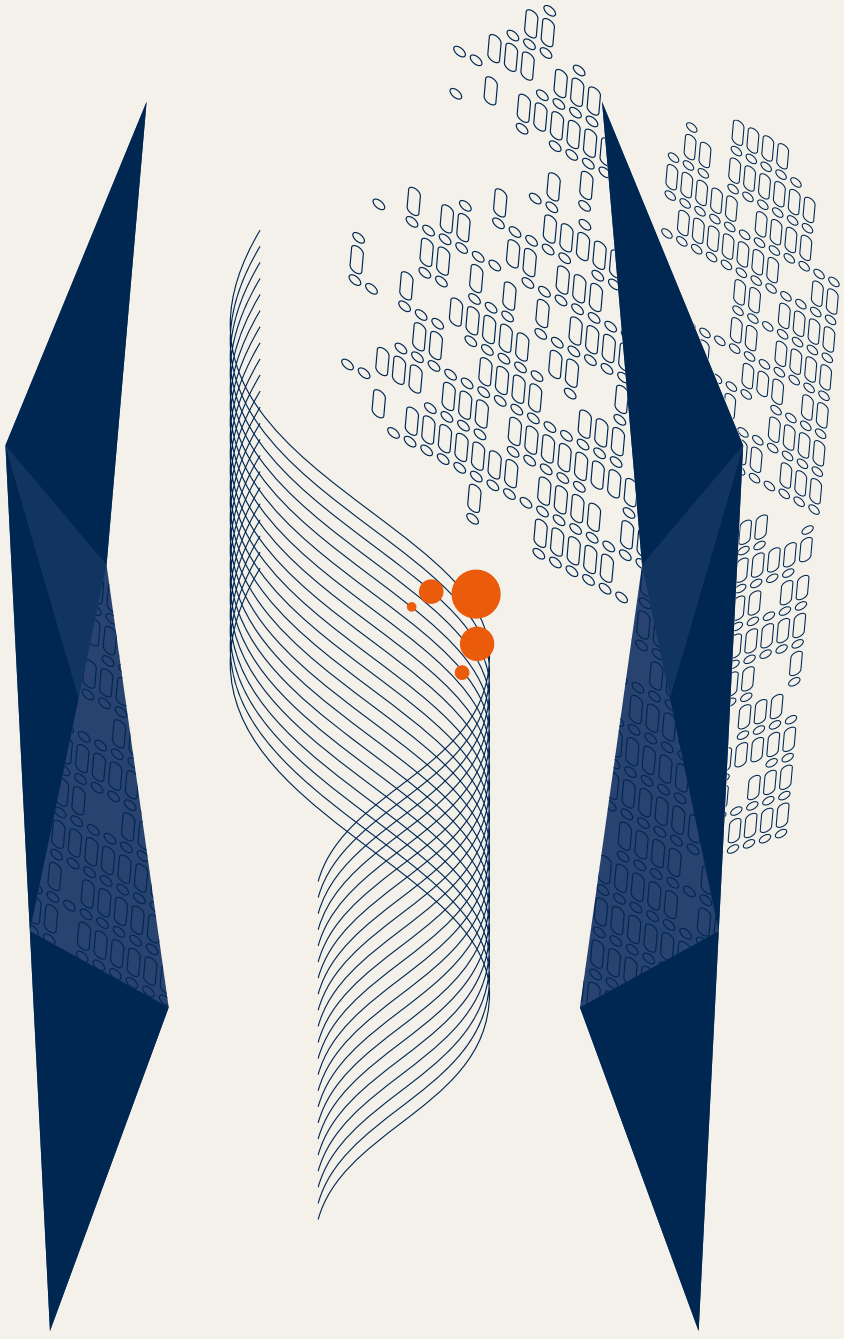
Digitalisierung & Compliance

Compliance-Studie 2022



In Kooperation mit:

Technische Universität München

Noerr

Vorwort

Die Digitalisierung der Wirtschaft nimmt gerade volle Fahrt auf. Für viele Unternehmen sind digitale Einsatzmittel, wie KI-gesteuerte Produktionsanlagen, konzernweite Personalplattformen oder sonstige Cloud-Lösungen, nicht mehr wegzudenken. Gleichzeitig steigt mit der Durchdringung neuer Technologien auch das Risiko von Rechtsverletzungen und Complianceverstößen. Daher ist die **Digital Compliance** heute wichtiger denn je.

Nach den Ergebnissen unserer ersten Digital-Compliance-Studie aus dem letzten Jahr scheinen die Unternehmen die rechtlichen Gefahren der Digitalisierung jedoch vielfach zu unterschätzen. In den Bereichen Cloud-Computing, künstliche Intelligenz und Big-Data-Analysen bewertete etwa die Hälfte der Befragten die rechtlichen Risiken als gering. Dieses Ergebnis steht in einem Spannungsfeld zu den stetig wachsenden regulatorischen Anforderungen, etwa beim Datenschutz oder der IT-Sicherheit.

Das Augenmerk unserer zweiten Digital-Compliance-Studie richtet sich diesmal auf den **Aufsichtsrat**, ein Organ, das sich – neben dem operativ tätigen Vorstand – im Rahmen seiner Kontrollfunktion den Digital-Compliance-Anforderungen stellen muss. In ca. 300 Interviews mit den Verantwortlichen privatwirtschaftlicher Unternehmen haben wir viel empirisches Material gewonnen und auch diesmal überrascht das Ergebnis nicht: Auch beim Thema Aufsichtsrat besteht noch **Handlungsbedarf**.

Prof. Dr. Peter Bräutigam

Dr. Julia Sophia Habbe

Prof. Dr. Dirk Heckmann

Inhalt

Executive Summary

Der digitale Sachverstand des Aufsichtsrats wird zunehmend wichtiger. Grund hierfür ist die fortschreitende Digitalisierung, die etablierte Geschäftsmodelle verändert und neue Unternehmensprozesse schafft, unter anderem in der Produktion, der Logistik und dem Vertrieb. Als zentrale Kontrollinstanz muss der Aufsichtsrat überwachen, ob die Geschäftsleitung die Risiken digitaler Technologien richtig ermittelt und innerhalb des Unternehmens zutreffend allokiert. Digital Compliance ist damit auch und gerade eine Aufgabe des Aufsichtsrats. Besondere Bedeutung für den Aufsichtsrat haben dabei die Themen IT-Sicherheit und Datenschutz. Der Aufsichtsrat muss über entsprechende Sachkenntnis verfügen, um seiner Kontrollfunktion bestmöglich gerecht zu werden. Es besteht Handlungsbedarf. In den meisten Fällen spielt die digitale Kompetenz für die Auswahl eines Aufsichtsratsmitglieds nur eine untergeordnete Rolle. Dies scheint selbst in Unternehmen der Fall zu sein, bei denen sich digitale Risiken bereits realisiert haben, etwa durch Datenschutzverstöße oder Ransomware-Angriffe. Zudem sollte der Aufsichtsrat auch sicherstellen, dass die Geschäftsleitung als Gremium über hinreichend digitalen Sachverstand verfügt, etwa in Form einer Due-Diligence bei der Neubesetzung einer Geschäftsleitungsstelle.

Inhaltlich befasst sich der Aufsichtsrat in rund der Hälfte der befragten Unternehmen regelmäßig mit digitalen Themen, weit überwiegend dann sogar quartalsweise. Begrüßenswert erscheint, dass die Digitalisierung von Geschäftsprozessen und IT-Sicherheitsthemen, wie zum Beispiel der Schutz der eigenen IT-Infrastruktur, als nahezu gleich relevant eingestuft werden.

Überwiegend behandelt der Aufsichtsrat digitale Themen im Gesamtgremium. Gerade wenn das Unternehmen einen hohen digitalen Reifegrad bzw. eine hohe Risikoexposition aufweist, erscheint indes eine spezialisierte Funktion innerhalb des Aufsichtsrats sinnvoll. Nur wenige der befragten Unternehmen verfügen im Aufsichtsrat über einen Digital Expert oder über einen Ausschuss für Digitalisierungsthemen. Sofern innerhalb des Aufsichtsrats ein Digital Expert vertreten ist, besitzt dieser außerdem meistens einen betriebswirtschaftlichen und keinen technischen Hintergrund.

In Unternehmen geht die digitale Transformation mit einer steigenden Automatisierung und Vernetzung von Systemen und Prozessen sowie der Verarbeitung enormer und vielfältiger Datenmengen einher. Der Stellenwert der IT-Sicherheit steigt in diesem Kontext rasant an. Dies liegt auch an der zunehmenden Bedrohungslage für die Vertraulichkeit, Integrität und Verfügbarkeit von Systemen durch Cyberattacken und exponentiell zunehmende Phänomene wie Ransomware. Die Unternehmen zeigen sich von dieser Bedrohungslage zusehends betroffen, was sich in ihrer Risikowahrnehmung und Sensibilisierung hierfür spiegelt. Trotz der teils stark differenzierten Anforderungen an die Unternehmen gab ein Großteil der Befragten an, wesentliche Maßnahmen zur Herstellung von IT-Sicherheit umzusetzen. Dabei konnten als Basisschutz qualifizierende Maßnahmen breitflächig festgestellt werden, während spezifischere Maßnahmen zum Stand der Technik noch weniger verbreitet sind. Auch bei der Organisation von IT-Sicherheitsmaßnahmen zeigt sich, dass viele Unternehmen bereits spezifische Stellen für die IT-Sicherheit oder einen IT-Sicherheitsbeauftragten haben. Dabei ist zu beobachten, dass diese zu großen Teilen in der IT-Abteilung angesiedelt sind, wobei auf Rollenkonflikte zwischen der operativen IT-Abteilung und den spezifisch für die IT-Sicherheit zuständigen Stellen zu achten ist. Eine Möglichkeit zur Steigerung der IT-Sicherheit für Unternehmen ohne entsprechende Kapazitäten ist der Einsatz von Cloud-Lösungen, die zu einer Erhöhung der IT-Sicherheit beitragen können. Dabei ist angesichts der Rechtsprechung des EuGH aber vermehrt auf die Frage des Serverstandorts und den Sitz des Unternehmens zu achten, um einen rechtssicheren Datentransfer zu gewährleisten und die dabei konfligierenden Ziele des Datenschutzes mit denen der IT-Sicherheit aufzulösen.

1. Der Aufsichtsrat im Kontext der digitalen Compliance

Mit der diesjährigen Compliance-Studie möchten wir unter anderem die Rolle des Aufsichtsrats[1] im Kontext der digitalen Compliance betrachten. Digitale Compliance ist auch und gerade eine Aufgabe des Aufsichtsrats.

Durch die fortschreitende Digitalisierung muss sich der Aufsichtsrat immer häufiger mit digitalen Themen befassen, etwa Fragen zur IT-Sicherheit, zu digitalen Geschäftsprozessen oder zum Einsatz neuer Technologien. Um seiner Organisations- und Kontrollfunktion gerecht zu werden, ist es entscheidend, dass der Aufsichtsrat über adäquate Sachkenntnisse und ein rechtliches Grundverständnis von digitaler Compliance verfügt.

Die Angaben der befragten Unternehmen zeigen, dass insbesondere bei der Auswahl von Aufsichtsratsmitgliedern insoweit Handlungsbedarf besteht. Für viele Unternehmen spielt der digitale Sachverstand eines Aufsichtsratsmitglieds für dessen Bestellung nur eine untergeordnete Rolle. Nur wenige Unternehmen verfügen zudem über einen Ausschuss für Digitalisierungsthemen. Sofern im Aufsichtsrat ein Digital Expert[2] vertreten ist, hat dieser überwiegend einen betriebswirtschaftlichen und keinen technischen Hintergrund. Insofern erscheint es wünschenswert, dass Unternehmen zukünftig noch mehr darauf achten, dass digitales bzw. technisches Fachwissen im Aufsichtsrat vertreten ist.

1.1 Digitale Compliance als Aufgabe des Aufsichtsrats

Der Aufsichtsrat spielt für die digitale Compliance des Unternehmens eine entscheidende Rolle.

Digitale Compliance ist auch Aufgabe des Aufsichtsrats. Als **Kontrollorgan** innerhalb der Unternehmensorganisation spielt der Aufsichtsrat eine wichtige Rolle (§ 111 Abs. 1 AktG).

Das Gremium ist unter anderem für die **Einsetzung und das Monitoring** der Mitglieder der Geschäftsleitung zuständig. Dabei sollte der Aufsichtsrat auch den digitalen Sachverstand der Geschäftsleitung sicherstellen, damit diese ihre Organisationspflichten im Kontext der Digitalisierung erfüllen kann. Hier kann es sinnvoll sein, die Position eines **Chief Digital Officer** zu erwägen.

Zudem hat er die Geschäftsleitung daraufhin zu überwachen, ob sie alles Notwendige unternimmt, um das Vermögen der Gesellschaft zu mehren und Schaden von ihr abzuwenden. Dabei muss er insbesondere überwachen, ob die Geschäftsleitung die mit der Digitalisierung verbundenen Risiken richtig ermittelt und innerhalb des Unternehmens zutreffend allokiert.

Der Aufsichtsrat muss sich in diesem Zusammenhang überzeugen, dass geeignete und angemessene **Compliance-Strukturen im Unternehmen existieren**, und deren Funktionsfähigkeit und Effizienz prüfen. Darüber hinaus hat er die effektive Durchsetzung der Compliance innerhalb des Unternehmens zu überwachen. Sollte der Aufsichtsrat von Umständen erfahren, die auf gravierende Mängel des Compliance-Systems oder schwerwiegende Compliance-Verstöße durch die Geschäftsleitung hindeuten, muss er ebenfalls tätig werden und im Zweifel selbst diese Vorfälle aufklären.

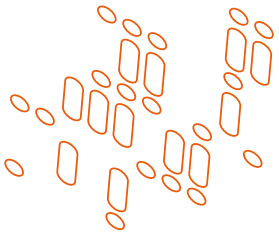
---

[1] Unter dem Begriff „Aufsichtsrat" werden im Folgenden auch weitere Aufsichtsorgane, wie etwa der Beirat zusammengefasst.

[2] 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.

Für die digitale Compliance als Querschnittsmaterie sind daneben auch digitale und technische Aspekte relevant. **Digitale Geschäftsmodelle, sich ändernde Unternehmensprozesse und neue Technologien** stehen immer öfter auf der Tagesordnung von Aufsichtsratssitzungen. Das Gremium muss daher in der Lage sein, die damit verbundenen Chancen und Risiken bewerten zu können. Dabei muss der Aufsichtsrat nicht zum IT-Spezialisten werden. Er sollte aber die für das Unternehmen relevanten digitalen Themen sowie deren technische und regulatorische Anforderungen verstehen, um seiner Überwachungs- und Kontrollfunktion gerecht zu werden.

Außerdem sollte sich der Aufsichtsrat bewusst sein, dass die fortschreitende Digitalisierung selbst mit Compliance-Risiken einhergeht. Insbesondere bestehen wegen der zunehmenden Regulierung im digitalen Bereich erhebliche rechtliche Risiken. In diesem Zusammenhang zeigte unsere **Compliance-Studie 2021 zum Thema Digitalisierung & Compliance**[3], dass den Entscheidungsträgern der befragten Unternehmen oftmals nicht umfassend bewusst war, dass neue Technologien ihrerseits neue Compliance-Risiken schaffen. Der Aufsichtsrat als Kontroll- und Überwachungsinstanz der Geschäftsleitung ist bei digitaler Compliance besonders gefragt.



[3] Digitalisierung & Compliance, Compliance-Studie 2021, abrufbar unter https://www.noerr.com/de/newsroom/news/gemeinsame-studie-von-noerr-und-technischer-universitat-munchen.

1.2 Digitale Kompetenz des Aufsichtsrats

In den meisten Fällen spielt die digitale Kompetenz eines Aufsichtsratsmitglieds für dessen Bestellung nur eine untergeordnete Rolle.

Um seiner Kontroll- und Überwachungsfunktion in einem zunehmend digitalen Umfeld bestmöglich gerecht zu werden, ist es erforderlich, dass der Aufsichtsrat über entsprechenden Sachverstand verfügt. In den meisten Fällen spielt dies in der Praxis für die Auswahl eines Aufsichtsratsmitglieds aber nur eine untergeordnete Rolle. Es erscheint zukünftig wünschenswert, dass Unternehmen verstärkt auf den digitalen Sachverstand innerhalb des Aufsichtsrats achten.

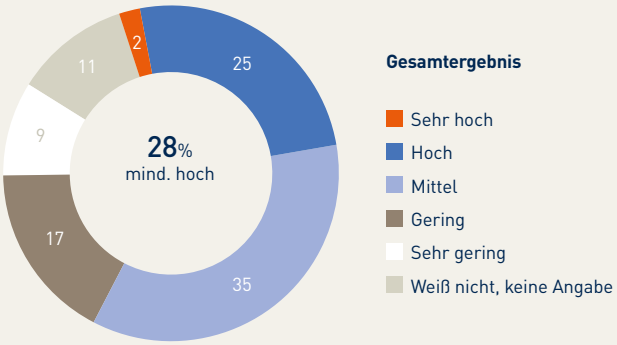
Digitale Kompetenz als Auswahlkriterium für ein Aufsichtsratsmitglied

Ein Großteil der befragten Unternehmen, die über einen Aufsichtsrat verfügen, schreibt der digitalen Kompetenz bei der Auswahl und Bestellung von Aufsichtsratsmitgliedern keine wesentliche Bedeutung zu.

