich zumeist um firmeneigene Analyse-, Detection- und Dokumentationstools sowie spezielle Tools, beispielsweise zum Monitoring oder zur digitalen Rechte- und Freigabeverwaltung.

Erwartungsgemäß sind fast alle digitalen Tools in den befragten Unternehmen mit hoher digitaler Reife und insbesondere in Firmen, in denen eine spezielle Position für digitale Compliance-Risiken vorhanden ist, stärker verbreitet als in Unternehmen mit geringerem digitalem Reifegrad (im Schnitt +7 Prozentpunkte) beziehungsweise ohne eine dedizierte Digital-Compliance-Position (im Schnitt +10 Prozentpunkte).

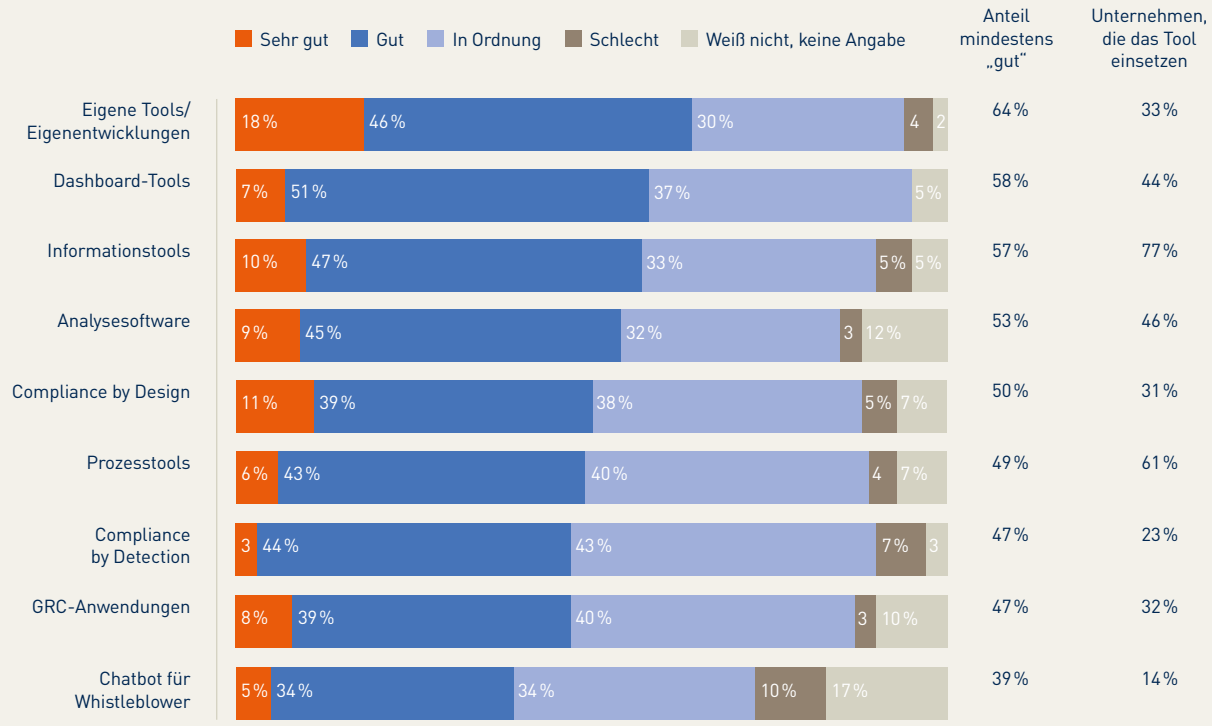
Zufriedenheit

Flexible Tool-Lösungen, die die jeweiligen Compliance-Bedürfnisse eines Unternehmens ausreichend abbilden, scheinen oftmals zu fehlen.

Die Zufriedenheit mit den eingesetzten Compliance-Tools schwankt zwischen den Befragten. Flexible Tool-Lösungen, die die jeweiligen Compliance-Bedürfnisse eines Unternehmens ausreichend abbilden, scheinen noch oftmals zu fehlen. Hierfür spricht, dass viele der befragten Unternehmen speziell eigene Compliance-Tools entwickelt haben und mit diesen, im Vergleich zu anderen Lösungen, deutlich öfter zufriedener sind.

