

2024



Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

Die zunehmende Anzahl von
Kommunikationstools, der Datenaustausch
mit externen Parteien und mangelnde
Kontrolle erhöhen das Risiko

Inhaltsverzeichnis

3 Vorwort

4 Zusammenfassung

5 Einleitung

- 5 Sicherheitsrisiken
 - 6 KI-Cyber-Risiken
 - 6 Compliance-Risiken
 - 6 Menschliche Risiken
 - 8 Methodik für diese Studie
-

9 Insights zu Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

9 Cyberattacken und Datenschutzverstöße

- 9 Insight: Zu viele Datenschutzverstöße bei der Kommunikation sensibler Inhalte
 - 11 Prozesskosten bei Datenschutzverletzungen
-

13 Datentypen und Klassifizierung

- 13 Insight: Keine Verfolgung und Kontrolle des gesamten Datenaustauschs
 - 15 Bewertung der Risiken einzelner Datentypen
-

18 Compliance und Risikomanagement

- 18 Insight: Compliance und Risikomanagement haben höchste Priorität
 - 20 Vorrangige Bereiche für gesetzliche Bestimmungen
 - 21 Schwerpunktbereiche für Validierungen und Zertifizierungen
 - 24 Herausforderungen beim Compliance-Reporting
-

26 Cybersicherheit und Risikomanagement

- 26 Insight: Der Schutz der Kommunikation sensibler Inhalte bleibt eine große Herausforderung
 - 28 Fortschritte in Richtung Zero Trust
 - 29 Mehr Sicherheit für den Schutz sensibler Inhalte
 - 30 Nachverfolgung, Klassifizierung und Kontrolle des Zugriffs auf sensible Inhalte
 - 32 Sicherheitstools für sensible Inhalte
-

33 Operative Prozesse

- 33 Insight: Es braucht ein "Dorf" - und eine Menge Zeit - um Datensicherheit und Compliance zu managen
 - 33 Multiplikation durch externe Parteien und die damit verbundenen Risiken
 - 35 Verbreitung der Kommunikationstools und Risiken
 - 37 Protokollabgleich, der sich summiert
 - 38 Dateigrößenbeschränkungen und Risiken
 - 39 Schlüsselfaktoren für das Risikomanagement bei der Kommunikation sensibler Inhalte
-

40 Fazit

41 Ergebnisse der Umfrage

83 Quellenangaben

Vorwort



Wir freuen uns, Ihnen unseren 2024 Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte vorstellen zu dürfen. Dieser umfassende Bericht bietet wertvolle Einblicke in den aktuellen Stand des Schutzes sensibler Inhalte und die Herausforderungen, denen sich Unternehmen beim Schutz ihrer geschäftskritischen Informationen gegenübersehen.

Der Schutz sensibler Inhalte ist heute wichtiger denn je. Da Unternehmen zunehmend auf digitale Kommunikation und Zusammenarbeit setzen und ihre Ökosysteme mit externen Parteien wachsen, nimmt das Risiko von Datenschutzverletzungen weiter zu. Unser Bericht beleuchtet die Trends und Herausforderungen, denen sich Unternehmen stellen müssen, um die Sicherheit und Compliance ihrer sensiblen Inhalte zu gewährleisten.

Die Schadensereignisse im vergangenen Jahr haben die Risiken im Zusammenhang mit externen Parteien und der Software-Lieferkette erhöht (z. B. die Datenschutzverletzungen bei MOVEit und GoAnywhere Managed File Transfer). Entsprechend hat Verizon in seinem Data Breach Investigations Report (DBIR) 2024 einen dramatischen Anstieg von Datenschutzverletzungen im Zusammenhang mit externen Parteien um 68 % festgestellt, die nun 15 % aller Vorfälle ausmachen. Gleichzeitig sind personenbezogene Daten das Ziel der meisten Cyberangriffe, was Regierungen und Branchenverbände dazu veranlasst, zusätzliche Datenschutzbestimmungen einzuführen, wodurch die Datensicherheit und die Einhaltung der Vorschriften immer komplexer und schwieriger werden.