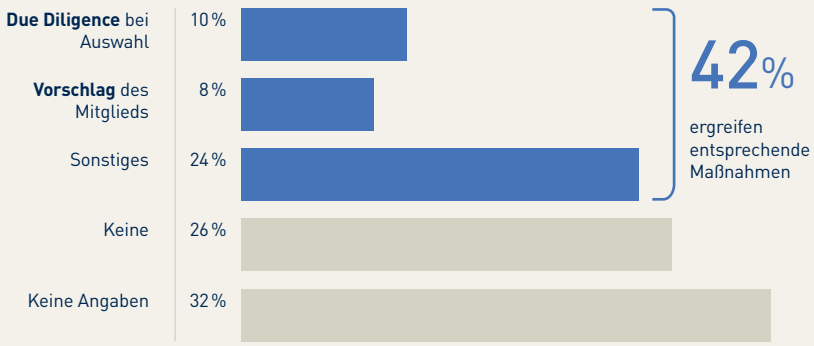
Nur 28 % der Unternehmen schätzen digitale Kompetenzen und Fähigkeiten bei der Besetzung von Aufsichtsratsposten **als wichtiges Kriterium** ein („(sehr) hohe Wichtigkeit"). In größeren Unternehmen ab 1.000 Beschäftigten ist der Anteil mit **31 %** zwar etwas höher, bewegt sich aber trotzdem auf niedrigem Niveau.

Digitale Kompetenz des Aufsichtsrats und der Geschäftsleitung

Relevanz der digitalen Kompetenz wird oftmals verkannt.



Ergriffene Maßnahmen für digitale Kompetenz der Geschäftsleitung



Fragen: Wie schätzen Sie die Wichtigkeit der digitalen Kompetenz bei der Auswahl und Bestellung von Aufsichtsratsmitgliedern ein? Welche Maßnahmen hat der Aufsichtsrat ergriffen, um den digitalen Sachverstand der Geschäftsleitung sicherzustellen?

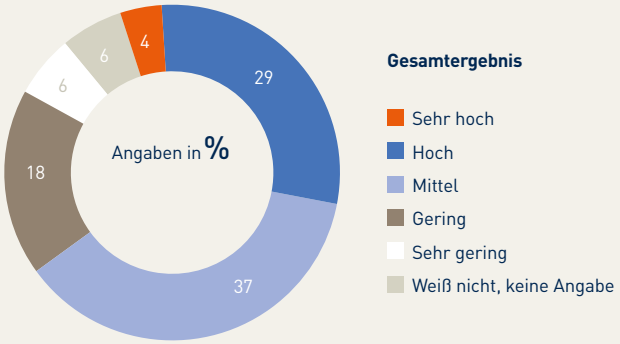
Basis: Aufsichtsrat vorhanden; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Bemerkenswert ist, dass sich dieser Befund bei Unternehmen fortsetzt, welche die digitalisierungsbedingten Risiken für die IT-Sicherheit oder den Datenschutz als besonders hoch einschätzen (siehe Abschnitt 2.1). Nur etwas mehr als ein Drittel dieser Unternehmen berücksichtigen überhaupt die digitale Kompetenz bei der Auswahl ihrer Aufsichtsratsmitglieder (37 % bzw. 39 % „(sehr) hohe Wichtigkeit").

Auch nach einem Compliance-Vorfall erachtet nur jedes dritte Unternehmen die digitale Kompetenz von Aufsichtsratsmitgliedern als wichtig.

Einschätzung der Relevanz der digitalen Kompetenz des Aufsichtsrats nach Compliance-Vorfällen



Frage: Wie schätzen Sie die Wichtigkeit der digitalen Kompetenz bei der Auswahl und Bestellung von Aufsichtsratsmitgliedern ein?

Basis: Aufsichtsrat vorhanden; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Selbst Unternehmen, die in den vergangenen Jahren bereits von **Compliance-Vorfällen** wie etwa Datenschutzverstößen, Ransomware-Angriffen oder Urheberrechtsverletzungen betroffen waren, berücksichtigen die Sachkenntnis von Aufsichtsratskandidaten bei digitalen Themen nicht immer. So erachtet nur jedes dritte betroffene Unternehmen digitale Kompetenz als wichtige Voraussetzung für die Bestellung von Aufsichtsratsmitgliedern (33 %). Der Unterschied zu den Unternehmen, in denen es in den letzten drei Jahren nicht zu einem solchen Vorfall kam, ist mithin marginal. Dies verwundert, weil sich digitale Rechtsrisiken für Unternehmen immer häufiger realisieren. Unsere **Compliance-Studie 2021 zum Thema Digitalisierung & Compliance** zeigte, dass dies bereits bei der Hälfte der damals befragten Unternehmen der Fall war.

Dennoch erachten die meisten Unternehmen digitale Kompetenz von Aufsichtsratsmitgliedern als weniger wichtig (37 % „mittlere Wichtigkeit"). Für knapp **ein Viertel** der Unternehmen mit einem Aufsichtsrat spielt dieses Kriterium **nur eine untergeordnete Rolle** (24 % „(sehr) geringe Wichtigkeit"). Unternehmen sollten daher erwägen, den Auswahlprozess und das Anforderungsprofil für neue Mitglieder im Aufsichtsrat zu prüfen und gegebenenfalls anzupassen.

Sicherstellung des digitalen Kompetenz der Geschäftsleitung

Viele der befragten Unternehmen stellen nach eigenen Angaben über ihren Aufsichtsrat sicher, dass die Geschäftsleitung hinreichend digitalen Sachverstand mitbringt.

So geben insgesamt **42 %** an, dass der Aufsichtsrat konkrete Maßnahmen ergreift, um den digitalen Sachverstand der Geschäftsleitung sicherzustellen. Einen nur geringen Anteil bildet dabei die Prüfung digitaler Kompetenzen von Neubesetzungen im Rahmen der Due Diligence. Nur jedes zehnte der befragten Unternehmen überprüft den jeweiligen Kandidaten bei der Neubesetzung von Funktionen in der Geschäftsleitung auf seine digitalen Fachkenntnisse. Daneben geben **24 %** an, dass sie sonstige Maßnahmen ergreifen, spezifizieren diese aber nicht weiter. Lediglich **8 %** der befragten Unternehmen berichten, dass der Aufsichtsrat bei der Auswahl geeignete Mitglieder vorschlägt, um den digitalen Sachverstand zu gewährleisten.

Die Mehrheit kann keine konkreten Maßnahmen des Aufsichtsrates zur Sicherstellung des digitalen Sachverstands der Geschäftsleitung benennen oder zieht es vor, hierzu keine Angaben zu machen. Lediglich Unternehmen, deren Aufsichtsräte das Thema Digitalisierung bereits entweder funktional besetzt haben oder sich regelmäßig damit befassen (siehe Abschnitt 1.3), ergreifen mehrheitlich entsprechende Maßnahmen (60 %). Allerdings verzichten selbst in dieser affinen Gruppe zwei von fünf Aufsichtsräten auf einen eigenen Beitrag zur Förderung digitaler Kompetenz der Geschäftsführung.

1.3 Befassung des Aufsichtsrats mit digitalen Themen

Nur ein Viertel der Aufsichtsräte in den befragten Unternehmen verfügt über einen Digital Expert.

In einem Großteil der befragten Unternehmen adressiert der Aufsichtsrat das Thema Digitalisierung. Oftmals befasst er sich regelmäßig mit digitalen Themen oder es existiert ein Digital Expert bzw. ein spezieller Ausschuss für Digitalisierungsthemen. Weit überwiegend widmet sich der Aufsichtsrat diesen Themen aber im Gesamtgremium. Sofern ein Digital-Expert vorhanden ist, verfügt dieser oftmals über einen betriebswirtschaftlichen Hintergrund.

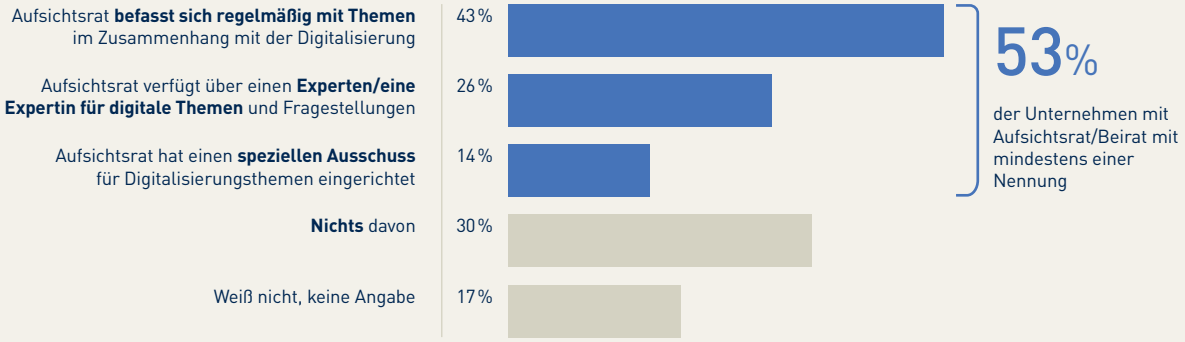
Auseinandersetzung

Zu begrüßen ist, dass der Aufsichtsrat in einem Großteil der befragten Unternehmen Themen rund um die Digitalisierung adressiert (53 %), sei es durch regelmäßige Befassung oder organisatorische Maßnahmen, wie etwa einen Ausschuss für Digitalisierungsthemen.

43 % der Aufsichtsräte setzen sich regelmäßig mit dem Thema Digitalisierung auseinander. Die Rückmeldungen legen nahe, dass hierbei auch die Größe des Unternehmens eine Rolle spielt. So befasst sich der Aufsichtsrat in Unternehmen mit mehr als 1.000 Beschäftigten in **45 %** der befragten Unternehmen mit der Digitalisierung und ihren Auswirkungen, während dies in Unternehmen mit weniger als 1.000 Mitarbeitern in **41 %** der Fall ist. Zudem haben einige Aufsichtsräte organisatorische Maßnahmen ergriffen und etwa einen speziellen Ausschuss gebildet (14 %, siehe „Turnus" in diesem Abschnitt) oder einen Digital Expert eingesetzt (26 %, siehe Digital Expert und beruflicher Hintergrund in diesem Abschnitt).

Rolle des Aufsichtsrats im Kontext der Digitalisierung

In der Hälfte der Unternehmen befasst sich der Aufsichtsrat mit digitalen Themen.



Frage: Was von dem Folgenden trifft auf den Aufsichtsrat bzw. Beirat Ihres Unternehmens zu?

Basis: Aufsichtsrat vorhanden; Mehrfachnennungen möglich; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Im Umkehrschluss setzt aber ein beachtlicher Teil der Aufsichtsräte in den befragten Unternehmen das Thema Digitalisierung noch nicht regelmäßig auf die Tagesordnung oder hat noch nicht einen Digital Expert benannt bzw. einen speziellen Ausschuss eingerichtet. In kleineren Unternehmen mit weniger als 1.000 Beschäftigten sind sogar **51 %** der Aufsichtsräte nicht aktiv involviert, wenn es um digitale Themen und Fragestellungen geht („weiß nicht, keine Angabe" werden hierbei mitgerechnet). Betrachtet man das Ausmaß und die potenziellen Risiken von Compliance-Vorfällen in diesem Bereich, sollte der Aufsichtsrat insofern stärker eingebunden werden.

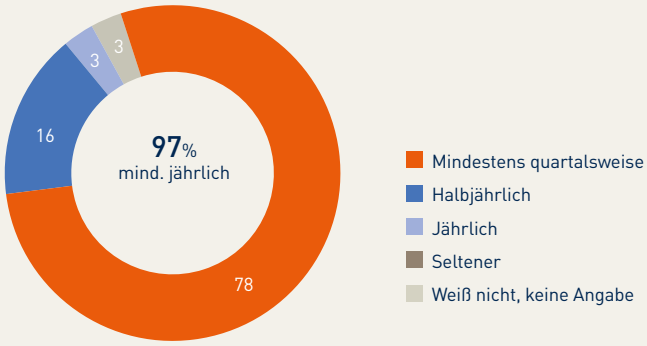
Turnus

Sofern sich der Aufsichtsrat mit digitalen Themen befasst, dann **weit überwiegend mindestens quartalweise**. Dies ist zu begrüßen, weil digitale Compliance kein statischer Prozess ist. So können bestehende Prozesse und Organisationsstrukturen kontinuierlich überprüft und neue Entwicklungen zeitnah aufgegriffen werden. In vier von fünf der zuständigen Kontrollgremien erfolgt dies mindestens quartalsweise. In nur knapp **20 %** der betreffenden Unternehmen geschieht dies seltener, dann in der Regel halbjährlich.

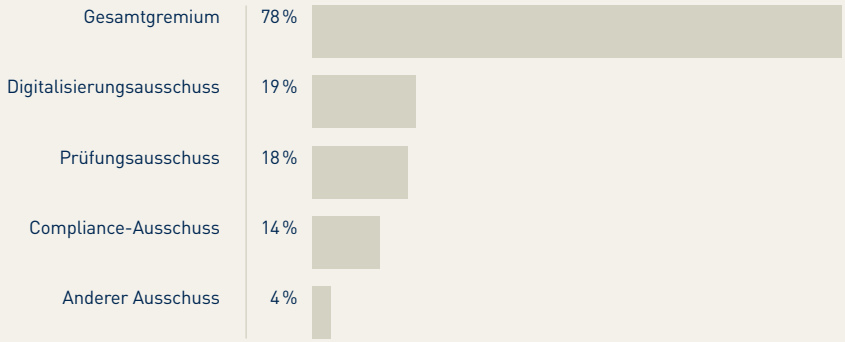
Rolle des Aufsichtsrats im Kontext der Digitalisierung

Befasst sich der Aufsichtsrat mit Digitalisierungsthemen, dann in acht von zehn Fällen mindestens einmal im Quartal.

Behandlungsturnus Digitalisierungsthemen



Aufsichtsrat-Gremium für Digitalisierungsthemen



Frage: In welchem Gremium des Autsichtsrats werden Digitalisierungsthemen behandelt? Und wie oft?

Basis: Aufsichtsrat befasst sich regelmäßig mit Digitalisierungsthemen; Mehrfachnennungen moglich; Angaben in Prozent

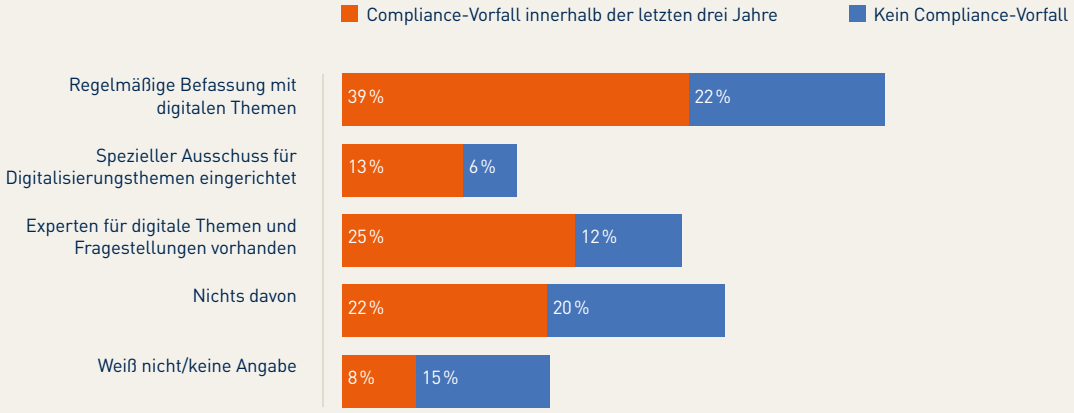
Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Musste ein Unternehmen in den letzten drei Jahren einen Compliance-Vorfall in den Bereichen Datenschutz oder IT-Sicherheit erleiden, unterscheidet sich die Rolle des Aufsichtsrats durchaus. In **61 %** der Fälle ist der Aufsichtsrat dann direkt in das Thema Digitalisierung involviert. Darunter befassen sich **39 %** der Aufsichtsräte selbst regelmäßig mit dem Thema, ein Viertel greift auf Experten zurück und **13 %** haben einen dedizierten Ausschuss eingerichtet.

Kam es in den letzten drei Jahren hingegen nicht zu Compliance-Vorfällen, sind lediglich **22 %** der Aufsichtsräte regelmäßig involviert. Der Aufsichtsrat scheint sich oftmals erst mit digitalen Themen auseinanderzusetzen, wenn das Unternehmen direkt von digitalen Compliance-Vorfällen betroffen war. Dies zeigt, dass Unternehmen auf Vorfälle reagieren und ihre Strukturen und Prozesse stärken. Allerdings könnten sie den Fokus stärker auch auf die präventive Compliance legen, zu der sie ebenfalls verpflichtet sind.

Befassung des Aufsichtsrats mit digitalen Themen

Aufsichtsräte befassen sich eher mit digitalen Themen, wenn es innerhalb der letzten drei Jahre bereits zu Compliance-Vorfällen gekommen ist.



Frage: Was von dem Folgenden trifft auf den Aufsichtsrat bzw. Beirat Ihres Unternehmens zu?

Basis: alle Unternehmen, Darstellungen zu Unternehmen ohne Aufsichtsrat ausgenommen; Mehrfachnennungen möglich; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Gesamtgremium oder Ausschuss?