Beurteilung eingesetzter Compliance-Tools

Spezialisierte Eigenentwicklungen schneiden am besten ab – gemischte Bewertungen für Chatbots



Frage: Wie sind Ihre bisherigen Erfahrungen mit den von Ihnen eingesetzten Compliance-Tools und Vorgehensweisen?

Basis: Jeweiliges Tool wird eingesetzt; für den Anteil Unternehmen, die das jeweilige Tool im Einsatz haben, ist die Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Knapp zwei Drittel der befragten Unternehmen, die **selbstentwickelte Compliance-Tools** einsetzen, beurteilen diese als **gut oder sogar als sehr gut** (46 % beziehungsweise 18 %).

Mit **Dashboard-Tools**, **Informationstools** und **Analysesoftware** ist ebenfalls noch jeweils die Mehrheit der befragten Führungskräfte zufrieden (zwischen 58 % und 54 % „gut“ beziehungsweise „sehr gut“). IT-Systeme nach dem Prinzip **Compliance by Design** beziehungsweise **Compliance by Detection** sowie **Prozesstools** und **GRC-Anwendungen** bekommen immerhin noch von etwa von der Hälfte der Befragten gute Bewertungen (zwischen 47 % und 50 %).

Whistleblower-Chatbots bewerten die Führungskräfte dagegen als vergleichsweise negativ. Immerhin jeder zehnte Befragte stellt solchen Tools ein schlechtes Zeugnis aus. Jedenfalls hat jede sechste Führungskraft Schwierigkeiten, hier überhaupt eine Beurteilung vorzunehmen (17 %).

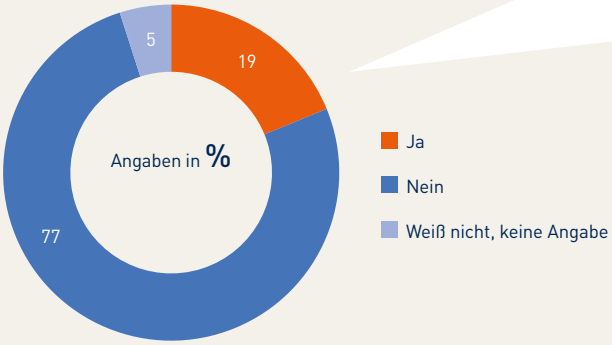
Risikobewusstsein

Der Umstand, dass der Einsatz von Compliance-Tools selbst mit Risiken für Unternehmen einhergehen kann, wird oftmals nicht erkannt.

Compliance-Risiken durch Compliance-Tools

Eines von fünf Unternehmen berichtet von kritischen Stimmen

Gibt es in Ihrem Unternehmen auch Stimmen, wonach die Nutzung der Compliance-Tools selbst neue Compliance-Risiken hervorbringt?



Detailergebnisse
Anteil „Ja"

Unternehmen mit **unter 1.000 Mitarbeitern**	16%
Unternehmen mit **1.000 Mitarbeitern und mehr**	22%
Unternehmen mit **Sitz in Deutschland**	16%
Unternehmen mit **Sitz im Ausland**	32%

Frage: Gibt es in Ihrem Unternehmen auch Stimmen, wonach die Nutzung der Compliance-Tools selbst neue Compliance-Risiken hervorbringt?

Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Der **weit überwiegende Anteil** gibt an, dass in ihrem Unternehmen nicht diskutiert wird, ob der Einsatz von Compliance-Tools selbst mit Compliance-Risiken einhergeht (77 %). Nur in jedem Fünften der befragten Unternehmen gibt es Stimmen, die in der Nutzung von Compliance-Tools entsprechende Risiken sehen (19 %).

Am häufigsten werden die Bedenken bei den Entscheidungsträgern in den Compliance-Abteilungen platziert (23 %). In der Geschäftsführung oder dem Vorstand kommen diese Stimmen dagegen scheinbar seltener an (11 %).

In **größeren Unternehmen** mit 1.000 oder mehr Beschäftigten sowie in **börsennotierten Unternehmen** sind diese Stimmen etwas lauter als in kleineren und nicht gelisteten Unternehmen (22 % beziehungsweise 24 % versus 16 % beziehungsweise 18 %).

In **Unternehmen mit Sitz im Ausland** wird dieses Problem offenbar wesentlich häufiger thematisiert. Jeder dritten befragten Führungskraft sind in solchen Unternehmen bereits entsprechende Einschätzungen zu Ohren gekommen (32 %).