Wie die Querschnittsanalyse unserer Umfragedaten zeigt, sind die Verbreitung von Kommunikationstools, die zum Versenden und Teilen sensibler Inhalte verwendet werden, sowie die anhaltend hohe Zahl externer Parteien, mit denen sensible Inhalte ausgetauscht werden, kritische Risikofaktoren. Auch das Versäumnis, Kommunikationstools daraufhin zu überprüfen, ob sie über erweiterte Sicherheitsfunktionen verfügen, ist ein wichtiger Aspekt der Umfrageergebnisse. Letztendlich zeigt die Umfrage, dass die Anzahl der Datenschutzverletzungen und die Kosten für Rechtsstreitigkeiten in Unternehmen, die eine größere Anzahl von Kommunikationstools verwenden, sensible Inhalte mit einer größeren Anzahl externer Parteien austauschen und keine fortschrittlichen Sicherheitstechnologien einsetzen, deutlich höher sind.

Auch wenn wir sicherlich ein wenig voreingenommen sind, glauben wir, dass das Kiteworks Private Content Network Unternehmen dabei helfen kann, diese Herausforderungen zu meistern, indem es die Kommunikation von E-Mails und Dateien schützt und es ihnen ermöglicht, die Einhaltung verschiedener Datenschutz- und Cybersicherheitsvorschriften nachzuweisen. Wir hoffen, dass Sie die Daten und Erkenntnisse des diesjährigen Berichts informativ und umsetzbar finden. Wie immer freuen wir uns über Ihre Kommentare und Anregungen.

Mit freundlichen Grüßen

Patrick Spencer

Patrick Spencer, Ph.D.

VP of Corporate Marketing and Research
Kiteworks

Zusammenfassung

Unser Bericht über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte (Sensitive Content Communications Privacy and Compliance Report) bietet Führungskräften in den Bereichen IT, Cybersicherheit, Risikomanagement und Compliance interessante Einblicke in die Daten ihrer Berufskollegen. Ziel ist es, sicherzustellen, dass sensible Inhalte, die über verschiedene Kommunikationskanäle wie E-Mail, Dateifreigabe, Managed File Transfer, Secure File Transfer Protocol (SFTP) und Webformulare versendet und ausgetauscht werden, geschützt sind und den verschiedenen Datenschutz- und Sicherheitsstandards und -validierungen entsprechen.

Die diesjährige Umfrage wurde von Centiment im Zeitraum Februar bis März 2024 durchgeführt. Sie umfasste 33 Fragen zu einer Vielzahl von Themen im Zusammenhang mit Datensicherheit, Datenschutz und Compliance. Einige der Fragen sind "alte Bekannte", d. h. Wiederholungen von Umfragen, die in den letzten ein oder zwei Jahren durchgeführt wurden, während andere neu hinzugekommen sind, um Details zu neuen Trends zu erfassen. Insgesamt gingen 572 Antworten von Führungskräften aus den Bereichen IT, Cybersicherheit, Risikomanagement und Compliance aus Nordamerika, Europa, dem Nahen Osten und Afrika (EMEA) sowie dem asiatisch-pazifischen Raum ein.

Einige Fragen, die wir untersuchen wollten, um wertvolle Trends und Erkenntnisse herauszuarbeiten:

- Wie die Anzahl der Kommunikationstools das Risikomanagement beeinflusst
- Die anhaltenden Auswirkungen von Datenschutzverletzungen auf die damit verbundenen Prozesskosten
- Welche Datentypen das größte Risiko darstellen und warum
- Wie gesetzliche Vorgaben, grundlegende Sicherheitsstandards und umfassendere Datenschutzbestimmungen zu einem besseren Datenschutz beitragen
- Wie erweiterte Sicherheitsfunktionen in Kommunikationstools das Risiko verringern können
- Wie veraltete und unangemessene Ansätze für die Kommunikation sensibler Inhalte zu Ineffizienzen und erhöhten Risiken für Datenschutz und Compliance führen

57%

Können den externen Austausch sensibler Inhalte nicht verfolgen, kontrollieren und dokumentieren

57 % der Befragten gaben an, dass sie nicht in der Lage sind, den Austausch von Inhalten mit externen Parteien zu verfolgen, zu kontrollieren und darüber Bericht zu erstatten. Dies stellt eine *erhebliche Lücke in der Governance* dar.