Die Art und Weise, wie sich der Aufsichtsrat mit digitalen Themen auseinandersetzt, variiert zwischen den befragten Unternehmen.

Während der **weit überwiegende Teil** derer, in denen sich der Aufsichtsrat regelmäßig mit digitalen Themen befasst, angibt, dass diese im **Gesamtgremium** des Aufsichtsrats diskutiert werden (78 %), gibt es auch solche, die diese Thematik in Ausschüssen behandeln. Teilweise beschäftigt sich etwa der Compliance-Ausschuss des Aufsichtsrats mit der Digitalisierung und ihren Folgen (14 %).

Vor allem Unternehmen mit einem hohen Digitalisierungsgrad bzw. einem hohen digitalen Risiko-Exposure können erwägen, im Aufsichtsrat einen **speziellen Ausschuss für Compliance- und Digitalisierungsthemen** einzurichten. Im Zuge einer professionalisierten Arbeitsteilung können so einzelne Mitglieder des Aufsichtsrats Themen rund um die Digitalisierung vertieft bearbeiten. Alternativ besteht die Möglichkeit, dass der Aufsichtsrat ein **fachkundiges Mitglied** in seinen Reihen aufnimmt, das sich regelmäßig mit den digitalen Themen des Unternehmens befasst.

Diese Form der Aufsichtsratsarbeit scheint hinsichtlich digitaler Themen noch nicht weit verbreitet zu sein. Nur **14 %** der befragten Unternehmen verfügen über einen **speziellen Ausschuss im Aufsichtsrat**. Anders sieht es in Aufsichtsräten aus, die sich regelmäßig mit digitalen Fragestellungen befassen. Bei diesen gibt es in **26 % der befragten Unternehmen einen eigenen Ausschuss zum Thema Digitalisierung**.

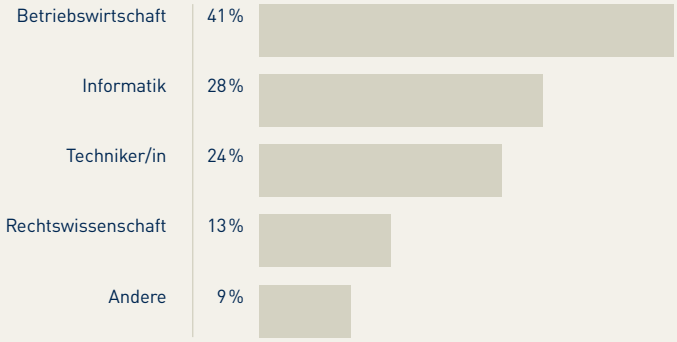
Digital Expert und beruflicher Hintergrund

Da Aufgaben innerhalb des Aufsichtsrats delegiert werden können, können besonders kundige Aufsichtsratsmitglieder etwa als Digital Expert eingesetzt werden. Vor allem in Unternehmen mit hohem Digitalisierungsgrad oder hohem digitalen Risiko-Exposure kann es sogar notwendig sein, eine solche Rolle im Aufsichtsrat zu besetzen.

Von dieser Möglichkeit machen bislang nur wenige Gebrauch. In nur **26 % der befragten Unternehmen gibt es einen oder mehrere solcher Digital Experts** im Aufsichtsrat.

Digitalisierungs-Experten im Aufsichtsrat: beruflicher Hintergrund

Zumeist betriebswissenschaftlicher Einschlag.



Frage: Welchen beruflichen Hintergrund hat der Experte/die Expertin für digitale Themen und Fragestellungen in Ihrem Aufsichtsrat bzw. Beirat?

Basis: Aufsichtsrat verfügt über Digitalisierungs-Expert*in; Mehrfachnennungen möglich; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Die meisten der Digital Experts besitzen einen betriebswirtschaftlichen Hintergrund (41 %). Techniker und Informatiker sind jeweils nur zu einem Viertel als Digitalisierungsexperten in Aufsichtsräten eingesetzt (28 % bzw. 24 %).

1.4 Relevanz von digitalen Themen im Aufsichtsrat

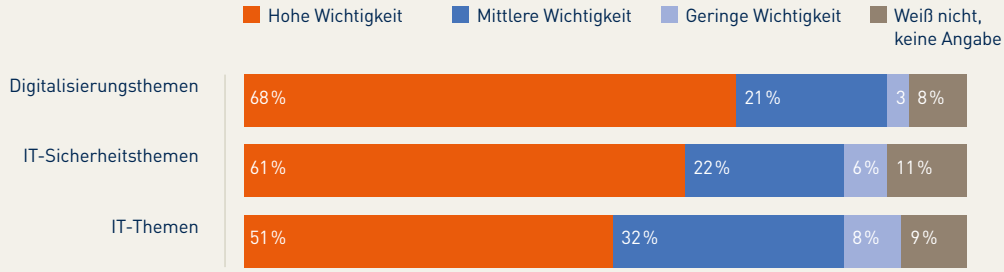
Digitalisierung der Geschäftsprozesse und IT-Sicherheitsthemen spielen für den Aufsichtsrat eine große Rolle.

Die befragten Unternehmen stufen die Digitalisierung von Geschäftsprozessen, die IT-Sicherheit und den Einsatz von Software im Unternehmen als unterschiedlich relevant für den Aufsichtsrat ein.

Stehen Fragen der Digitalisierung regelmäßig auf der Agenda des Aufsichtsrates, betreffen diese am häufigsten den Umfang oder die Umsetzung der Digitalisierung selbst. Dies gilt insbesondere für Fragen, inwieweit die **Geschäftsprozesse** in Produktion und Logistik bis hin zum Vertrieb bereits digitalisiert sind bzw. werden können (**Digitalisierungsthemen**). Für mehr als zwei Drittel der betreffenden Aufsichtsräte ist dies eine der wichtigsten Fragen im Kontext der Digitalisierung (68 % „hohe Wichtigkeit"). Dies gilt vor allem für größere Unternehmen mit mehr als 1.000 Beschäftigten (76 % „hohe Wichtigkeit").

Relevanz von Digitalisierungsthemen im Aufsichtsrat

Steht Digitalisierung regelmäßig auf der Agenda, genießen insbesondere Digitalisierungs- und IT-Sicherheitsthemen hohe Wichtigkeit im Aufsichtsrat.



Frage: Was von dem Folgenden trifft auf den Aufsichtsrat bzw. Beirat Ihres Unternehmens zu?

Basis: Aufsichtsrat befasst sich regelmäßig mit Digitalisierungsthemen; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Daneben spielen in den Aufsichtsräten Themen der IT-Sicherheit und entsprechender Maßnahmen zum **Schutz von Rechenzentren, Cloud-Anwendungen und der unternehmenseigenen IT-Infrastruktur (IT-Sicherheitsthemen)** eine fast ebenso wichtige Rolle (61 % „hohe Wichtigkeit"). Allein **30 %** der Unternehmen, in denen sich der Aufsichtsrat regelmäßig mit Digitalisierungsthemen auseinandersetzt, schreiben der IT-Sicherheit eine „überaus wichtige" Bedeutung zu. Hier sollte jedoch ein ausreichendes Bewusstsein hinsichtlich potenzieller Sicherheitsrisiken vorhanden sein. Nicht nur Datenschutzrechtsverstöße sind von Bedeutung. Vielmehr können Unternehmen jederzeit Hacking- oder Ransomware-Attacken zum Opfer fallen. Mithin muss deutlich werden, welche Risiken etwa durch die Nutzung von Cloud-Anbietern oder externen Rechenzentren entstehen können und wie man diese minimieren kann.

Weiteren IT-Themen, wie etwa Outsourcing von IT-Leistungen oder Auswahlentscheidungen zum Einsatz von Software (**IT-Themen**), wird von einer knappen Mehrheit der befragten Unternehmen eine hohe Wichtigkeit für den Aufsichtsrat attestiert (51 %). Im direkten Vergleich wird Digitalisierungs- und IT-Sicherheitsthemen jedoch größere Bedeutung beigemessen.

2. Compliance-Risiken und Maßnahmen

2.1 Risiken durch Digitalisierung

Der Aufsichtsrat spielt für die digitale Compliance des Unternehmens eine entscheidende Rolle.

Mit der sich durch die zunehmende Automatisierung und Vernetzung von Systemen und Prozessen sowie der Verarbeitung riesiger Datenmengen charakterisierenden **digitalen Transformation** ist auch der Stellenwert der **IT-Sicherheit** in den vergangenen Jahren um ein Vielfaches gestiegen. Insbesondere für Unternehmen ist es essenziell, die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Systeme sicherzustellen. Die Anforderungen an die IT-Sicherheit und Compliance-Pflichten divergieren je nach Größe und Tätigkeitsbranche des Unternehmens und sind ebenso abhängig von den individuell eingesetzten Systemen und Prozessen. Ihre Nichteinhaltung ist mit erheblichen **finanziellen Risiken** verbunden, zudem geht der Eintritt digitaler Restrisiken neben finanziellen Verlusten oftmals mit **Imageschäden** einher. IT-Sicherheit ist ein wichtiger **Wettbewerbsfaktor** und die Risiken sind aktueller denn je. Allein im vergangenen Jahr gab es viele Cyberangriffe auf bekannte Unternehmen, bei denen teilweise die komplette Produktion vorübergehend lahmgelegt wurde. Nach einem **Ransomwareangriff** auf eine Landkreisverwaltung musste der betroffene Landkreis im letzten Jahr sogar den Katastrophenfall ausrufen; der Regelbetrieb ist Monate später immer noch nicht gewährleistet.

Bereits in der **Compliance-Studie 2021** wurden die Unternehmen nach den zunehmenden und immer komplexer werdenden digitalen Restrisiken befragt. Dabei ergab die Studie, dass ca. die Hälfte der Unternehmen (47 %) bereits von Risikoszenarien wie Hacking, Datenschutzrechtverstößen, Ransomware, IT-Sicherheitsdefiziten, Urheberrechtsverletzungen oder weiteren Risiken betroffen war.[4] **22 %** der befragten Unternehmen gaben in dieser Studie an, bereits Opfer eines **Hacking-Angriffs** gewesen zu sein. Dieses Ergebnis deckte sich auch mit den Angaben aus dem Lagebericht 2020 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur IT-Sicherheit in Deutschland. Die Bedrohungslage durch Cyberattacken und die damit einhergehenden wachsenden rechtlichen Anforderungen wachsen demnach stetig an. Allein für das Jahr 2020 registrierte das BSI die Verbreitung ca. 117 Mio. neuer Schadprogramm-Varianten. Neben Hacking-Angriffen legte die Studie auch die besonderen Herausforderungen durch den Einsatz von **Ransomware** offen. **16 %** der befragten Unternehmen waren hiervon betroffen, bei börsennotierten Unternehmen sogar **37 %**. Bei nicht von Ransomware-Angriffen betroffenen Unternehmen legte die Studie einen erheblichen Nachholbedarf bezogen auf Maßnahmen der IT-Sicherheit offen. Lediglich **57 %** dieser Unternehmen hatten sich inhaltlich mit diesem Thema auseinandergesetzt.

In der **Compliance-Befragung 2022** geben **47 %** der Großunternehmen an, in den letzten drei Jahren von Compliance-Vorfällen betroffen gewesen zu sein. Neben allgemeinen Datenschutzverstößen (29 %) beziehen sich diese Angaben vor allem auf **Compliance-Verstöße im Zusammenhang mit IT-Sicherheit (27 %)**.

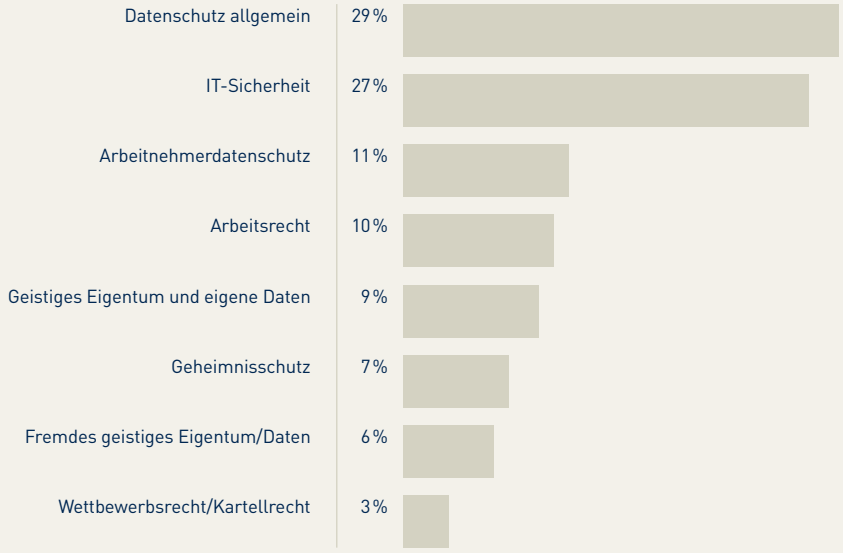
[4] Digitalisierung & Compliance, Compliance-Studie 2021, S. 14f., abrufbar unter https://www.noerr.com/de/newsroom/news/gemeinsame-studie-von-noerr-und-technischer-universitat-munchen.

Risiken durch Digitalisierung

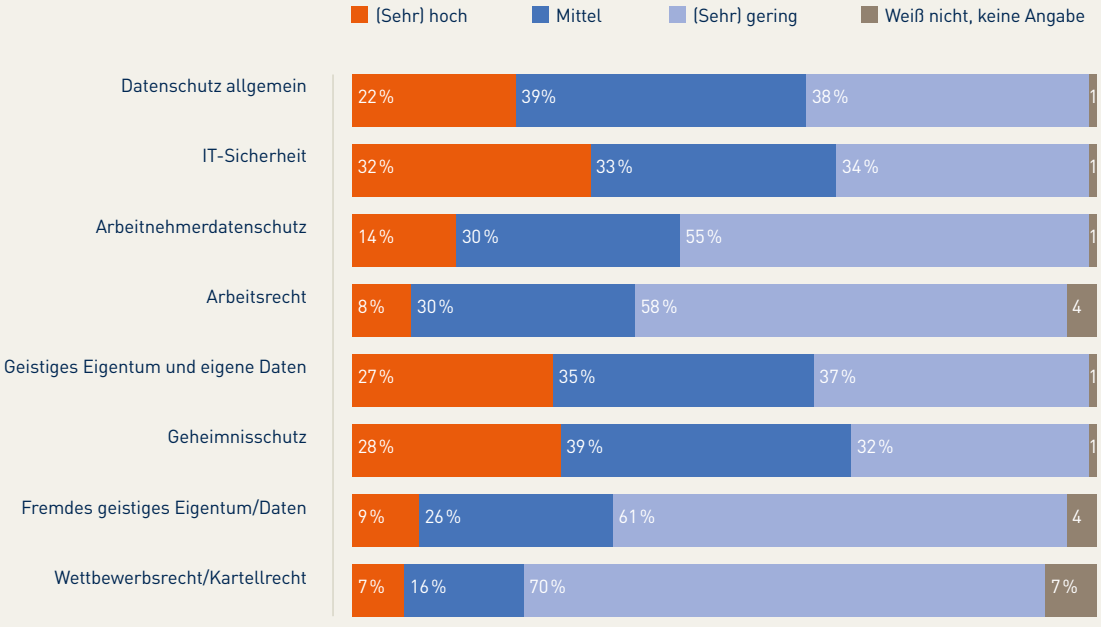
47 % der Unternehmen waren in den letzten drei Jahren von Compliance-Vorfällen betroffen.

Bedrohungslage

Berichtete Compliance-Vorfälle in den letzten drei Jahren



Risikowahrnehmung



Fragen: In welchen dieser Bereiche gab es in den letzten drei Jahren Compliance-Vorfälle in Ihrem Unternehmen? Wie schätzen Sie in den folgenden Bereichen das Risiko für Ihr Unternehmen durch die Digitalisierung ein? Bitte verwenden Sie für Ihre Bewertung eine Skala von 1 „sehr gering" bis 5 „sehr hoch".

Basis: alle Unternehmen; Bedrohungslage: Mehrfachnennungen möglich; Angaben in Prozent, Zahlen gerundet.

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Im Bereich IT-Sicherheit decken sich Betroffenheit und Bedrohungslage mit den Studienerkenntnissen zur jeweiligen Risikowahrnehmung. **32 %** der Befragten schätzen das Risiko für Compliance-Verstöße für ihr Unternehmen im Bereich IT-Sicherheit als hoch oder sehr hoch ein, weitere **33 %** der befragten Führungskräfte identifizieren IT-Sicherheitsrisiken als mittleres Risiko. Bei kleineren Unternehmen ist die Risikowahrnehmung etwas geringer, allerdings waren größere Unternehmen (mindestens 1.000 Mitarbeitende) im Bereich IT-Sicherheit auch häufiger betroffen (+9 Prozentpunkte). Ein positiver Einfluss auf die Risikowahrnehmung bei größeren Unternehmen mit Aufsichtsrat kann sich daraus ergeben, dass der IT-Sicherheit als Thema im Aufsichtsrat eine große Relevanz beigemessen wird (siehe Abschnitt 1.4).