4. Digitale Compliance während der Covid-19-Pandemie

Die Covid-19-Pandemie setzt Unternehmen auf vielfältige Art und Weise starken Belastungen aus. Insbesondere wirkt sie sich auch auf die digitale Compliance der Unternehmen aus. So hat die Covid-19-Pandemie beispielsweise die Nutzung digitaler Arbeitsmittel in bis dahin unbekanntem Umfang gefördert. Zugleich führte die Krise zu einem flächendeckenden Zuwachs an Homeoffice-Arbeitsplätzen. Dementsprechend ist ein Blick lohnenswert, wie die befragten Unternehmen den vermehrten Einsatz digitaler Arbeitsmittel bewerten und ob die Covid-19-Pandemie notgedrungen zu Lockerungen in den internen Compliance-Richtlinien geführt hat.

Die Rückmeldungen zu den beiden Themengebieten sind durchaus unterschiedlich. Auch wenn die digitalen Helfer aus dem heutigen Arbeitsalltag nicht mehr wegzudenken sind, haben viele der befragten Unternehmen bei ihrem Einsatz Compliance-Bedenken. Dass die Pandemie zu Lockerungen im Umgang mit Compliance-Richtlinien geführt hätte, kann ein Großteil der befragten Unternehmen nicht bestätigen, wenngleich sie im Branchenumfeld solche Lockerungen wahrgenommen haben.

4.1 Compliance-Risiken digitaler Arbeitsmittel

Einsatz digitaler Arbeitsmittel trotz Compliance-Bedenken verbreitet.

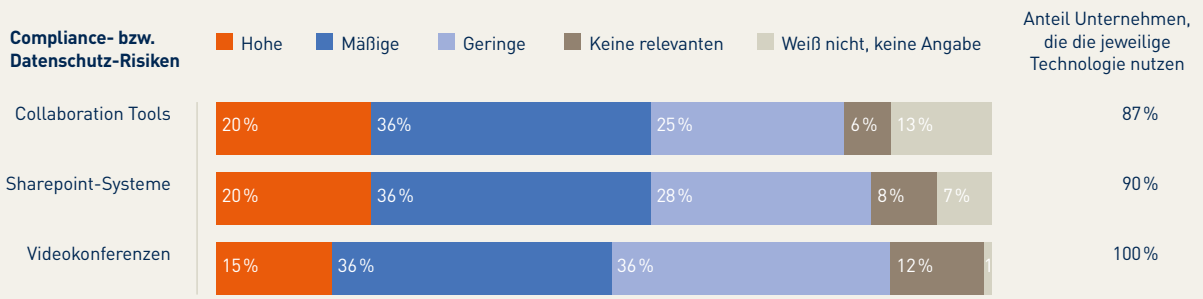
Digitale Arbeitsmittel sind auch wegen der Covid-19-Pandemie aus dem heutigen Arbeitsalltag nicht mehr wegzudenken. Dies gilt insbesondere für Collaboration- und Conferencing-Tools, die die ortsunabhängige Zusammenarbeit per Audio- oder Videokonferenz, Chats oder die gemeinsame Dateibearbeitung ermöglichen.

Fast keines der befragten Unternehmen verzichtet völlig auf Video-Conferencing in der einen oder anderen Form. Auch Sharepoint-Systeme und Collaboration-Tools kommen inzwischen bei etwa neun von zehn Studienteilnehmern zum Einsatz. In **börsennotierten Unternehmen** liegen die Nutzeranteile sogar noch höher (95 % beziehungsweise 98 %).

So komfortabel diese Tools auch zu benutzen sind, birgt ihre Verwendung rechtliche Risiken insbesondere für den Datenschutz. Denn mit der Nutzung von Cloud-Lösungen kann die Übermittlung personenbezogener Daten in Länder verbunden sein, in denen kein angemessenes Datenschutzniveau besteht. Die Verarbeitung des Nutzerinputs (etwa die Kommunikation in einem virtuellen Meeting oder das Teilen von Inhalten) erfolgt auf zentralen Servern des Anbieters, die über die ganze Welt verteilt sein können. Nach dem Urteil des Europäischen Gerichtshofs vom 16. Juli 2020 (Rs. C 311/18 – Schrems II) können sich Unternehmen jedoch nicht mehr auf die vertragliche Zusagen des Providers verlassen, sondern müssen prüfen, ob die vertraglichen Pflichten vom Datenimporteur auch tatsächlich eingehalten werden können und die übermittelten Daten vor dem Zugriff ausländischer Sicherheitsbehörden geschützt sind.