Zwei Drittel

der Unternehmen tauschen sensible Inhalte mit mehr als 1.000 externen Parteien aus

66 % der Befragten gaben an, dass sie sensible Inhalte mit mehr als 1.000 externen Parteien austauschen. Sobald die Daten das Unternehmen verlassen, wird die Fähigkeit, den Zugriff zu verfolgen und zu kontrollieren, sehr viel wichtiger.

3,55x

höhere Wahrscheinlichkeit mehr als 10 Datenschutzverletzungen zu erleiden, wenn mehr als 7 Kommunikationstools verwendet werden

Je mehr Kommunikationstools ein Unternehmen einsetzt, desto höher ist das Risiko. Befragte, die mehr als 10 Tools nutzen, haben mehr als 10 Datenpannen erlebt - 3,55 mal mehr als die Gesamtheit der Befragten, die zwischen einer und mehr als 10 Datenpannen erlebt haben.

USD 5 Mio.

Prozesskosten aufgrund von Datenschutzverletzungen für die Hälfte der Befragten

Die Hälfte der Befragten, die sensible Inhalte mit 5.000 oder mehr externen Parteien austauschen, hat im letzten Jahr mehr als 5 Mio. USD für Gerichtsverfahren ausgegeben.

89%

gaben zu, dass sie die Compliance bei der Kommunikation sensibler Inhalte verbessern müssen

Nur 11 % der Befragten gaben an, dass sie keinen Verbesserungsbedarf bei der Messung und dem Management der Compliance für die Kommunikation sensibler Inhalte haben.

62%

wenden mehr als 1.500 Arbeitsstunden für die Erstellung von Compliance-Berichten auf

62 % der Unternehmen wenden jährlich mehr als 1.500 Stunden für die Zusammenstellung und den Abgleich von Protokollen der Kommunikationstools für Compliance-Berichte auf.

Einleitung

Willkommen zum dritten jährlichen Kiteworks-Bericht über die Kommunikation sensibler Inhalte! Für diesen Bericht haben wir eine detaillierte Umfrage durchgeführt, wie zuverlässig Unternehmen den Datenschutz und die Sicherheit ihrer sensiblen Inhalte gewährleisten und die Datenschutzbestimmungen und Sicherheitsstandards einhalten.

Wir verwenden den Begriff "sensible Inhalte", um diverse Inhalte zu beschreiben, die das Ziel krimineller Akteure sind und ein erhebliches Risiko für seriöse Unternehmen darstellen, wenn diese Inhalte in die Hände von Kriminellen gelangen. Es handelt sich um die Daten, die kompromittiert wurden, wenn der Begriff "Datenschutzverletzung" allzu oft in den Schlagzeilen auftaucht. Zu den sensiblen Inhalten gehören Kunden- und Mitarbeiterdaten, wie personenbezogene Daten, geschützte Patienteninformationen und Kreditkartendaten, das geistige Eigentum eines Unternehmens, rechtlich relevante Korrespondenz und Dokumente, Finanzdaten, Daten über Fusionen und Übernahmen sowie andere Arten privater und vertraulicher Informationen.

Sicherheitsrisiken

Das Sicherheitsproblem bei sensiblen Inhalten besteht darin, dass sie nicht an einem Ort bleiben. Während der täglichen Arbeit werden sie nicht nur zwischen Mitarbeitern ausgetauscht, sondern auch zwischen Mitarbeitern und Partnern, Lieferanten, Subunternehmern, Rechtsberatern, Buchhaltern, Wirtschaftsprüfern und vielen anderen. Damit Unternehmen erfolgreich sein können, müssen diese Informationen reibungslos zwischen dem Unternehmen und Tausenden von externen Parteien ausgetauscht werden. Wie wir sehen werden, geschieht dies über eine Vielzahl von Kommunikationskanälen.