In den Aufsichtsräten werden Themen der IT-Sicherheit und entsprechende Schutzmaßnahmen als sehr wichtig erachtet (61 % „hohe Wichtigkeit", siehe Abschnitt 1.4). **30 %** der Unternehmen, in denen sich der Aufsichtsrat regelmäßig mit Digitalisierungsthemen befasst, sehen eine „überaus wichtige" Bedeutung der IT-Sicherheit. War ein Unternehmen in den vergangenen drei Jahren von Compliance-Vorfällen im Bereich IT-Sicherheit betroffen, unterscheidet sich die Rolle des Aufsichtsrats, bei **61 %** der betroffenen Unternehmen ist er direkt in das Thema Digitalisierung involviert (siehe „Turnus" unter Abschnitt 1.3). Allerdings berücksichtigen betroffene Unternehmen die Digitalkompetenz bei der Auswahl ihrer Aufsichtsratsmitglieder weiterhin eher wenig (siehe „Digitale Kompetenz als Auswahlkriterium für ein Aufsichtsratsmitglied" unter Abschnitt 1.2).

Der aktuelle Lagebericht des BSI 2021 bewertet die IT-Sicherheitslage als „angespannt bis kritisch" und sieht einen Schwerpunkt in der Ausweitung der Erpressungskriminalität und **Ransomware**, wobei insbesondere Löse-, Schutz- und Schweigegelderpressungen genannt werden.[5] Auch die Anzahl an jährlich neu hinzukommenden Schadprogrammvarianten steigt weiter an und umfasst nun 144 Mio. neue Programme, was einen Sprung von **22 %** im Vergleich zum Vorjahr darstellt. Ein ähnliches Bild ergibt sich durch die Analysen des BKA, die einen Anstieg der Cyberstraftaten um **12 %** im Jahr 2021 verzeichnen und **Ransomware als größte Bedrohung** in diesem Zusammenhang ansehen.[6] Insgesamt wird durch die Studie eine kontinuierlich hohe Betroffenheit der Unternehmen deutlich. Bestand nach Erkenntnissen der Compliance-Studie 2021 noch ein erheblicher Nachholbedarf für unternehmerische Maßnahmen in Bezug auf Ransomware, zeigen die aktuellen Entwicklungen eine starke Verbesserung in diesem Bereich.

Bereits durchgeführte IT-Sicherheitsmaßnahmen korrelieren ausweislich der Befragung zudem mit der hierdurch ausgelösten Schutzwirkung. Haben Unternehmen bereits Instrumente zur Gewährleistung von IT-Sicherheit ergriffen, zeigten sie sich weniger skeptisch im Hinblick auf das Risiko von Compliance-Vorfällen als Unternehmen, die solche Maßnahmen noch nicht durchgeführt haben.

2.2 Maßnahmen zur Gewährleistung von IT-Sicherheit und Datenschutz

In Anbetracht der Cyberkriminalität und zunehmenden IT-Sicherheitsrisiken liegt es im eigenen Interesse der Unternehmen, IT-Compliance wirkungsvoll umzusetzen.

Bestimmte Anforderungen können sich dabei unmittelbar oder mittelbar aus gesetzlichen Bestimmungen für die Unternehmen ergeben. Bei der Untersuchung konkret umgesetzter Maßnahmen im Bereich der IT-Sicherheit ist zu beachten, dass kein einheitliches IT-Sicherheitsgesetz besteht, das die umzusetzenden Pflichten und Maßnahmen für alle Unternehmen gleichermaßen reguliert und umsetzt.[7]

Unmittelbare behördlich überprüf- und durchsetzbare Pflichten[8] ergeben sich für bestimmte Unternehmen aus dem **BSIG**, das in Umsetzung der IT-Sicherheitsgesetze und der NIS-RL erweitert wurde und einen größeren Adressatenkreis umfasst. Direkt adressiert sind dort **Anbieter kritischer Infrastrukturen** (KRITIS-Betreiber) sowie wichtige **Zulieferer, bestimmte öffentliche Stellen, Anbieter digitaler Dienste und Unternehmen im besonderen öffentlichen Interesse**.

---

5 Bundesamt für Sicherheit in der Informationstechnik (BSI): Die Lage der IT-Sicherheit in Deutschland 2021, S. 9.

6 Bundeskriminalamt (BKA): Bundeslagebild Cybercrime 2021, S. 2.

7 Vgl. auch Conrad in Auer-Reinsdorff/Conrad: Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 33 Rn. 10.

8 Vgl. dazu auch Riehm/Meier: MMR 2020, 571.

Diese Unternehmen müssen in unterschiedlichen Abstufungen angemessene technische und organisatorische Maßnahmen zum Schutz der IT-Sicherheit nach dem **Stand der Technik** umsetzen. Konkretisiert werden die Anforderungen an technisch-organisatorische Maßnahmen durch anerkannte Branchenspezifische Sicherheitsstandards (B3S) oder eine Orientierung an nationalen und internationalen Standards und Normen.

Ist ein Unternehmen keinem dieser Bereiche zuzuordnen, können sich IT-sicherheitsrechtliche Pflichten daneben aus **mittelbarer Betroffenheit des BSIG** oder **branchenspezifischen Gesetzen** wie etwa im Rahmen von Bank- und Finanzdienstleistungen ergeben.[9] Arbeiten Unternehmen als Dienstleister mit KRITIS-Betreibern zusammen, können sich auch für sie mittelbare Verpflichtungen aus dem BSIG aufdrängen.[10] Diese Pflichten werden zudem auch von nicht regulierten Unternehmen oftmals als „**Best Practice**" berücksichtigt und ebenso als **IT-Sicherheitsstandard** etabliert.[11] Daneben ergeben sich technisch-organisatorische IT-Sicherheitspflichten auch aus dem in der DS-GVO verankerten **datenschutzrechtlichen Grundsatz der Vertraulichkeit und Integrität**.[12]

Außerhalb (un)mittelbarer gesetzlicher Verpflichtungen ist die Einhaltung der IT-Sicherheit insbesondere **haftungsrechtlich** relevant und deshalb im Hinblick auf die Einhaltung von Compliance-Pflichten essenziell. Die Umsetzung der IT-Sicherheit kann aus zivilrechtlicher, aber auch versicherungs- oder wettbewerbsrechtlicher Perspektive wichtig sein.[13] Pflichten für die Umsetzung von IT-Sicherheit können sich aber auch im Rahmen der **allgemeinen Sorgfalts- und Geschäftsleitungspflichten** ergeben.[14] Durch ihre immer größer werdende Bedeutung kann die Gewährleistung der IT-Sicherheit zur Sorgfalt einer ordentlichen und gewissenhaften Geschäftsleitung gehören.[15] Je nach Art und Größe des Unternehmens[16] sind angemessene Instrumente wie die verpflichtende Einrichtung von Sicherheitsmaßnahmen sowie ein Risikomanagement zu implementieren.[17] Die Pflicht der Geschäftsleitung erfasst zudem die Pflicht zur Sicherung des Fortbestands des Unternehmens[18] sowie eine nicht näher konturierte[19] **Risikofrüherkennungspflicht** auch hinsichtlich IT-Sicherheitsgefährdungen. Auch der Aufsichtsrat ist als Kontroll- und Überwachungsorgan mittelbar von der Einhaltung dieser Pflicht betroffen (siehe Abschnitt 1.1).[20] Aus diesem Grund ist es zu begrüßen, dass IT-Sicherheitsthemen und entsprechende Schutzmaßnahmen in den Aufsichtsräten als sehr wichtig erachtet werden (61 % „hohe Wichtigkeit", siehe Abschnitt 1.4). Im Hinblick auf die Digitalkompetenz von Aufsichtsräten sollten Unternehmen allerdings erwägen, die Anforderungen und die Auswahl für neue Mitglieder im Aufsichtsrat zu prüfen (siehe „Digitaler Sachverstand als Auswahlkriterium für ein Aufsichtsratsmitglied" unter Abschnitt 1.2). Schließlich muss z.B. handelsrechtlich auch die elektronische **Buchführung** rechtssicher ausgestaltet sein.[21]

Insgesamt zeigt sich für Unternehmen ein komplexes Bild, das es erschwert, einzelne und branchenunabhängig einheitlich umzusetzende Maßnahmen der Unternehmen festzulegen und übergreifend abzugleichen.

---

[9] Vgl. zu dieser Pflicht aus § 25a Abs. 1 KWG auch Riehm/Meier: MMR 2020, 571 mwN; vgl. zur IT-Sicherheit bei Banken Frisse/Glaßl/Baranowski/Duwald: BKR 2018, 177.

[10] Schmidl/Tannen in Kipker: Cybersecurity, 1. Aufl. 2020, Kap. 6 Rn. 13; so auch Rath/Kuß, Unmuß: Corporate Compliance Checklisten, 4. Aufl. 2020, Kap. 8 Rn. 9.

[11] Rath/Kuß in Unmuß: Corporate Compliance Checklisten, 4. Aufl. 2020, Kap. 8 Rn. 9.

[12] Vgl. dazu Schuhmacher in Bräutigam: IT-Outsourcing und Cloud-Computing, 4. Aufl. 2019, Teil 5 Kap. C. Rn. 114 ff.

[13] Vgl. dazu auch Heckmann: MMR 2006, 280 (283); Riehm/Meier: MMR 2020, 571 (573 ff.).

[14] Vgl. dazu umfassend V.d. Bussche/Schelinski in Leupold/Wiebe/Glossner: IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 81.

[15] Gleiches gilt etwa für die SE, vgl. V.d. Bussche in Kipker: Cybersecurity, 1. Aufl. 2020, Kap. 4. Rn. 36.; für Abweichungen zur GmbH vgl. V.d. Bussche, Kipke: Cybersecurity, 1. Aufl. 2020, Kap. 4. Rn. 51f.

[16] V.d. Bussche in Kipker: Cybersecurity, 1. Aufl. 2020, Kap. 4. Rn. 36.

[17] V.d. Bussche/Schelinski in Leupold/Wiebe/Glossner: IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 99.

[18] Vgl. dazu umfassend V.d. Bussche/Schelinski in Leupold/Wiebe/Glossner:. IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 87.

[19] V.d. Bussche/Schelinski in Leupold/Wiebe/Glossner: IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 87 ff.; vgl. auch Conrad/Streitz in Auer-Reinsdorff/Conrad:. Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 33 Rn. 39 ff.

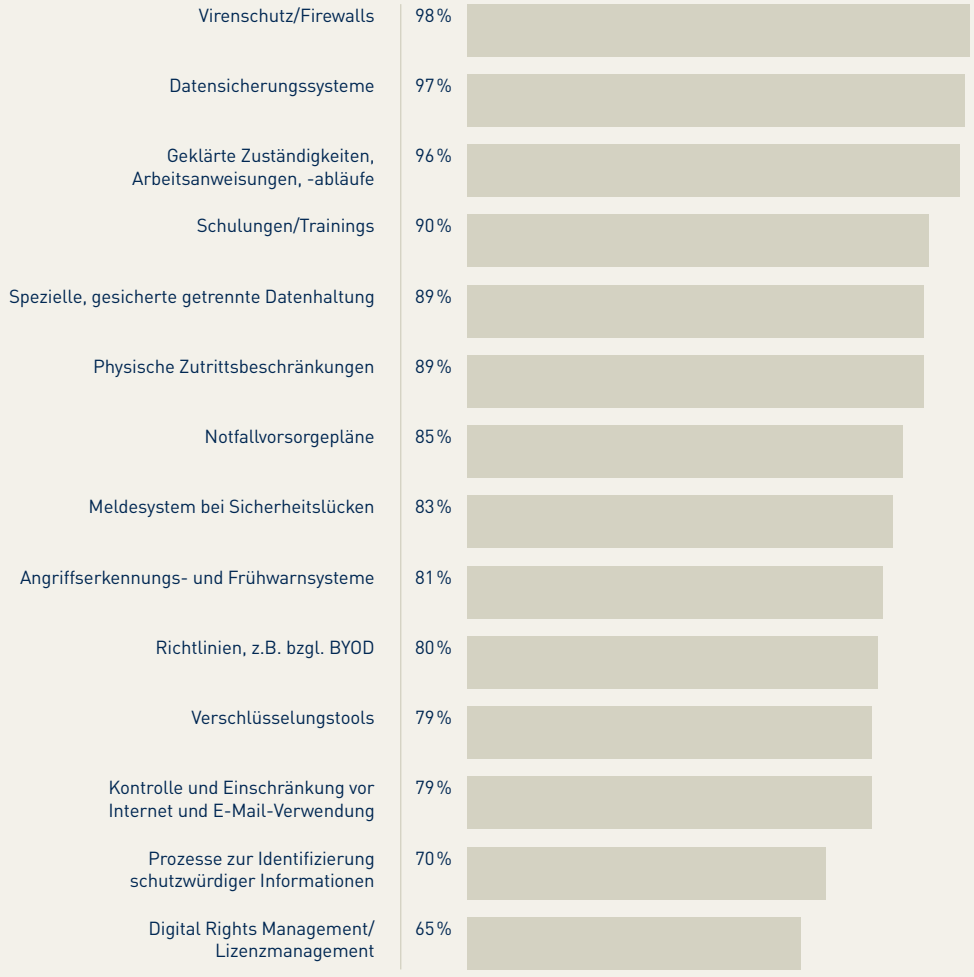
[20] Vgl. Heckmann, MMR 2006, 280 (282).

[21] V.d. Bussche/Schelinski in Leupold/Wiebe/Glossner: IT-Recht, 4. Aufl. 2021, Teil 7.1 Rn. 106.

Orientierung kann dabei das **freiwillige BSI-Grundschutzkompendium** bieten. Das BSI stellt damit eine Zusammenstellung von Maßnahmen zur Verfügung, um einer normalen Gefährdungslage zu begegnen. So kann auf pauschalisierte Vorgehensweisen zurückgegriffen werden, ohne dabei in vielen Fällen auf eigene Risikoanalysen angewiesen zu sein. Diese Maßnahmen sind insbesondere auch an KMUs adressiert und sollen leicht umgesetzt werden können. Daraus kann ein gewisser Grundschutz entstehen, auf dessen Basis das Anstreben von Zertifizierungen möglich wird. Das Grundschutzkompendium ist in verschiedene Bausteine unterteilt und unterscheidet die abgebildeten Maßnahmen nach drei Kategorien: **Basis (B)**, **Standard (S)** und **Erhöhter Schutzbedarf (H)**. Basismaßnahmen stellen das vernünftige Minimum an Schutzvorkehrungen dar, die jedes Unternehmen erfüllen sollte und die es vorrangig umzusetzen gilt, um einen Basisschutz zu gewährleisten. Standardmaßnahmen gewährleisten einen Schutz nach dem Stand der Technik. Maßnahmen mit erhöhtem Schutzbedarf sind nur für Unternehmen erforderlich, die einen solchen insgesamt oder im Hinblick auf einzelne Leistungen bzw. Bestandteile aufweisen.

Maßnahmen zur Gewährleistung von IT-Sicherheit und Datenschutz

Zwölf der 14 Maßnahmen sind in mindestens acht von zehn Unternehmen implementiert.



Frage: Welche Maßnahmen hat Ihr Unternehmen ergriffen, um Ihren Anforderungen an die IT-Sicherheit und den Datenschutz gerecht zu werden?

Basis: alle Unternehmen; Mehrfachnennungen möglich; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Im Rahmen der Studie wurden Unternehmen vorrangig nach der Umsetzung von IT-Sicherheitsmaßnahmen befragt, die sich dem Basis- und Standardschutz des BSI-Grundschutzkompendiums zuordnen lassen können. In branchenüblichen Standards, die eine Umsetzung nach dem Stand der Technik erfordern, sind diese Maßnahmen folglich alle vorgesehen und für bestimmte Unternehmen verpflichtend. Hervorzuheben ist, dass einige der als Minimum erforderlichen Basismaßnahmen von den Unternehmen bereits großflächig umgesetzt wurden: Die Implementierung von Firewalls/Virenschutz (98 %), der Einsatz von Datensicherungssystemen (97 %) und Zuständigkeitsklärungen (96 %) sind bereits in fast allen Unternehmen etabliert. Bei physischen Zutrittsbeschränkungen (89 %) und insbesondere den Richtlinien, z.B. zu BYOD (80 %) besteht dagegen noch Nachholbedarf, da sie vorrangig umgesetzt werden sollten. Meldesysteme bei Sicherheitslücken finden sich mit **83 %** seltener in der Unternehmenspraxis, wobei sich im Branchenvergleich zeigt, dass diese im Handels- und Dienstleistungssektor häufiger umgesetzt wurden (87 %). Instrumente, die als Standardmaßnahmen eingeordnet werden können, sind dagegen nicht so häufig implementiert. Während Schulungen und Trainings noch von **90 %** sowie Notfallpläne von **85 %** der Unternehmen umgesetzt werden, weisen nur **81 %** Angriffserkennungssysteme aus. Zumindest für KRITIS-Betreiber wird – in Umsetzung des IT-Sicherheitsgesetzes 2.0 – der Einsatz von Systemen zur Erkennung und Behandlung von IT-Angriffen ab dem 1. Mai 2023 nicht nur mittelbar über den Stand der Technik, sondern auch gesetzlich im BSIG verpflichtend verankert.

Bei Schulungen und Trainings zeigt sich, dass diese von Unternehmen mit mehr als 1.000 Mitarbeitern mit **93 %** gegenüber **87 %** noch häufiger eingesetzt werden. Weniger Unternehmen setzen Verschlüsselungstools (79 %), Kontrolle der E-Mail- und Internetnutzung (79 %) oder ein Lizenzmanagement (65 %) ein. Im Branchenvergleich zeigt sich, dass Lizenzmanagementsysteme im verarbeitenden Gewerbe mit **72 %** stärker vertreten sind. Im Hinblick auf alle eingesetzten Instrumente ist ein eher reaktiver Umgang mit Risiken zu erkennen. Sicherheitskonzepte wie Trainings, Verschlüsselungstools oder Prozesse zur Identifizierung schutzwürdiger Informationen werden häufiger in Unternehmen eingesetzt, die bereits Compliance-Vorfällen begegnet sind.