Compliance-Risiken digitaler Arbeitsmittel im Bereich Datenschutz

Jeweils mindestens ein Fünftel hat größere Bedenken – trotzdem finden die Technologien breite Verwendung



Frage: Wie schätzen Sie die Compliance-Risiken der folgenden digitalen Arbeitsmittel – insbesondere im Bereich Datenschutz – ein?

Basis: Unternehmen, die die jeweilige Technologie nutzen; für den Anteil Unternehmen, die die jeweilige Technologie im Einsatz haben, ist die Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Viele Unternehmen sind sich dabei der Compliance-Risiken der verschiedenen digitalen Arbeitsmittel – insbesondere im Bereich Datenschutz – durchaus bewusst. In jeweils der **Mehrzahl der befragten Unternehmen**, in denen die abgefragten Technologien auch im Einsatz sind, wird von **zumindest mäßigen, wenn nicht hohen Compliance- beziehungsweise Datenschutzrisiken** durch die Nutzung von Collaboration-Tools, Sharepoint-Systemen und Videokonferenz-Tools ausgegangen (51 % bis 56 %).

Größere Datenschutzbedenken äußern die Befragten vor allem im Hinblick auf **Collaboration-Tools** für die Teamarbeit wie etwa Teams, Slack oder Trello, die eine gemeinsame Dokumentbearbeitung, Projekt-Chats oder ein zentrales Aufgabenmanagement gemeinsamer Projekte ermöglichen, aber auch hinsichtlich der für die unternehmensweite Dateiablage und Kommunikation und oft als Intranet genutzten **Sharepoint-Systeme**. Jede fünfte befragte Führungskraft (jeweils 20 %) sieht hier hohe Compliance- beziehungsweise Datenschutz-Risiken.

Vor allem die Experten der **IT-Abteilungen** halten diese aus Compliance-Sicht für riskant. Jeweils **mehr als zwei Drittel** der befragten IT-Entscheider haben hier **Bedenken hinsichtlich des Datenschutzes und der Compliance** (68 % beziehungsweise 72 %). **33 %** der IT-Entscheider haben hinsichtlich der Compliance und **27 %** hinsichtlich des Datenschutzes sogar große Bedenken. Ein erhöhtes Risikobewusstsein im Hinblick auf Collaboration-Tools und Sharepoint-Systeme haben auch befragte Unternehmen mit hohem oder sehr hohem digitalem Reifegrad (jeweils 60 % mäßiges beziehungsweise hohes Risiko).

Videokonferenzen gelten dagegen als etwas weniger riskant. Obwohl über die entsprechenden Conferencing-Tools Gesprächsinhalte digital verfügbar und teilbar werden und der jeweilige Teilnehmerkreis relativ einfach erweiterbar ist, stellen sie nur für **15 %** der befragten Entscheider ein großes und für **36 %** ein zumindest nicht zu vernachlässigendes Risiko dar. Auffällig ist hier die vergleichsweise große Awareness der befragten Unternehmen, deren Mutterkonzern im Ausland sitzt. Mehr als drei von fünf Studienteilnehmern befürchten zumindest mäßige, fast jeder Fünfte sogar hohe Risiken (63 % beziehungsweise 19 %).

4.2 Überwiegend keine Lockerungen von Compliance-Richtlinien

Kaum Lockerungen von Compliance-Richtlinien während der Covid-19-Pandemie.

Die Covid-19-Pandemie hat Unternehmen auf vielfältige Weise starken Belastungen ausgesetzt. In diesem Zusammenhang stellt sich die Frage, ob die Gefahr möglicher Umsatzeinbußen oder behördliche Auflagen dazu geführt haben, dass Unternehmen

ihren Umgang mit internen Richtlinien wegen der Covid-19-Pandemie gelockert haben. Dies scheint nach den Rückmeldungen auf den weit überwiegenden Anteil der Befragten nicht zuzutreffen.

Allerdings hat etwas mehr als **jede fünfte Führungskraft im eigenen Branchenumfeld beobachtet**, dass im Zuge der Covid-19-Pandemie Compliance-Richtlinien gelockert oder gar außer Kraft gesetzt wurden (22 %).

Besonders oft fielen solche Lockerungen regulatorischer oder interner Standards den Befragten in **kleineren Unternehmen** mit weniger als 1.000 Beschäftigten auf (26 %). Die Befragten in größeren Unternehmen mit 1.000 oder mehr Beschäftigten berichten dagegen seltener von krisenbedingten Aufweichungen von Compliance-Richtlinien (18 %).