Daher müssen Unternehmen ihre Inhalte nicht nur dort schützen, wo sie gespeichert sind, sondern auch auf dem Weg über die verschiedenen Kommunikationskanäle zu externen Parteien. Leider haben Cyberkriminelle in den letzten Jahren Schwachstellen in der Software-Lieferkette entdeckt, die ihnen Zugang zu Hunderten oder gar Tausenden von Unternehmen und Millionen sensibler Dateien verschaffen. Der diesjährige Data Breach Investigations Report (DBIR) von Verizon bestätigt diesen Trend. Er zeigt, dass die Zahl der ausgenutzten Software-Schwachstellen im Vergleich zum Vorjahr um 180 % gestiegen ist und dass die Zahl der Datenschutzverletzungen in der Software-Lieferkette im Vergleich zum Vorjahr um 68 % zugenommen hat - sie machen 15 % aller Datenschutzverletzungen aus.¹ Die Clop-Ransomware-Angriffe auf die Managed File Transfer (MFT)-Lösungen MOVEit² von Progress Software und GoAnywhere von Fortas³ im vergangenen Jahr verdeutlichen das Risiko.

KI-Cyber-Risiken

Neben dem Schutz der Kommunikationskanäle für Inhalte gibt es eine weitere Priorität für Unternehmen und Behörden, die in den letzten 18 Monaten an Dringlichkeit gewonnen hat. Da die künstliche Intelligenz (KI) sowohl im Hinblick auf den technischen Fortschritt als auch im Hinblick auf ihre öffentliche Nutzung explosionsartig zunimmt, ist es von entscheidender Bedeutung, dass sie ihre sensiblen Inhalte von den großen öffentlichen Sprachmodellen (LLMs) fernhalten, die nun möglicherweise routinemäßig von ihren Mitarbeitern und Partnern verwendet werden.

Laut Gartner sind die drei größten Risiken mit dem Einsatz von GenKI LLMs der Zugriff auf sensible Daten durch externe Parteien (laut fast der Hälfte der Cybersicherheitsbeauftragten), GenKI-Anwendungen und Datenverletzungen (laut 40 % der Befragten) sowie Fehlentscheidungen (laut mehr als einem Drittel der Befragten) verbunden.⁴ Das Risiko, dass Mitarbeiter sensible Daten in GenKI-Tools einstellen, ist real. In einer Ende 2023 durchgeführten Umfrage gab fast ein Drittel der Mitarbeiter zu, sensible Daten in öffentliche GenKI-Tools eingestellt zu haben. Es überrascht daher nicht, dass 39 % der Befragten in derselben Studie das potenzielle Abfließen sensibler Daten als Hauptrisiko für die Nutzung öffentlicher GenKI-Tools in ihrem Unternehmen nannten.⁵

Gleichzeitig führen die niedrigeren Einstiegshürden, die die Nutzung von KI für die breite Öffentlichkeit möglich gemacht haben, dazu, dass weniger versierte Cyberkriminelle immer komplexere Angriffe starten.⁶ Dies verstärkt das Gefühl, dass sich Schurkenstaaten und Cyberkriminelle in einem eskalierenden "Wettrüsten" mit seriösen Unternehmen befinden - mit möglicherweise existenziellen Auswirkungen.

Compliance-Risiken

Wenn Ihr Unternehmen nicht nur in einer einzigen Rechtssphäre tätig ist, besteht die Schwierigkeit bei der Einhaltung der Datenschutzvorschriften in der Vielzahl unterschiedlicher Anforderungen, die die Komplexität und die Kosten für die Einhaltung und Dokumentation dieser Anforderungen erhöhen. Die Zunahme neuer und die Weiterentwicklung bestehender Vorschriften haben 93 % der Unternehmen dazu veranlasst, ihre Cybersicherheitsstrategie im letzten Jahr zu überdenken.⁷ Die 2018 in Kraft getretene Datenschutz-Grundverordnung (DSGVO) der Europäischen Union hat die 27 EU-Mitgliedsstaaten unter einem einzigen Datenschutzstandard vereint.