Insgesamt kann festgehalten werden, dass einige vom minimalen Basisschutz umfasste Maßnahmen bereits von den meisten Unternehmen umgesetzt werden, während Instrumente, die dem Standardschutz zuzuordnen sind, weniger oft eingeführt wurden. Allerdings besteht auch bei einzelnen Basismaßnahmen noch Nachholbedarf, da diese für einen Minimalschutz primär umzusetzen sind. Nicht abgefragt wurde die Qualität der Umsetzung, also wie die Unternehmen diese Maßnahmen implementiert haben und ob sie dabei nach bestimmten Standards vorgegangen sind.

2.3 Datenschutzvorfälle und deren Verarbeitung

Trotz der zahlreichen von den Unternehmen ergriffenen technischen und organisatorischen Maßnahmen konnten knapp drei von zehn Unternehmen Datenschutzvorfälle im Sinne von „Verletzungen des Schutzes personenbezogener Daten“[22] in der jüngeren Vergangenheit nicht gänzlich verhindern.

Zentrales Kriterium für die nach der DS-GVO im Falle solcher Datenschutzverletzungen zu treffenden Maßnahmen sind die Risiken, die aus solchen Verstößen für die betroffenen Personen folgen. Verstöße, die keine oder nur geringe Risiken für die betroffenen Personen mit sich bringen, sind der zuständigen Datenschutzbehörde nicht zu melden, mittlere oder hohe Risiken auslösende Verstöße sind hingegen zwingend meldepflichtig. Bei Verstößen mit hohen Risiken sind zusätzlich zu einer Behördenmeldung auch die von dem Vorfall betroffenen Personen zu informieren.[23]

28 % der befragten Führungskräfte geben an, dass es in den letzten drei Jahren Anlass zur Meldung von Datenschutzvorfällen gegeben hat. Interessant: Unternehmen, die im Bereich Datenschutz und IT-Sicherheit über eine besonders breite Palette getroffener Maßnahmen verfügen, berichten häufiger von meldepflichtigen Vorfällen. Bei Unternehmen, die eine hohe Zahl von Datenschutz- und IT-Sicherheitsmaßnahmen umgesetzt hatten (mindestens 13 von 14 eingesetzten Maßnahmen), registrierte immerhin jedes Dritte Datenschutzvorfälle, wohingegen bei Unternehmen, die weniger Maßnahmen getroffen hatten, nur jedes Fünfte in den letzten drei Jahren Datenschutzvorfälle registrierte (34 ggü. 21 %).

---

[22] Vgl. die Definition einer „Verletzung des Schutzes personenbezogener Daten“ in Art. 4 Nr. 12 DS-GVO.

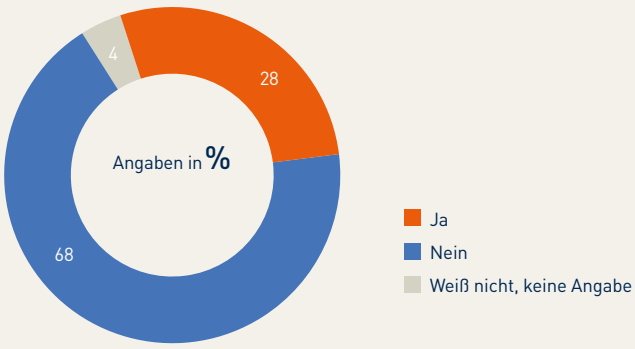
[23] Art. 34 DS-GVO.

Dieses Ergebnis dürfte insbesondere damit zusammenhängen, dass Unternehmen, die zur Gewährleistung von IT-Sicherheit und Datenschutz schon umfassende Maßnahmen getroffen haben und meist auch über im Datenschutz spezialisierte Ressourcen verfügen, Datenschutzverletzungen typischerweise eher feststellen als andere Unternehmen, die meldepflichtige Datenschutzverletzungen infolge fehlender Sensibilisierung und fehlender datenschutzrechtlicher Kompetenzen überhaupt nicht als solche erkennen, entdecken und deshalb auch erforderliche Meldungen nicht vornehmen. Ähnlich ist vermutlich auch zu erklären, warum Unternehmen mit einer eigenen Datenschutzabteilung oder einer speziellen IT-Sicherheitsabteilung mehr Datenschutzvorfälle angeben als Unternehmen ohne dedizierte Fachabteilungen.

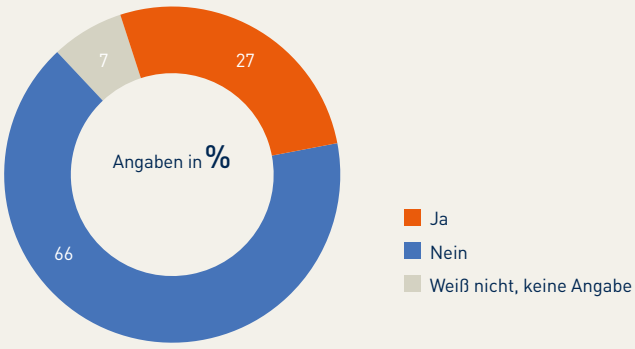
Datenschutzvorfälle

27 % der Unternehmen sahen sich gezwungen, Vorfälle zu melden.

Anlass zur Meldung in den letzten drei Jahren



Tatsächliche Meldung in den letzten drei Jahren



Fragen: Hatte Ihr Unternehmen in den letzten drei Jahren Jahr Anlass zur Meldung von Datenschutzvorfallen? Und hat Ihr Unternehmen in den letzten drei Jahren Datenschutzvorfälle gemeldet?

Basis: alle Unternehmen; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Größere Unternehmen ab 1.000 Beschäftigten berichten insgesamt deutlich häufiger von Datenschutzverletzungen (33 %) als kleinere (21 %). Dabei ist der Anteil der betroffenen Unternehmen im Handels- und Dienstleistungssektor signifikant größer als im verarbeitenden Gewerbe. Das dürfte schon daran liegen, dass mit der Größe des Unternehmens meist auch die Intensität der Datenverarbeitung steigt und damit auch das Risiko von Datenschutzverletzungen. Auch dürften Handels- und Dienstleistungsunternehmen regelmäßig personenbezogene Daten in größerem Umfang und/oder an mehr Schnittstellen innerhalb ihrer Unternehmensprozesse verwenden als verarbeitende Unternehmen. Auch das erhöht bei Handels- und Dienstleistungsunternehmen die Wahrscheinlichkeit von Datenschutzverletzungen.

Der Anteil der Unternehmen, die von ihnen erkannte meldepflichtige Datenschutzvorfälle dann auch tatsächlich der zuständigen Aufsichtsbehörde gemeldet haben, unterscheidet sich nur minimal vom Anteil der Unternehmen, die insgesamt von meldepflichtigen Vorfällen berichten (27 ggü. 28 %). Lediglich in vier Interviews wurde angegeben, dass Datenschutzvorfälle schlussendlich noch nicht gemeldet worden seien. Die genauen Hintergründe dieser Diskrepanz konnten im Rahmen dieser Studie nicht weiter beleuchtet werden.

Auch Datenschutzvorfälle, die infolge ihrer niedrigen Risikoklassifizierung der zuständigen Behörde nicht gemeldet werden müssen, sind in jedem Fall exakt zu dokumentieren.[24] Das umfasst neben einer genauen Beschreibung des Vorfalls, der getroffenen Maßnahmen sowie weiterer Informationen insbesondere auch die Risikobeurteilung und -klassifizierung selbst. Zusätzlich verpflichtet auch die datenschutzrechtliche Rechenschaftspflicht[25] die verantwortlichen Unternehmen dazu, geeignete Dokumentationen vorzuhalten, um nachweisen zu können, dass und wie sie die Anforderungen des Datenschutzrechts einhalten.

Abgesehen davon, dass jedes Unternehmen verpflichtet ist, durch geeignete Richtlinien und Arbeitsanweisungen interne Prozesse zum Umgang mit Datenschutzverletzungen zu implementieren, sind der ordnungsgemäße Umgang mit Datenschutzverletzungen und deren korrekte Dokumentation ohne hierfür festgelegte Unternehmensprozesse in der Praxis kaum zu bewältigen. So haben auch drei von vier Unternehmen in Deutschland (73 %) entsprechende Prozesse aufgesetzt, die eine Feststellung und Aufarbeitung von Datenschutzverletzungen regeln. Während nur jedes siebte größere Unternehmen ab 1.000 Beschäftigten dezidiert angibt, keine entsprechenden Prozesse implementiert zu haben (14 %), ist dieser Anteil in kleineren Unternehmen immerhin fast doppelt so hoch (27 %).

[24] Art. 33 Abs. 5 DS-GVO.

[25] Art. 5 Abs. 2 DS-GVO.

3. Cloud-Anbieter

3.1 Cloud und Compliance

Das Cloud-Computing hat in den letzten Jahren für die Unternehmen enorm an Bedeutung gewonnen.

Laut einer Studie der Wirtschaftsprüfungsgesellschaft KPMG nutzten im Frühjahr 2022 bereits **84 %** der Unternehmen Cloud-Dienste.[26] Im Jahr 2018 lag dieser Wert noch bei **73 %**.[27] Die Vorteile dieser IT-Lösung liegen für die Unternehmen auf der Hand. Über die Cloud kann der individuelle Bedarf an IT flexibel vom Provider angefordert werden. Das Unternehmen muss selbst keine unnötigen Ressourcen vorhalten, sondern kann die im jeweiligen Moment benötigten Kapazitäten vom Anbieter abrufen („pay as you go"). Die bedarfsorientierte Bereitstellung der IT-Infrastruktur ermöglicht es den Unternehmen, sich auf ihr Kerngeschäft zu konzentrieren. In Zeiten des rasanten technologischen Fortschritts bietet dieser Aspekt den Vorteil, dass der Provider die IT-Infrastruktur jeweils auf dem aktuellen Stand hält. Darüber hinaus ist der Bezug von IT-Leistungen über die Cloud gegenüber dem eigenen Betrieb wesentlich **kostengünstiger**, weil sich hier die Skaleneffekte des Providers nutzen lassen.

Die Nutzungsgebühren für Cloud-Dienste sind in der Regel niedriger als die Kosten für individuelle Nutzerlizenzen und der Wartungsaufwand für Hard- und Software ist deutlich geringer.[28] Zudem erfordern Cloud-Dienste oft lediglich eine **schlichte Internetverbindung**, sodass sie zeit- und vor allem ortsunabhängig genutzt werden können. Insgesamt wird damit eine Infrastruktur geboten, die sich jeder leisten kann. Es kommt mithin zu einer **Demokratisierung der Digitalisierung**. Zudem damit kann auch den Mitarbeiterinnen und Mitarbeitern der Unternehmen ein flexibles Arbeiten ermöglicht werden.

Auf dem Markt finden sich viele verschiedene Servicemodelle: Grundsätzlich kann jede Infrastruktur, Plattform oder Software in die Cloud verlagert werden. Beim „**Infrastructure as a Service**" stellt der Provider die IT-Infrastruktur bereit, mithin Speicherkapazität, Netzwerkbandbreiten oder weitere für den Betrieb eines virtuellen Systems erforderliche Ressourcen. Im Rahmen der „**Platform as a Service**" stellt der Provider neben der Hardware zusätzlich auch eine Plattform zur Konzeption, Entwicklung und Testung von Anwendungen zur Verfügung. Bietet der Provider dem Kunden eine fertige Anwendung, handelt es sich um „**Software as a Service**".

Trotz der weiten Verbreitung und der vielen verfügbaren Servicemodelle sind den Unternehmen die mit dem Einsatz der „Cloud" verbundenen Risiken offenbar nicht vollständig bewusst. In der **Compliance-Studie 2021** wurde dies bereits letztes Jahr festgestellt: Nur **16 %** der Verantwortlichen sahen beim Einsatz von Cloud-Computing ein hohes Risiko von Rechtsverletzungen. Ganz überwiegend war das **Risikobewusstsein eher gering ausgeprägt**. Über ein Drittel der Befragten (35 %) verbanden mit dem Cloud-Einsatz nur ein mittleres, **44 %** der Verantwortlichen sogar nur ein geringes Risiko.[29]

Diese Aussagen sind verwunderlich, fallen doch in diesem Bereich sofort zahlreiche Herausforderungen ins Auge.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat sich ebenfalls mit den Risiken des Cloud-Computing beschäftigt und dabei mehrere Risiken identifiziert, wobei die folgenden herausstechen:

Zum einen ist mit der Auslagerung der Infrastruktur in die Cloud der **Verlust der physischen Kontrolle**[30] über die beauftragten IT-Leistungen an den Anbieter verbunden. Damit kann das Unternehmen nicht mehr selbst den reibungslosen Betrieb seiner Anwendungen sicherstellen und hat die Behebung

---

[26] https://www.cio.de/a/der-boom-im-cloud-markt-haelt-an,3687430.

[27] https://www.office-conference.com/news/studie-cloud-nutzung-auf-rekordniveau-bei-unternehmen#:~:text=Cloud%20Computing%20w%C3%A4chst%20so%20stark,(2017%3A%2066%20Prozent).

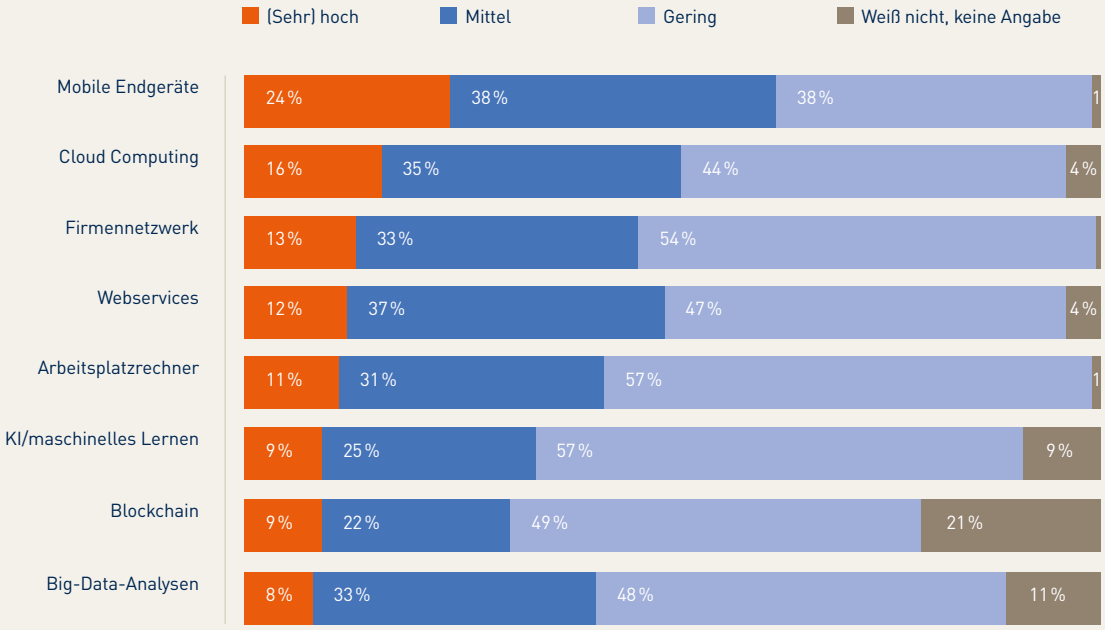
[28] Bräutigam/Thalhofer: Bräutigam in IT-Outsourcing und Cloud-Computing, 2019, S. 1270.

[29] Noerr Partnerschaftsgesellschaft mbB/Technische Universität München (TUM): Digitalisierung und Compliance, Compliance-Studie 2021, S. 17 f.

[30] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/Cloud-Risiken-und-Sicherheitstipps/cloud-risiken-und-sicherheitstipps_node.html.

Risikograd von Rechtsverletzungen im Bereich digitaler Technologien

Laptops, Smartphones und Tablets am ehesten risikobehaftet.



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, Zahlen gerundet.

Quelle: Kantar – quantitative Befragung 2021 im Auftrag von Noerr

von Störungen nicht mehr selbst in der Hand. Zum anderen können **Lock-in-Effekte** entstehen,[31] die das Unternehmen aus technischen oder funktionellen Gründen faktisch daran hindern, die Cloud-Leistungen auf einen anderen Provider oder wieder zurück in die eigene IT-Abteilung zu migrieren. Dem wird in der Praxis mit entsprechender vertraglicher Gestaltung, insbesondere der Aufnahme von besonderen Kündigungsrechten begegnet. Ob darüber hinaus gesetzliche Pflichten zur Datenportabilität statuiert werden müssen – wie etwa im Falle der Art. 23 ff. des „Data Act"[32] , den die Europäische Kommission vorgelegt hat – ist vor diesem Hintergrund fraglich. Hier bleibt die weitere Diskussion abzuwarten.