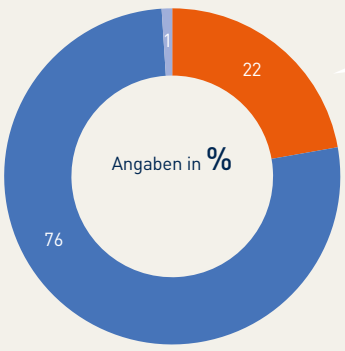
Auffällig ist auch, dass offenbar im Branchenumfeld **börsennotierter Unternehmen** weitaus weniger Compliance-Richtlinien während der Covid-19-Pandemie gelockert werden. Hier hat nur etwas mehr als jede Zehnte der befragten Führungskräfte eine pandemiebedingte Lockerung von Compliance-Richtlinien wahrgenommen (12 %). In den befragten Unternehmen ohne Börsennotierung war der Anteil demgegenüber doppelt so hoch (24 %).

Ob diese Rückmeldungen vor dem Hintergrund der extremen Herausforderungen der letzten Monate ein realistisches Abbild darstellen, kann man durchaus kritisch hinterfragen. Hierfür spricht zum Beispiel der hohe Anteil an Homeoffice, der seinerseits insbesondere arbeits- und datenschutzrechtliche Implikationen mit sich bringt. Es ist zu vermuten, dass die Dunkelziffer der Lockerungen von Compliance-Richtlinien im Zuge der Covid-19-Pandemie durchaus höher ausfällt.

Lockerung von Compliance-Richtlinien während der Corona-Krise

Insbesondere in kleineren Unternehmen wird von Lockerungen berichtet

Lockerung/Außerkraftsetzung von Richtlinien im Branchenumfeld beobachtet



Detailergebnisse
Anteil „Ja"

Unternehmen mit **unter 1.000 Mitarbeitern**	26 %
Unternehmen mit **1.000 Mitarbeitern und mehr**	18 %
Unternehmen mit **Sitz in Deutschland**	12 %
Unternehmen mit **Sitz im Ausland**	24 %

Frage: Seit mehr als einem Jahr müssen die Unternehmen in Deutschland mit den Folgen der Corona-Pandemie umgehen. Haben Sie in Ihrem Branchenumfeld beobachtet, dass im Zuge der Corona-Krise Compliance-Richtlinien außer Kraft gesetzt oder gelockert wurden?

Basis: Alle Unternehmen; Angaben in Prozent

Quelle: Kantar – Quantitative Befragung 2021 im Auftrag von Noerr

Studiendesign

Im Auftrag von Noerr führte Kantar Public im Zeitraum von März bis Mai 2021 telefonische Befragungen von verantwortlichen Personen in Unternehmen in Deutschland durch. Zielgruppe waren die Führungskräfte der ersten und zweiten Ebene in privatwirtschaftlichen Unternehmen ab 250 Mitarbeitern. Die Fragebögen für die Interviews wurden von Noerr in Zusammenarbeit mit der Technischen Universität München erstellt. In diesen Bericht sind die Ergebnisse von insgesamt 300 Interviews eingeflossen, die Kantar Public durchführte.

Bei der Darstellung der Ergebnisse ist in methodischer Hinsicht Folgendes zu beachten: Da die dargestellten Anteilswerte auf ganze Zahlen gerundet sind, kann es vorkommen, dass sie sich nicht zu 100 % aufsummieren. Aus demselben Grund können durch Addition zusammengefasste Kategorien (zum Beispiel sogenannte „Top-Two-Werte" wie „sehr zufrieden" und „eher zufrieden") von der Summe der dargestellten Einzelkategorien abweichen. Bei Fragen mit mehreren Antwortoptionen können die aufaddierten Nennungen 100 % überschreiten. Die Prozentsätze im Text beziehen sich auf die Ergebnisse der Umfrage. Besonders wichtige Resultate der Studie sind zudem grafisch dargestellt.