Zudem geht mit der Internetanbindung der Cloud-Dienste nach Auffassung des BSI auch das Risiko eines unbefugten Zugriffs Dritter von außen einher. Erfolgt der Zugriff über unsichere Netze – etwa einen WLAN Hotspot am Flughafen –, könnten Angreifer die Zugangsdaten abgreifen und damit Informationen in der Cloud **leicht ausspähen**.[33] In diesem Zusammenhang steht auch die Gefahr, dass Angreifer mithilfe von Anfragen einer großen Zahl von Rechnern den **Cloud-Dienst blockieren** (sog. „**Distributed-Denial-of-Service-Angriff**"); die Cloud-Leistungen also für die Kunden nicht mehr verfügbar sind.[34]

Der verstärkte Einsatz von Cloud-Lösungen im Unternehmen muss daher auch den Aufsichtsrat auf den Plan rufen. Oft verarbeiten die Unternehmen über diese Technologie die für den Jahresabschluss relevanten Zahlen.

---

[31] Bundesamt für Sicherheit in der Informationstechnik: Sichere Nutzung von Cloud-Diensten. Schritt für Schritt von der Strategie bis zum Vertragsende, 2016, S. 17.

[32] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über harmonisierte Vorschriften für einen fairen Datenzugang und eine faire Datennutzung, COM(2022) 68 final.

[33] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/Cloud-Risiken-und-Sicherheitstipps/cloud-risiken-und-sicherheitstipps_node.html.

[34] European Network and Information Security Agency: Cloud computing: benefits, risks and recommendations for information security, S. 5 (abrufbar unter: https://www.enisa.europa.eu/media/news-items/cloud-computing-speech).

Möglicherweise liegt der Grund für das geringere Risikobewusstsein der Unternehmen beim Cloud-Computing jedoch auch darin, dass sich viele Cloud-Provider, insbesondere die großen „Hyper-Scaler" durch umfangreiche Maßnahmen dieser Risiken bereits angenommen haben. Dazu gehören auf Ebene der **physischen IT-Sicherheit** etwa die mehrfache Prüfung der Zutrittsberechtigung sowohl innerhalb als auch außerhalb der Rechenzentrumsgebäude, die Überwachung des Geländes durch Videokameras und der Einsatz von Sicherheitspersonal rund um die Uhr.[35] Zudem setzen die Provider oft speziell auf die Cloud-Umgebung angepasste, **mehrschichtige, intelligente Firewalls** ein, die bestimmte Angriffsmuster erkennen und abblocken.[36] Zur Verhinderung eines unbefugten Zugriffs auf die Cloud-Systeme setzen die Provider zudem auf eine **Multi-Faktor-Authentifizierung**, also die Verwendung von mehr als einer Verifizierungsmethode, wenn ein User auf die Systeme zugreifen möchte.[37]

Überdies bieten die Cloud-Provider ihren Kunden **umfangreiche Zertifizierungen**. Darunter befinden sich insbesondere solche der **ISO-27000-Familie**, der weltweit anerkanntesten und verbreiteten Standards für das Informationssicherheitsmanagement.[38] Auch deutsche Zertifizierungsstandards wie den **Cloud-Computing-Standard für die IT-Sicherheit in Deutschland (C5)** können die Provider oft erfüllen.[39] Ein weiteres wichtiges Sicherheitselement ist die **Verschlüsselungen der Daten**. Die Provider bieten ihren Kunden dazu Tools, mit denen die Daten während der Übertragung („encryption in transit") und im Ruhezustand („encryption at rest") verschlüsselt werden, um sicherzustellen, dass nur autorisierte Benutzer darauf zugreifen können.[40] Um zusätzlich der Gefahr eines Ausfalls vorzubeugen, setzen die Provider auch auf **redundante Systeme**, sodass im Falle der Störung eines Systems auf ein weiteres problemlos zugegriffen werden kann.[41] Damit haben die großen „Serverfarmen" oft ein höheres Sicherheitsniveau als die von den Unternehmen selbst betriebenen Hardwaresysteme und On-Premise-Lösungen.

Unabhängig davon lohnt es sich aber dennoch, einen genaueren Blick auf die Themen IT-Sicherheit und Datenschutz zu werfen.

3.2 Datenschutz und Cloud

Sofern Cloud-Anwendungen auf Servern außerhalb der EU betrieben werden und damit einhergehend personenbezogene Daten in außerhalb der EU belegene Drittländer transferiert werden, sind die erhöhten Anforderungen der DS-GVO an solche Drittlandtransfers zu beachten.

Das gilt auch dann, soweit aus Drittländern heraus auf in der EU belegene Daten zugegriffen wird, etwa im Zusammenhang mit Supportleistungen von Cloud-Providern. Soweit die EU-Kommission das Datenschutzniveau einzelner Drittländer als ausreichend angemessen erachtet und entsprechende Angemessenheitsbeschlüsse erlassen hat,[42] sind Datentransfers in solche Drittländer vergleichbar mit Datentransfers innerhalb der EU und grundsätzlich unproblematisch. Für Datentransfers in andere Drittländer, für die kein Angemessenheitsbeschluss besteht, sieht die DS-GVO eine Reihe von Möglichkeiten vor, um geeignete Garantien für Datentransfers zu schaffen. Das setzt voraus, dass die vom Drittlandtransfer betroffenen Personen im jeweiligen Drittland hinreichend durchsetzbare Rechte und Rechtsbehelfe haben, insbesondere mit Blick auf etwaige Zugriffe auf die sie betreffenden Daten im jeweiligen Drittland.

---

35 Vgl. dazu etwa die physischen Sicherheitsmaßnahmen des Providers IBM, https://www.ibm.com/cloud/architecture/architectures/physical-security-arch/.

36 Vgl. dazu etwa die Beschreibung der vom Cloud-Anbieter Oracle eingesetzten Firewall, https://blogs.oracle.com/cloudsecurity/post/announcing-oracle-cloud-infrastructure-network-firewall.

37 Vgl. die Ausführungen des Anbieters Microsoft zum „Identity Management" unter https://docs.microsoft.com/en-us/azure/security/fundamentals/identity-management-overview.

38 Der Anbieter IBM listet dazu auf seiner Webseite ein umfangreiches Verzeichnis seiner regionalen und globalen Zertifizierungen, vgl. https://www.ibm.com/de-de/cloud/compliance.

39 Vgl. dazu etwa die Zertifizierung des Provider AWS, https://aws.amazon.com/de/compliance/bsi-c5/.

40 Der Provider AWS etwa verschlüsselt die Daten des Kunden automatisch auf physischer Ebene am Standort des Rechenzentrums, vgl. https://aws.amazon.com/de/security/.

41 Der Anbieter Microsoft Azure setzt in seinen Rechenzentren redundante Stromversorgung, ein redundantes Netzwerk und ein redundantes Klimasystem ein, https://azure.microsoft.com/de-de/global-infrastructure/.

42 Art. 45 DS-GVO.

In seiner vielbeachteten Schrems II-Entscheidung[43] hat der EuGH im Juli 2020 den Angemessenheitsbeschluss der EU-Kommission zum EU-US-Privacy Shield für ungültig erklärt und den Unternehmen so eine in der Praxis sehr wichtige Grundlage für einfache Datentransfers in die USA entzogen. Aufgrund diverser behördlicher Zugriffsbefugnisse von US-Behörden und mangelnder Rechtschutzmöglichkeiten für EU-Bürger in den USA, so der EuGH, könne man den USA aktuell schlechterdings kein angemessenes Datenschutzniveau attestieren.

Auf dieses Urteil haben die EU-Kommission und die US-Administration im März 2022 mit der politischen Verständigung über ein neues Abkommen zum Datentransfer in die USA, das **Trans-Atlantic Data Privacy Framework**, reagiert. Die Verantwortlichen zeigten sich dabei zuversichtlich, dass diese neue Grundlage für Datentransfers einer gerichtlichen Überprüfung standhält. Der zuständige Kommissar auf EU-Seite, Didier Reynders, bekräftigte, dass die gefundene Lösung solide sei und „den Besonderheiten des amerikanischen Rechtssystems und den Besonderheiten der verschiedenen Akteure Rechnung" trage. Beide Seiten hätten „sehr innovative" Wege gefunden, um die Bedenken des EuGH auszuräumen.[44] Einzelheiten dieses Abkommens, insbesondere zu wirksamen Mitteln der Rechtsdurchsetzung in den USA, sind allerdings noch nicht bekannt. Es bleibt zu hoffen, dass das Trans-Atlantic Data Privacy Framework eine tragfähige, in der Praxis gut handhabbare Lösung bilden wird.

Mit Blick auf bis dahin fortbestehende andere Transfermechanismen hat der EuGH zwar in seiner Schrems II-Entscheidung klargestellt, dass die in der Praxis häufig für den internationalen Datentransfer verwendeten EU-Standarddatenschutzklauseln (oder auch „Standardvertragsklauseln") nicht per se untauglich sind. Weil man bei deren Verwendung die beanstandeten Zugriffsmöglichkeiten von US-Behörden naturgemäß aber nicht ausschließen kann, sind vom Datenexporteur technische, vertragliche und organisatorische Maßnahmen zu treffen, um das geforderte Datenschutzniveau zu erreichen. Dasselbe gilt für Binding Corporate Rules als weiteren möglichen Transfermechanismus.

In der Folge verlangen die europäischen Datenschutzbehörden für Datentransfers in solche Drittländer, denen die EU-Kommission (noch) kein angemessenes Datenschutzniveau bescheinigt hat, neben Standardvertragsklauseln oder Binding Corporate Rules als grundsätzlich weiterhin gültigen Transfermechanismen noch eine genaue Prüfung des konkreten Datentransfers und der Rechtslage im jeweiligen Drittland.[45] Das gilt insbesondere mit Blick auf etwaige Zugriffsmöglichkeiten von Behörden des jeweiligen Drittlandes auf die betroffenen Daten und die EU-Bürgern hiergegen zustehende Rechtsbehelfe. Soweit die betroffenen Daten angesichts der Rechtslage und Behördenpraxis im Drittland nicht ausreichend sicher vor Zugriffen sind, die rechtsstaatlich nicht dem Schutzstandard der DSGVO genügen, bleiben vor allem zusätzliche technische und organisatorische Maßnahmen, um solche Zugriffe zumindest rein faktisch zu verhindern. Diese Prüfungen und Risiken sind im Rahmen sogenannter „Transfer Impact Assessments" im Einzelnen zu dokumentieren.

Cloud-Anwendungen konfligieren daher mit der problematischen datenschutzrechtlichen Fragestellung sicherer Drittstaatentransfers.

3.3 IT-Sicherheit und Cloud

Cloud-Anwendungen werden oft im Zusammenhang mit Sicherheitsrisiken und Datenschutzproblemen genannt, insbesondere wenn dabei personenbezogene Daten in Drittländer transferiert werden (siehe Abschnitt 3.2)

Vor allem bei kleinen und mittleren Unternehmen (KMU) können sie aber auch zur Stärkung der IT-Sicherheit führen. Gerade in diesen Fällen entsteht der Eindruck, dass **Cloud-Lösungen** zwar **sicherheitsrechtlich indiziert**, aber **datenschutzrechtlich kontraindiziert** sind. Anders ausgedrückt: Um IT-Sicherheit zu gewährleisten, benötigt man zuweilen einen größeren Zugriff auf personenbezogene Daten. Hier gilt es, einen angemessenen Ausgleich zu finden.

---

[43] Entscheidung des EuGH vom 16.07.2020 (Rechtssache C311/18 – „Schrems II").

[44] Lima: E.U. justice chief 'confident' data deal with U.S. will survive legal challenge, https://www.washingtonpost.com/politics/2022/06/08/eu-justice-chief-confident-data-deal-with-us-will-survive-legal-challenge/.

[45] Vgl. die Empfehlungen des Europäischen Datenschutzausschusses (EDSA) 01/2020 zu Maßnahmen zur Ergänzung von Übermittlungstools zur Gewährleistung des unionsrechtlichen Schutzniveaus für personenbezogene Daten (Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data | European Data Protection Board (europa.eu)), hierzu im Überblick auch Europäischer Datenschutzausschuss: Aktualisierte Empfehlungen zu internationalen Datentransfers - siehe Noerr News.

Durch Cloud-Lösungen sind Informationen überall und jederzeit verfügbar. Die Vorteile ihrer Nutzung sind neben der guten Skalierbarkeit nicht zuletzt durch die stark zunehmende und aufgrund der COVID-19-Pandemie signifikant gestiegene Arbeit im Homeoffice offensichtlich geworden. In kleinen und mittleren Unternehmen können **Cloud-Lösungen, trotz der zu beachtenden Risiken** (siehe Abschnitt 3.1) mit einer Verbesserung der **IT-Sicherheit** einhergehen, wenn sie ordnungsgemäß implementiert und konfiguriert sind. Die Einhaltung von **Sicherheitsstandards** und **Zertifizierungen** ist mit hohen finanziellen und administrativen Aufwendungen verbunden, die KMU in technisch-organisatorischer Hinsicht und gesetzeskonformer Weise oft nicht gleichermaßen umsetzen können wie große Cloud-Anbieter. Diese weisen zahlreiche Standards und Zertifizierungen nach eigenen Angaben vor und können oftmals einen durchweg hohen Schutzstandard auf dem Stand der Technik gewährleisten (siehe Abschnitt 3.2). Dadurch können sie sich in der Regel durch eine hohe **Ausfallsicherheit** und ein sachverständiges **Ausfallmanagement** auszeichnen, da sie grundsätzlich schneller auf Bedrohungslagen und aufkommende Sicherheitslücken reagieren und die Infrastruktur immer auf dem aktuellen Stand halten können. Aufgrund dieser personellen und strukturellen Kapazitäten können Cloud-Lösungen insbesondere bei KMU mit begrenzten Ressourcen für die dedizierte Gewährleistung der IT-Sicherheit somit einen Anstieg der IT-Sicherheit bedeuten.

Sie stehen aber regelmäßig vor der Problematik, dass viele Anbieter aus EU-Drittländern, insbesondere aus den USA stammen. Dies führt dazu, dass personenbezogene Daten über Server transferiert werden, die in den USA liegen, oder US-Ermittlungsbehörden nach dem sog. **Cloud Act** Daten von den Unternehmen herausverlangen können, selbst wenn diese ihre Server angebotsbezogen in Europa betreiben (siehe Abschnitt 3.2). Cloud-Anwendungen konfligieren daher mit der **problematischen datenschutzrechtlichen Fragestellung sicherer Drittstaatentransfers**.

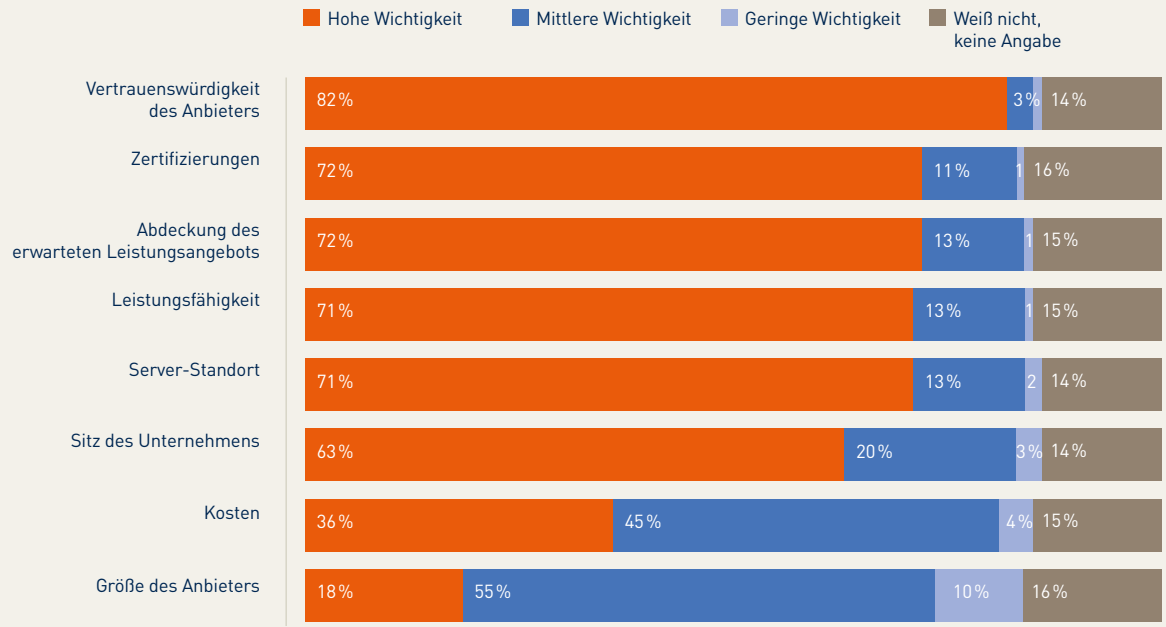
Das Konfliktpotenzial zeigt sich insbesondere seit dem **Schrems II**-Urteil des EuGH im Juli 2020, wodurch der bis dahin bestehende Angemessenheitsbeschluss zwischen der EU und den USA (**Privacy Shield Framework**) mangels eines mit der EU vergleichbaren Datenschutzniveaus in den USA für ungültig erklärt wurde (siehe Abschnitt 3.2). Seitdem besteht erhebliche Rechtsunsicherheit für Datentransfers in die USA. Trotz der auf politischer Ebene erzielten Einigung für ein neues **Trans-Atlantic Privacy Framework** (siehe Abschnitt 3.2), ist gleichwohl zweifelhaft, inwieweit man das erforderliche Datenschutzniveau durch Datenschutzklauseln oder weitere Garantien vollständig rechtssicher erreichen kann. [46]

Unter Heranziehung der Studienergebnisse wird die hohe Bedeutung von Cloud-Lösungen für Führungskräfte sehr deutlich. Dabei wurde die Relevanz bestimmter Kriterien für die Auswahl von Cloud-Anbietern erfragt. Generell zeigen sich dabei hohe Erwartungen an die Cloud-Anbieter, unabhängig von der Größe und der Tätigkeitsbranche der Unternehmen.