Über den Lehrstuhl für Recht und Sicherheit der Digitalisierung – Prof. Dr. Dirk Heckmann

Mit der Leuchtturmberufung des Staatsrechtlers und Internetrecht-Pioniers Dirk Heckmann an die TU München im Oktober 2019 wurde der Lehrstuhl für Recht und Sicherheit der Digitalisierung als Joint Appointment der TUM School of Governance und der Fakultät für Informatik neu eingerichtet. Mit diesem Lehrstuhl betont die Technische Universität München (**TUM**) die besondere Bedeutung der Rechtswissenschaften insbesondere im interdisziplinären Schnittfeld der Digitalisierung zwischen Technik, Gesellschaft und Regulierung. Vor diesem Hintergrund wurden mittlerweile weitere Professuren mit juristischem Bezug an der TUM besetzt, so etwa zu Legal Tech oder Digital Commerce. Ab Oktober 2021 bildet der Lehrstuhl von Prof. Heckmann eine wichtige Säule in der neu gegründeten School of Social Science and Technology.

Mit seinem mittlerweile auf rund 15 Personen angewachsenen Team von Mitarbeiterinnen und Mitarbeitern widmet sich Prof. Heckmann schwerpunktmäßig den Grundlagen des Rechts in der digitalen Gesellschaft, Legal Tech und Rechtsfragen der Entwicklung und des Einsatzes künstlicher Intelligenz. KI in der Hochschulbildung betrifft gleichermaßen einen Schwerpunkt der vom Lehrstuhl übergreifend angebotenen Lehre als auch eine Nachwuchsforschergruppe – beides geleitet vom Postdoc am Lehrstuhl, Dr. Lorenz Marx.

Um den Bereichen digitale Verwaltung, digitale Bildung und Digitalisierung im Gesundheitswesen ein noch größeres Gewicht zu verleihen, errichtete Prof. Heckmann gemeinsam mit seiner Geschäftsführerin Sarah Rachut im Juni 2020 das TUM Center for Digital Public Services, für das das Bayerische Staatsministerium für Digitales die Anschubfinanzierung übernahm. Sie ist als Forschungsstelle in den Lehrstuhl integriert.

Die zahlreichen Publikationen, die Prof. Heckmann bereits in seiner Zeit als Universitätsprofessor an der Universität Passau verantwortete, werden vom Lehrstuhl an der TUM weiter betreut – allen voran der „juris Praxis Kommentar Internetrecht. Das Recht der Digitalisierung", den Heckmann seit der 7. Auflage 2021 gemeinsam mit seiner Kollegin Anne Paschke (TU Braunschweig) herausgibt und an dem u.a. auch Dr. Marx als Autor beteiligt ist.

Mit der Kanzlei Noerr verbinden bereits der frühere Passauer Lehrstuhl und nunmehr auch die TUM enge Verbindungen in Forschung und Lehre. Das betrifft u.a. die Beteiligungen von Heckmann/Paschke am „Rechtshandbuch Internet of Things" von Bräutigam/Kraul (2021) oder auch den Beitrag von Heckmann am Standwerk „IT-Outsourcing und Cloud Computing" (4. Aufl. 2019).

Über Noerr

Noerr ist Exzellenz und unternehmerisches Denken. Mit Teams aus starken Persönlichkeiten findet Noerr Lösungen für komplexe und anspruchsvolle Fragestellungen. Vereint durch gemeinsame Werte, haben die über 500 Berater bei Noerr ein gemeinsames Ziel: den Erfolg der Mandanten. Auf den Rat der Kanzlei vertrauen börsennotierte Konzerne und mittelständische Unternehmen ebenso wie Finanzinstitute und -investoren.

Unternehmerisches Denken

Die Berater von Noerr machen die Herausforderungen ihrer Mandanten zu ihren eigenen. Sie denken nicht nur mit, sondern auch voraus. Dabei sind sie frei in ihren Entscheidungen und übernehmen Verantwortung. Noerrs Anspruch ist es, für den Mandanten immer einen Schritt weiter zu gehen. Und komplexe Fragestellungen mit Erfahrung, Exzellenz und Augenmaß zu lösen.

Innovative Lösungen

In komplexen und dynamischen Märkten sind regelmäßig neue Lösungsansätze gefragt. Von Experten, die neben dem Know-how auch die nötige Leidenschaft mitbringen. Das ist Noerrs Domäne: integrierte und innovative Lösungen, effizient umgesetzt.

Globale Reichweite

Um sich wirklich grenzenlos für Mandanten einsetzen zu können, ist Noerr als eine führende europäische Kanzlei auch international bestens aufgestellt: mit Büros in elf Ländern und einem weltweiten Netzwerk an befreundeten Top-Kanzleien.

Zudem ist Noerr exklusives deutsches Mitglied von Lex Mundi, dem global führenden Netzwerk unabhängiger Kanzleien mit umfangreicher Erfahrung in mehr als 100 Ländern.

Kompetent in Mittel- und Osteuropa

Seit Langem ist Noerr in allen wesentlichen Hauptstädten Mittel- und Osteuropas vertreten. Regelmäßig berät die Kanzlei deutsche und internationale Investoren bei Greenfield Investments, Joint Ventures, Akquisitionen und Desinvestitionen in Mittel- und Osteuropa. Mit über 100 Professionals gehört Noerr zu den führenden Kanzleien in der Region.

Noerr-Gruppe

Noerr PartGmbB – Noerr Consulting AG – TEAM Treuhand GmbH – NOERR AG Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

Standorte

Alicante, Berlin, Bratislava, Brüssel, Budapest, Bukarest, Dresden, Düsseldorf, Frankfurt, Hamburg, London, Moskau, München, New York, Prag, Warschau

Autoren

Prof. Dr. Peter Bräutigam

Rechtsanwalt und Fachanwalt für IT-Recht
Partner und Co-Head des Fachbereichs Commercial

T +49 89 28628145
peter.braeutigam@noerr.com

Prof. Dr. Peter Bräutigam ist ausgewiesener Spezialist auf dem Gebiet des Rechts der Informationstechnologie. Sein Beratungsspektrum umfasst alle Fragestellungen des IT-Rechts und der Digitalisierung/Industrie 4.0 mit folgenden Schwerpunkten: IT-Outsourcing-/BPO-Verträge, Rahmen- und Projektverträge und Service Level Agreements, Datenschutz, Recht an Daten, Cyber-Security, Haftungsfragen, (Software-)lizenzrechtliche Themen und Problemstellungen im IP-Umfeld. Prof. Dr. Peter Bräutigam ist Honorarprofessor für Medien- und Internetrecht an der Universität Passau und veröffentlicht regelmäßig in diesen Rechtsgebieten (z.B. ist er (Mit-)Herausgeber der Rechtshandbücher „IT-Outsourcing und Cloud Computing", „E-Commerce" und „Internet of Things"). Er ist u.a. stellvertretender Vorstandsvorsitzender der Gesellschaft für Recht und Informatik, stellvertretender Verwaltungsratsvorsitzender der Stiftung Datenschutz und Mitherausgeber der NJW.

Dr. Julia Sophia Habbe

Rechtsanwältin
Partnerin
Co-Head der Praxisgruppe Compliance & Interne Ermittlungen

T +49 69 971477252
sophia.habbe@noerr.com

Dr. Julia Sophia Habbe leitet gemeinsam mit Dr. Torsten Fett die Praxisgruppe Compliance & interne Ermittlungen.

Sie verfügt über umfangreiche Erfahrungen bei komplexen behördlichen und internen Untersuchungen und berät im Nachgang hierzu im Bereich des Prozess- und Krisenmanagements. Julia Sophia Habbe vertritt börsennotierte und inhabergeführte Unternehmen und deren Organe bei Compliance-Vorfällen, insbesondere im Bereich der Organverantwortung und in Haftungsfragen. Ein weiterer Schwerpunkt ihrer Praxis liegt in der Beratung zu gesellschafts- sowie kapitalmarktrechtlichen Fragestellungen, einschließlich der Prozessführung in Rechtsstreitigkeiten vor Aufsichtsbehörden und Gerichten.

Sie veröffentlicht regelmäßig zu Themen an der Schnittstelle von Gesellschafts-, Kapitalmarkt- und Zivilprozessrecht.

Dr. Philipp Gergen, LL.M. (Exeter)

Rechtsanwalt
Associated Partner

T +49 69 971477219
philipp.gergen@noerr.com

Dr. Philipp Gergen ist Associated Partner und berät nationale und internationale Mandanten in komplexen behördlichen und internen Untersuchungen. Die Schnittstelle zwischen Compliance-relevanten und technischen beziehungsweise digitalen Fragestellungen bildet dabei einen Schwerpunkt seiner Tätigkeit. Darüber hinaus verfügt Dr. Philipp Gergen über vertiefte Erfahrungen im Bank- und Kapitalmarktrecht sowie als Prozessanwalt vor deutschen Gerichten. Spezielle Branchenkenntnisse besitzt er unter anderem im Bank- und Automobilsektor.