[46] Vgl. hierzu Heckmann: Datenschutzkonforme Nutzung von Cloud-Lösungen aus unsicheren Drittländern durch Trennung von Service und Inhalten, Wissenschaftliches Rechtsgutachten vom 27.5.2021, S. 14 ff. (https://www.rohde-schwarz.com/de/loesungen/cybersicherheit/landing-pages/rechtsgutachten-r-s-trusted-gate_255438.html); hier bleiben die weitere Detaillierung des Trans-Atlantic Data Privacy Framework und die Entwicklung abzuwarten, siehe dazu unten auch Ziffer 4.3.

Relevanz von Auswahlkriterien bei Cloud-Anbietern

Fachleute setzen insbesondere auf Vertrauenswürdigkeit der Anbieter.



Frage: Welche Bedeutung messen Sie den folgenden Kriterien bei der Auswahl von Cloud-Anbietern bei? Bitte verwenden Sie für Ihre Bewertung eine Skala von 1 „völlig unwichtig" bis 10 „überaus wichtig".

Basis: alle Unternehmen; Angaben in Prozent, Zahlen gerundet.

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Mit **82 %** wird dabei die Vertrauenswürdigkeit von Anbietern als elementares Auswahlkriterium bei der Wahl der Cloud-Lösung angesehen. Während mehr als **70 %** der Befragten Zertifizierungen sowie den Serverstandort als maßgebliches Kriterium nennen, ist der Sitz des Unternehmens für nur **63 %** der Unternehmen bei der Entscheidung über den Einsatz ihrer Cloud-Lösung wichtig. Unternehmen sollten sich im Hinblick auf US-Anbieter, die dem Cloud-Act unterliegen, auf das beschriebene Spannungsverhältnis zum europäischen Datenschutzrecht sensibilisieren oder für europäische Anbieter offen zeigen, soweit sie ein vergleichbares Schutzniveau und eine entsprechende Leistungsfähigkeit etablieren können. Die Leistungsfähigkeit und die Abdeckung des Leistungsgebots stellen mit über **70 %** ebenfalls wichtige Auswahlparameter dar, während die Kosten (36 %) und die Größe des Anbieters (18 %) keine vergleichbar hohe Wichtigkeit bei der Auswahl des Anbieters genießen. Die Kosten spielen vermehrt für kleine und mittlere Unternehmen eine Rolle.

Der bestehenden Rechtsunsicherheit kann durch Datentreuhandmodelle[47], technische Innovationen oder die Etablierung europäischer Anbieter begegnet werden. Vorgeschlagen wird hierbei insbesondere eine Intermediärslösung, mit der die Nutzung von Cloud-Diensten mit Serverstandort oder Sitz in den Vereinigten Staaten ohne die Übermittlung von Klardaten gewährleistet werden soll.[48] Bis dahin müssen sich Unternehmen aber bei Cloud-Anbietern aus den Vereinigten Staaten der rechtlichen Risiken bewusst sein, selbst wenn diese Server in Europa anbieten. Einen Überblick über mögliche Alternativen zertifizierter deutscher Anbieter bietet u.a. das Projekt TrustedCloud unter der Schirmherrschaft des Bundesministeriums für Wirtschaft und Klimaschutz.[49]

[47] Vgl. Gausling: MMR 2018, 578 (582).

[48] Heckmann: Wie wir den Kreislauf der Schrems-Urteile durchbrechen, libra-rechtsbriefing, 9.5.2022.

[49] Zu finden unter https://www.trusted-cloud.de/de/.

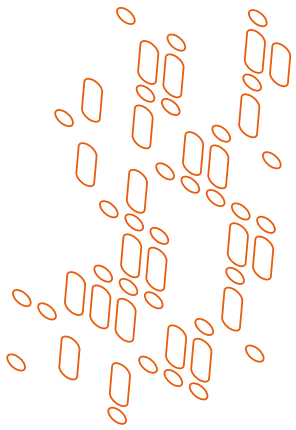
4. Organisation der Unternehmensfunktionen für Datenschutz und IT-Sicherheit

4.1 Organisation der Datenschutzfunktion

Die Einhaltung der datenschutzrechtlichen Anforderungen im Unternehmen kann in der Praxis nur durch ein effektives und tatsächlich gelebtes Datenschutzmanagement gelingen.

Dazu gehört neben wirksamen **Datenschutzprozessen (Ablauforganisation)** insbesondere eine solide **Datenschutz-Governance-Struktur (Aufbauorganisation).**

Die DS-GVO überlässt die Gestaltung der **Datenschutz-Governance** im Sinne eines risikobasierten Ansatzes unter Berücksichtigung der datenschutzrechtlichen Rechenschaftspflicht im Wesentlichen den Unternehmen als datenschutzrechtlich Verantwortlichen. Der Gesetzgeber lässt der Geschäftsleitung also im Rahmen ihrer übergeordneten Gesamtverantwortung für den Datenschutz im Unternehmen großen Spielraum bei der Einrichtung einer angemessenen internen Datenschutzorganisation.



In bestimmten Konstellationen schreiben die DS-GVO und das BDSG die Benennung eines **Datenschutzbeauftragten** vor.[50] Deutsche Unternehmen müssen gemäß BDSG bereits dann einen solchen benennen, wenn sie in der Regel mindestens 20 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen.[51] Unternehmen können entweder einen **internen oder einen externen Datenschutzbeauftragten** benennen.[52] Eine **Unternehmensgruppe** darf unter bestimmten Voraussetzungen auch einen **gemeinsamen Datenschutzbeauftragten** benennen.[53] Zu den **gesetzlich vorgegebenen Aufgaben** des Datenschutzbeauftragen zählen neben der Beratung in Datenschutzfragen vor allem die **Überwachung und Kontrolle** der Einhaltung des Datenschutzes im Unternehmen.[54] Der Datenschutzbeauftragte darf zwar grundsätzlich auch andere Aufgaben und Pflichten wahrnehmen. Allerdings ist dann sicherzustellen, dass derartige Aufgaben und Pflichten nicht zu einem **Interessenkonflikt** führen.[55]

Zwei von drei befragten Unternehmen (67 %) haben bereits eine eigene Abteilung oder Funktion für Datenschutz geschaffen. Ein Drittel verzichtet dagegen bislang auf die Schaffung einer solchen Abteilung oder Funktion. Häufig sind das kleinere Unternehmen mit weniger als 1.000 Beschäftigten (38 %).

---

50 Art. 37 Abs. 1 DS-GVO, § 38 Abs. 1 BDSG.

51 Dazu ausführlich Rücker/Dienst in Gola/Heckmann: Bundesdatenschutzgesetz 13. Aufl. 2019, § 38 Rn. 1-52.

52 Art. 37 Abs. 6 DS-GVO.

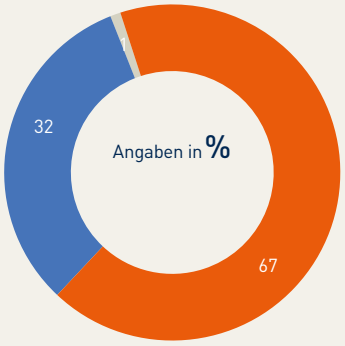
53 Art. 37 Abs. 2 DS-GVO.

54 Art. 39 DS-GVO.

55 Art. 38 Abs. 6 DS-GVO.

Organisation der Datenschutzfunktion

Zwei Drittel der Unternehmen verfügen über eine dedizierte Abteilung bzw. Spezialisten.



Existenz Datenschutzabteilung/ Datenschutzexperten

- Ja
- Nein
- Weiß nicht, keine Angabe

Verortung der/des Datenschutzbeauftragten

50 % **intern**

49 % **extern**

Fragen: Haben Sie eine Datenschutzabteilung oder einen Datenschutzrechtsspezialisten/eine Datensschutzrechtspezialistin im Unternehmen, z.B. innerhalb der Rechtsabteilung? Wer übernimmt in Ihrem Unternehmen die Rolle des oder der Datenschutzbeauftragten?

Basis: alle Unternehmen; Angaben in Prozent Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Mit zunehmender Risikowahrnehmung für die Compliance im Bereich Datenschutz steigt jedoch auch der Anteil der Unternehmen, die eine dedizierte Datenschutzabteilung oder Datenschutzfunktion vorhalten. So haben vier von fünf Befragten (79 %), die das digitalisierungsbedingte Compliance-Risiko für den Datenschutz in ihrem Unternehmen als hoch einschätzen, eine entsprechende Abteilung oder Funktion eingerichtet. Bei schwächerer Risikobewertung fällt auch der entsprechende Anteil mit **64 %** deutlich geringer aus.

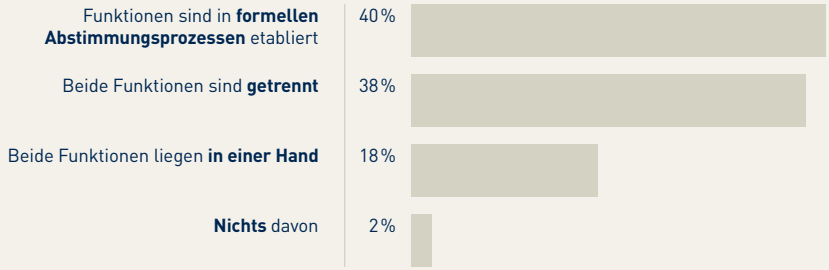
Zudem geht die Einrichtung einer speziellen Datenschutzabteilung oder Datenschutzfunktion oft auch einher mit anderen Datenschutz- und IT-Sicherheitsmaßnahmen, die Unternehmen ergreifen. So verfügen drei Viertel der Teilnehmer, die bereits mindestens 13 der 14 in der Studie betrachteten Maßnahmen im Bereich Datenschutz und IT-Sicherheit umgesetzt haben, auch über eine dedizierte Datenschutzabteilung oder Datenschutzfunktion (74 %).

Die Hälfte der Unternehmen besetzt die Rolle ihres Datenschutzbeauftragten mit einer Person aus den eigenen Reihen (50 %), die andere Hälfte benennt externe Datenschutzbeauftragte (49 %). Bei kleineren Unternehmen ist die Benennung eines externen Datenschutzbeauftragten deutlich verbreiteter (56 % bei Unternehmen mit weniger als 1.000 Beschäftigten). Größere bevorzugen dagegen mehrheitlich die Benennung eines internen Datenschutzbeauftragten (57 %), vor allem, wenn im Unternehmen bereits eine eigene dedizierte Abteilung oder Funktion für den Datenschutz existiert (70 %).

Die Einhaltung des Datenschutzes stellt ein zentrales und in den vergangenen Jahren durch die verschärften rechtlichen Anforderungen zunehmend wichtiges Element der Compliance dar. Insoweit stellt sich auch die Frage, wie Unternehmen die Zusammenarbeit zwischen Datenschutz- und Compliance-Abteilungen gestalten.

Zusammenarbeit Datenschutzfunktion/ Compliance-Abteilung

Vier von zehn Unternehmen verfügen über formale Abstimmungsprozesse, fast genauso häufig sind die Funktionen getrennt organisiert.



Frage: In welcher Form arbeitet die Datenschutzabteilung bzw. der oder die Datenschutzbeauftragte mit der Compliance-Abteilung zusammen?

Basis: Unternehmen mit einer Datenschutzabtellung/einem oder einer Datenschutzbeauftragten; Angaben in Prozent, Zahlen gerundet.

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Fast vier von zehn Unternehmen trennen ihre Datenschutz- und Compliance-Abteilungen strikt voneinander (38 %). Die Mehrheit bevorzugt dagegen eine Organisation, bei der die beiden Funktionen entweder in formellen Abstimmungsprozessen zusammenwirken (40 %) oder sogar ganz in einer Hand liegen (18 %). Größere Unternehmen ab 1.000 Beschäftigten tendieren dabei eher als kleinere zu einer formalisierten Zusammenarbeit der Abteilungen (44 ggü. 37 %). Industrie-Unternehmen tendieren eher als jene des Handels und der Dienstleistungssektoren zu einer klaren Trennung (42 ggü. 35 %).

4.2 Verzeichnis von Verarbeitungstätigkeiten

Ganz allgemein verpflichtet schon die datenschutzrechtliche Rechenschaftspflicht[56] Unternehmen dazu, geeignete Dokumentationen vorzuhalten, um nachweisen zu können, dass und wie sie die Anforderungen des Datenschutzrechts einhalten.

Zusätzlich und ganz konkret verpflichtet die DS-GVO die Unternehmen zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten[57], also zur Dokumentation der Geschäftsprozesse, in denen sie personenbezogene Daten verarbeiten.

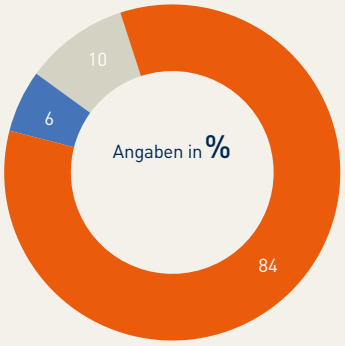
Da es sich um gesetzliche Vorgaben handelt, wundert es wenig, dass mit **84 %** die große Mehrheit der befragten Führungskräfte bestätigt, dass ihr Unternehmen ein solches Verarbeitungsverzeichnis führt.

[56] Art. 5 Abs. 2 DS-GVO.

[57] Vgl. Art. 30 DS-GVO.

Verzeichnis von Verarbeitungstätigkeiten

84 % der Unternehmen führen ein Verzeichnis; meist ist der/die Datenschutzbeauftragte verantwortlich.



Existenz eines Verzeichnisses von Verarbeitungstätigkeiten

- Ja
- Nein
- Weiß nicht, keine Angabe

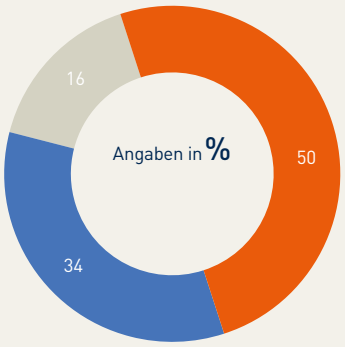
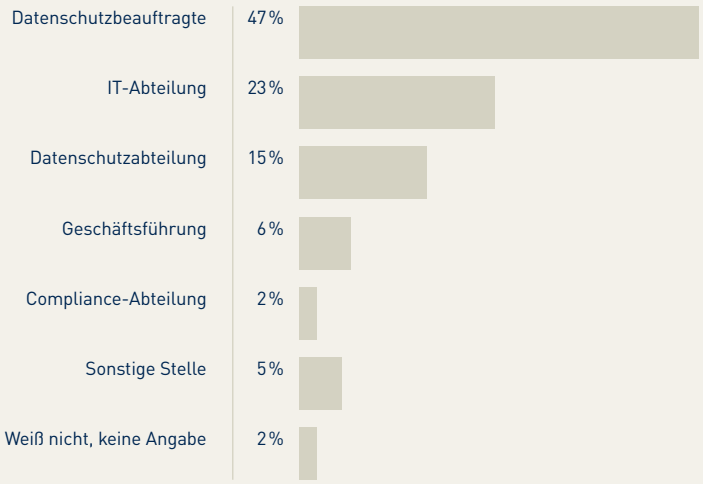


Abbildung durch ein Softwaretool
Basis: Unternehmen mit Verarbeitungsverzeichnis

- Ja
- Nein
- Weiß nicht, keine Angabe

Verantwortungsbereich
Basis: Unternehmen mit Verarbeitungsverzeichnis



Fragen: Führt Ihr Unternehmen ein Verzeichnis von Verarbeitungstatigkeiten? Ist das Verarbeitungsverzeichnis durch ein Softwaretool abgebildet? Wer führt das Verzeichnis?

Basis: alle Unternehmen bzw. Unternehmen mit einem Verarbeitungsverzeichnis; Angaben in Prozent

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Von den größeren Unternehmen haben sogar fast neun von zehn (88 %) ein solches Verzeichnis, in größeren Unternehmen, die zudem noch durch einen Aufsichtsrat kontrolliert werden, der sich mit Fragen der Digitalisierung auseinandersetzt, ist das sogar fast immer der Fall (95 %).

Jedes zweite Unternehmen nutzt dabei für sein Verarbeitungsverzeichnis ein spezielles Softwaretool, das bei der Inventarisierung und oft auch Prüfung datenschutzrelevanter Verarbeitungen unterstützt. Gut ein Drittel der Unternehmen (34 %) erstellt das Verarbeitungsverzeichnis dagegen ohne Softwarelösung. **16 %** der befragten Fachleute machen hierzu keine Angaben. Unternehmen im verarbeitenden Gewerbe greifen dabei etwas häufiger zu Softwarelösungen (54 %). Auch Unternehmen mit einer Datenschutzabteilung arbeiten vermehrt softwareunterstützt, wenn es um die rechtssichere Erfassung von Datenverarbeitungstätigkeiten im Unternehmen geht (53 %).