Andreas Daum, LL.M. (LSE)

Rechtsanwalt
Associate

T +49 89 28628466
andreas.daum@noerr.com

Andreas Daum, LL.M. (LSE) ist spezialisiert auf die rechtliche Beratung bei Digitalisierungsprozessen und komplexen IT-Projekten nationaler und internationaler Mandanten in diversen Branchen und der öffentlichen Hand (insbesondere agile Softwareentwicklung, IT-Outsourcing, Cloud-Computing, Automatisierung von Unternehmensprozessen, Datenschutz) sowie auf die rechtliche Beratung im Zusammenhang mit Software as a Service (SaaS), Datennutzungs-Verträgen, Cyber-Security, IT-Transaktionen und Software-Urheberrecht.

Prof. Dr. Dirk Heckmann

Prof. Dr. Dirk Heckmann war seit 1996 Inhaber des Lehrstuhls für Öffentliches Recht, Sicherheitsrecht und Internetrecht an der Universität Passau, bevor er im Oktober 2019 einem Ruf an die Technische Universität München auf den neu errichteten Lehrstuhl für Recht und Sicherheit der Digitalisierung folgte. Seine Lehr- und Forschungsschwerpunkte liegen im Schnittfeld von IT und Recht, insbesondere im Datenschutzrecht, IT-Sicherheitsrecht, E-Government, E-Health und digitale Bildung. 2003 wurde Heckmann zum nebenamtlichen Verfassungsrichter am Bayerischen Verfassungsgerichtshof gewählt, 2007 in den Expertenkreis des Nationalen IT-Gipfels der Bundesregierung und 2018 in die Datenethikkommission der Bundesregierung berufen. Seit 2018 ist er Direktor am Bayerischen Forschungsinstitut für Digitale Transformation bidt und seit 2020 Direktor des TUM Center for Digital Public Services. Von 2007 bis 2021 war Heckmann Mitglied des Vorstands der Deutschen Gesellschaft für Recht und Informatik, von 2014 bis 2021 deren Vorsitzender.

Dr. Lorenz Marx, LL.M.

Dr. Lorenz Marx, LL.M. (KCL) ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Recht und Sicherheit der Digitalisierung an der Technischen Universität München. Dort forscht er zu den rechtlichen Herausforderungen der digitalen Transformation, insbesondere zu Fragen der Plattformregulierung, KI-Regulierung, Wettbewerbs- und Datenschutzrecht. Zuvor war er mehrere Jahre als Rechtsanwalt in internationalen Wirtschaftskanzleien tätig.

Jakob Auer

Jakob Auer ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Recht und Sicherheit der Digitalisierung an der Technischen Universität München. Er forscht in einem weiten Feld an Themen aus dem Bereich der rechtlichen Gestaltung der Digitalisierung. Dieses reicht von Fragestellungen aus dem Bereich des E-Government über Plattformregulierung bis hin zu LegalTech. Der überwiegende Schwerpunkt seiner Forschungsarbeit liegt dabei im Datenschutzrecht, in dem er auch seine Dissertation verfasst.

Thimo Brand

Thimo Brand ist wissenschaftlicher Mitarbeiter am Lehrstuhl für Recht und Sicherheit der Digitalisierung von Prof. Dr. Dirk Heckmann. Er beschäftigt sich mit der Schnittstelle zwischen Rechtsfragen der Digitalisierung und dem Verfahrensrecht. Darüber hinaus verfügt Thimo Brand über vertiefte Kenntnisse im Immaterialgüterrecht und im internationalen Zivilprozessrecht.

Mitarbeit

Michael Bressler, Technische Universität München
Jonas Hacker, Technische Universität München
Valentin Vogel, Technische Universität München
Nadine Vogt, Noerr Partnerschaftsgesellschaft mbB

Herausgeber

Noerr Partnerschaftsgesellschaft mbB
Brienner Straße 28
80333 München
T +49 89 28628-0
www.noerr.com

Lehrstuhl für Recht und Sicherheit der Digitalisierung
Technische Universität München
Richard-Wagner-Straße 1
80333 München
T +49 89 907793-301
www.gov.tum.de/elaw
www.tum-cdps.de

Alicante
Berlin
Bratislava
Brüssel
Budapest
Bukarest
Dresden
Düsseldorf
Frankfurt/M.
Hamburg
London
Moskau
München
New York
Prag
Warschau

noerr.com