Das Führen des Verarbeitungsverzeichnisses ist in fast der Hälfte der Unternehmen (47 %) dem Datenschutzbeauftragten zugewiesen. In knapp einem Viertel ist dagegen die IT-Abteilung für die Erfassung aller datenschutzrelevanten Verarbeitungstätigkeiten verantwortlich, in Unternehmen des verarbeitenden Gewerbes noch etwas häufiger als im Bereich Handel und Dienstleistungen (27 ggü. 20 %). Die relativ häufige Verortung dieser für die datenschutzrechtliche Compliance entscheidenden Aufgabe in der IT mag auch an der mit der Digitalisierung einhergehenden inhaltlichen Verzahnungen zwischen IT-Sicherheit und Datenschutz liegen.

Ist neben dem/der Datenschutzbeauftragten auch eine Datenschutzabteilung im Unternehmen vorhanden, so ist oft auch diese zuständig (15 %).

Zuweilen ist das Führen des Verarbeitungsverzeichnisses aber auch „Chefsache". Vor allem in kleineren Unternehmen mit weniger als 1.000 Beschäftigten kümmert sich die Geschäftsführung selbst um die Inventarisierung der entsprechenden Verarbeitungstätigkeiten: In jedem zehnten kleineren Unternehmen ist die Chefetage dafür verantwortlich (10 %), in größeren Unternehmen spielt diese Variante dagegen kaum eine Rolle (3 %).

4.3 Organisation der IT-Sicherheitsfunktion

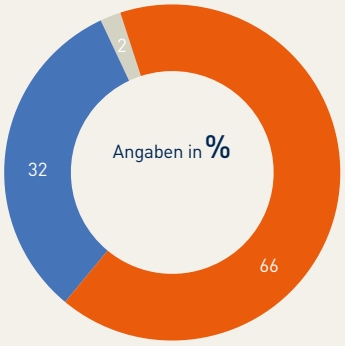
Die hohe Bedeutung einer spezifischen IT-Sicherheitsstelle aufgrund gesetzlicher Verpflichtungen oder der unmittelbaren Bedrohungslage spiegelt sich auch in den Unternehmen wider.

Derzeit verfügen **zwei Drittel der Unternehmen** über eine dezidierte Stelle für die IT-Sicherheit oder einen IT-Sicherheitsbeauftragten bzw. Informationssicherheitsbeauftragten, wobei die Verbreitung trotz der komplexen und unterschiedlichen Anforderungen an die Unternehmen je nach Branche und Unternehmensgröße kaum variiert. Signifikante Unterschiede ergeben sich lediglich bei der Unterscheidung von Unternehmen mit Aufsichtsrat und solchen ohne. Dies kann auch darauf zurückzuführen sein, dass im Aufsichtsrat IT-Sicherheitsthemen eine hohe Relevanz genießen (siehe Abschnitt 1.4) Unternehmen mit Aufsichtsrat haben eine solche Stelle mit **70 %** häufiger eingerichtet als solche ohne, die diese nur zu **56 %** eingerichtet haben. Noch höher ist die Zahl, wenn sich der Aufsichtsrat regelmäßig mit Digitalisierungsthemen befasst (76 %).

Lokalisiert ist die zuständige Stelle in den Unternehmen mit **51 %** größtenteils in der IT-Abteilung. Im Bereich des verarbeitenden Gewerbes findet sich die IT-Sicherheitsstelle sogar zu **65 %** in der IT-Abteilung. Dagegen gibt es branchenübergreifend nur bei **29 %** der Unternehmen einen eigenen Informationssicherheitsbeauftragten. In anderen Abteilungen ist die IT-Sicherheitsstelle seltener aufzufinden. Teilweise ist sie in der Compliance-Abteilung angesiedelt (6 %), beim Datenschutzbeauftragten (5 %), in der Rechtsabteilung (2%) oder an anderer Stelle (5 %). Unterschiede ergeben sich hier in der Handels- und Dienstleistungsbranche. Dort sind die Ansprechpartner häufiger in der Compliance-Abteilung (9 %) oder beim Datenschutzbeauftragten (7 %) angesiedelt.

Organisation der IT-Sicherheitsfunktion

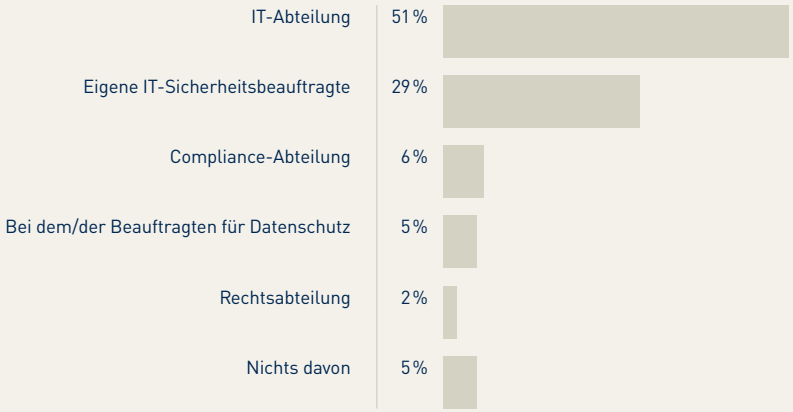
84 % der Unternehmen führen ein Verzeichnis; meist ist der/die Datenschutzbeauftragte verantwortlich.



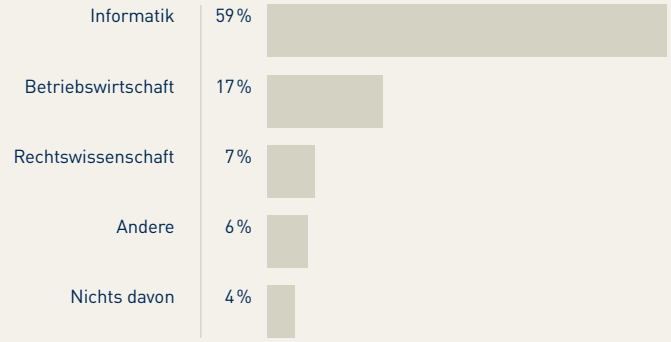
Existenz einer Abteilung/Stelle für IT-Sicherheit

- Ja
- Nein
- Weiß nicht, keine Angabe

Verortung IT-Funktionsstelle im Organigramm
Basis: IT-Sicherheitsstelle/-Abteilung vorhanden



Qualifizierung des/der Beauftragten
Basis: IT-Sicherheitsstelle/-Abteilung vorhanden



Fragen: Haben Sie eine Abteilung oder Stelle (IT-Sicherheitsbeauftragte*r) im Unternehmen speziell für IT-Sicherheit, z.B. in der Rechts- oder IT-Abteilung? Wo ist die beauftragte Stelle oder Abteilung angesiedelt? Welche Qualifizierung hat der oder die Beauftragte?

Basis: alle Unternehmen bzw. Unternehmen mit einer IT-Sicherheitsstelle/Abteilung; Angaben in Prozent, Zahlen gerundet.

Quelle: Kantar – quantitative Befragung 2022 im Auftrag von Noerr

Der Einsatz eines dezidierten Informationssicherheitsbeauftragten ist in vielen Unternehmen, anders als teilweise beim Datenschutzbeauftragten (siehe Abschnitt 4.1), keine unmittelbare gesetzliche Pflicht. Eine solche ergibt sich bereichsspezifisch nur für bestimmte Unternehmen und Branchen, insbesondere nach dem TKG für die Betreiber öffentlicher Telekommunikationsnetze oder Erbringer von öffentlichen Telekommunikationsdiensten.[58] Durch Konkretisierung der Anforderungen kann die Einsetzung eines Informationssicherheitsbeauftragten auch mittelbar vorgesehen sein, z.B. nach aufsichtsrechtlichen Konkretisierungen der technisch-organisatorischen Maßnahmen[59] oder im Bank- und Versicherungswesen.[60] Dies kann auch für Unternehmen mit Pflichten aus dem BSIG gelten, bei denen die Benennung eines Beauftragten zum Stand der Technik bei den erforderlichen technisch-organisatorischen Maßnahmen zu zählen ist.[61] Für andere Unternehmen ist zu hinterfragen, ob sich eine solche Pflicht aus den allgemeinen Pflichten der Geschäftsleitung ergeben kann. Angesichts der akuten Bedrohungslage und der Bedeutung der Verfügbarkeit, Integrität und Vertraulichkeit von IT-Systemen ist die Einrichtung eines Informationssicherheitsbeauftragten aber auch unabhängig von gesetzlichen Vorschriften ein wichtiger Bestandteil der IT-Sicherheit. Auch das BSI empfiehlt die Ernennung eines Beauftragten, wobei es mittlerweile die Bezeichnung Informationssicherheitsbeauftragter (ISB) in Abkehr vom Begriff des IT-Sicherheitsbeauftragten verwendet.[62]

Kritisch zu sehen ist die häufige Ansiedlung der IT-Sicherheitsstelle in der IT-Abteilung. Jedenfalls bezogen auf den dezidierten Informationssicherheitsbeauftragten empfiehlt das BSI, diesen aufgrund von möglichen Rollenkonflikten nicht in der IT-Abteilung, sondern direkt in der obersten Leitungsebene anzusiedeln.[63] Ähnliche Anhaltspunkte ergeben sich z.B. auch aus den „bankaufsichtlichen Anforderungen an die IT (BAIT)“[64]. Danach soll die Funktion zur Vermeidung von Interessenskonflikten organisatorisch und prozessual unabhängig ausgestaltet und funktional von Bereichen getrennt werden, die „für den Betrieb und die Weiterentwicklung der IT-Systeme“ zuständig sind.[65] Insgesamt sollten die Unternehmen darauf achten, bei IT-Sicherheitsstellen, insbesondere eigenen Informationssicherheitsbeauftragten, auf die Vermeidung von Rollen- und Interessenskonflikten zu achten und diese nicht in der operativen IT-Abteilung zu lokalisieren. Eine Vereinheitlichung des Informationssicherheitsbeauftragten und des Datenschutzbeauftragten sieht das BSI dabei als grundsätzlich möglich an, wenn die beiden Rollen klar abgegrenzt sowie dokumentiert sind und genügend Kapazitäten für beide Rollen vorhanden sind; dabei muss auch ein Vertreter bestellt sein.[66]

Für die Qualifikation des Informationssicherheitsbeauftragten finden sich keine unmittelbaren und zentralen branchenübergreifenden Vorgaben.[67] Eine Orientierung bieten die Empfehlungen des BSI-Grundschutzes. Danach soll die Person neben allgemeinen Qualifikationen zu Projektmanagement und der Identifikation mit Zielen der IT-Sicherheit „über Wissen und Erfahrung auf den Gebieten der Informationssicherheit und IT“ verfügen sowie Kenntnisse zu den Geschäftsprozessen der Institution mitbringen.[68] Dies deckt sich mit den meisten angegebenen Qualifikationen der Unternehmen. Danach haben 59 % der IT-Sicherheitsstellen einen informatischen Hintergrund. Bei Unternehmen mit mindestens 1.000 Mitarbeitern machen Informatiker sogar 65 % aus. Weit weniger angegeben sind beispielsweise juristische Hintergründe oder andere Qualifikationen, wobei immerhin 17 % einen betriebswirtschaftlichen Hintergrund haben. Bei kleineren Unternehmen ist zu beobachten, dass hier etwas seltener ein informatischer Hintergrund und etwas häufiger andere Professionen wie die Betriebswirtschaft angegeben wurden. Dabei

---

58 Vgl. Thalhofer in Hornung/Schallbruch: IT-Sicherheitsrecht, § 16 Rn. 47 zu § 109 TKG a.F. (nunmehr § 166 TKG).

59 Vgl. BAIT, Vorbemerkung, Ziffer I Nr. 2.

60 Vgl. Thalhofer in Hornung/Schallbruch: IT-Sicherheitsrecht, § 16 Rn. 48; vgl. zum Bankwesen BAIT, S. 9 Ziffer II Nr. 4.4.

61 Vgl. Thalhofer in Hornung/Schallbruch: IT-Sicherheitsrecht, § 16 Rn. 47.

62 Vgl. BSI: BSI-Standard 200 2, S. 12, 40.

63 Vgl. BSI: BSI-Standard 200 2, S. 40; s. dazu auch BAIT, S. 11 Ziffer 4.5.

64 Rundschreiben der BaFin vom 3.1.2017 auf der Grundlage des § 25a Abs. 1 KWG, https://www.bundesbank.de/resource/blob/832354/f140b319f52671b456b6728506dd15f9/mL/2017-10-bait-data.pdf.

65 BAIT, Ziffer II Nr. 4.5.

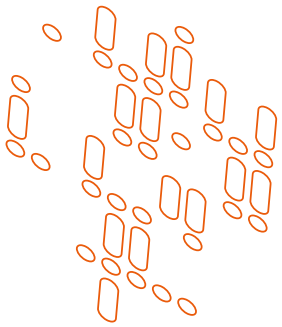
66 Vgl. BSI-Standard 200-2, S. 42f.

67 Vgl. zu § 166 TKG Ferne in Graf: BeckOK StPO mit RiStBV und MiStra, § 166 TKG Rn. 1.

68 Vgl. BSI: BSI-Standard 200 2, S. 41.

ist zu hinterfragen, ob dadurch die erforderliche und geeignete Umsetzung der IT-Sicherheit in Ansehung der Aufgaben und empfohlenen Qualifikationen bei der Umsetzung gewährleistet werden kann. Bei den Aufgaben des Informationssicherheitsbeauftragten können sich Unternehmen an Standards und Normen wie ISO 27002, BSI-Standard 200-2, VdS 3473[69] oder spezifischen Branchenstandards orientieren, um die für das Unternehmen erforderlichen Qualifikationen abgleichen zu können.

Aufgrund der zahlreichen mittelbaren Pflichten zur Einführung von Sicherheitsbeauftragten und der generellen Bedeutung der IT-Sicherheit nicht nur für die Unternehmen selbst, sondern auch potentiell dritte Betroffene, bleibt hier zu fragen, inwieweit gesetzlicher Regelungsbedarf für eine einheitliche Einführung eines Informationssicherheitsbeauftragten analog zum Datenschutzbeauftragten besteht. Eine gesetzliche zentrale Normierung mit abgestuften Pflichten könnte die Rechtsanwendung und Rechtssicherheit durch Auflösung der komplexen Erfordernisse für Unternehmen in unterschiedlichen Branchen und Größen erleichtern.



[69] Däubler in Kipker: Cybersecurity, 1. Aufl. 2020, Kap. 10 Rn. 114; vgl. zu den Aufgaben vgl. BSI, BSI-Standard 200 2, S. 41ff.

Studiendesign

Im Auftrag von Noerr führte Kantar Public im Zeitraum von März bis Mai 2022 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. Seit 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 20 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 und Forschung, geleitet von Herrn Bronner. Ein weiterer Forschungsschwerpunkt des Lehrstuhls liegt im Bereich des IT-Sicherheitsrechts. Unter der Projektleitung von unter anderem Herrn Vogel wird im durch den Verband der Bayerischen Metall- und Elektro-Industrie e.V. (vbm) und den Bayerischen Unternehmensverband Metall und Elektro e.V. (bayme) geförderten Projekt BayWiDi 2.0 kleinen und mittelständischen Unternehmen das IT-Sicherheitsrecht greifbar gemacht.

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.

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 zehn 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, München, New York, Prag, Warschau

Autoren

Prof. Dr. Peter Bräutigam
Rechtsanwalt und Fachanwalt für IT-Recht
Partner
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 bzw. 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 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), Datennutzungsverträgen, Cyber-Security, IT-Transaktionen und Software-Urheberrecht.

Dr. Daniel Rücker, LL.M.
Rechtsanwalt
Partner
Leiter Datenschutz
Mitglied der Practice Group Digital Business

T +49 89 28628457
daniel.ruecker@noerr.com

Daniel Rücker ist spezialisiert im Datenschutz- und IT-Recht und leitet bei Noerr die Praxisgruppe Datenschutz. Neben komplexen datenschutzrechtlichen Fragen, etwa der Strukturierung internationaler Datenflüsse, unterstützt er Mandanten bei der Entwicklung von Datenschutzkonzepten, der Bewältigung von Datenschutzvorfällen und vertritt sie bei datenschutzrechtlichen Auseinandersetzungen vor Gerichten und mit Behörden. Herr Rücker ist Lehrbeauftragter für Datenschutzrecht an der Universität Passau, Mitherausgeber des Rechtshandbuchs „E-Commerce“ sowie Mitherausgeber des internationalen Handbuchs „The New European General Data Protection Regulation, Impact on Corporate Practice – A Guidance for Legal Advisors and Enterprises“.

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-Si- cherheitsrecht, 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.

Valentin Vogel

Valentin Vogel ist wissenschaftlicher Mitarbeiter und Doktorand am Lehrstuhl für Recht und Sicherheit der Digitalisierung an der Technischen Universität München. Dort beschäftigt er sich mit allen Themen rund um das Recht der Digitalisierung. Dies reicht von Fragen des Internetstrafrechts zu solchen des Datenschutzes, der IT-Sicherheit oder Legal Tech. Schwerpunktmäßig forscht er zum Sicherheitsrecht im Kontext der Digitalisierung.

Pascal Bronner

Pascal Bronner ist wissenschaftlicher Mitarbeiter 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. Der Schwerpunkt seiner Forschungsarbeit liegt dabei im Daten- und Datenschutzrecht sowie rechtlichen Fragestellungen Künstlicher Intelligenz.

Mitarbeit
Julian Hofmann
Studentische Hilfskraft

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
München
New York
Prag
Warschau

noerr.com