Für den Rest der Welt sind die Dinge nicht so einfach. Daten der Vereinten Nationen zeigen, dass 137 der weltweit 194 Länder inzwischen über Datenschutzgesetze verfügen, die sehr unterschiedlich sind.⁸ In den USA ist das strengste Bundesgesetz der Health Insurance Portability and Accountability Act (HIPAA), der sich auf Patienteninformationen, nicht aber auf personenbezogene Daten bezieht. Da der US-Kongress keinen US-weiten Standard verabschieden konnte, haben die einzelnen US-Bundesstaaten die Initiative ergriffen, beginnend mit der Verabschiedung des California Consumer Privacy Act (CCPA) im Jahr 2018. Seitdem haben 17 weitere US-Bundesstaaten umfassende Datenschutzgesetze verabschiedet, und in 10 weiteren sind Gesetzgebungsverfahren im Gange.⁹ Es ist zwar gut, dass mehr US-Bürger und -Einwohner durch solche Gesetze geschützt werden, doch für diejenigen, die sie einhalten müssen, wird der gesetzliche Flickenteppich dadurch immer größer.

Die verschiedenen Datenschutzbehörden üben weiterhin Druck auf die Unternehmen aus, damit diese die Vorschriften einhalten. Die Bußgelder und Strafen für die Nichteinhaltung der DSGVO beliefen sich im Jahr 2023 auf 2,269 Mrd. USD (2,1 Mrd. EUR) und überstiegen damit die der Jahre 2019, 2020 und 2021 zusammen.¹⁰ Auch die Höhe der Geldbußen bewegt sich in einer Spirale nach oben: 4,75 Mio. USD (4,4 Mio. EUR) pro Verstoß im letzten Jahr, verglichen mit 540.000 USD (500.000 EUR) pro Verstoß im Jahr 2019. Ebenso erschreckend sind die Bußgelder und Strafen im Zusammenhang mit dem HIPAA, die sich im letzten Jahr auf 4,176 Mrd. USD beliefen.¹¹

Neben Datenschutzbestimmungen sind Cybersicherheitsstandards ein wichtiger Schwerpunkt für Regierungs- und Aufsichtsbehörden. Zu den wichtigsten neuen Cybersicherheitsvorschriften, die im vergangenen Jahr eingeführt wurden, gehören die SEC-Vorschriften zum Cyber Security Risk Management und zum Cyber Incident Reporting für börsennotierte Unternehmen, der Cyber Incident Reporting Act for Critical Infrastructure (CIRCA), der Cyber Resilience Act (CRA) und der Digital Operational Resilience Act (DORA) in Europa sowie das Cybersecurity Framework (CSF) 2.0 des National Institute of Standards & Technology (NIST).

Menschliche Risiken

Das mit menschlichem Fehlverhalten verbundene Risiko in Bezug auf Datensicherheit und Compliance ist nach wie vor ein ernstes Problem und die Ursache für viele Datenschutzverletzungen. Das DBIR hat festgestellt, dass die Benutzer für 68 % der Fehler verantwortlich sind, die zu Datenschutzverletzungen führen.¹² Dies geschieht auf verschiedene Weise, z. B. indem Mitarbeiter und externe Parteien sensible Informationen an falsche Empfänger senden, Daten nicht ordnungsgemäß sichern oder Opfer von Social-Engineering-Angriffen wie der Kompromittierung von Geschäfts-E-Mails und Phishing werden. Mangelnde Transparenz und Kontrolle über die Kommunikation sensibler Inhalte sind neben unzureichenden Sicherheitsinfrastrukturen und -kontrollen einer der Hauptfaktoren.

The image shows the black silhouettes of three people's heads and shoulders against a white background. They are positioned horizontally across the middle of the page.

**Fast die Hälfte der Verantwortlichen
für Cybersicherheit nennen den
Zugriff auf sensible Daten durch
externe Parteien als ihr größtes
Risikopotenzial in diesem Jahr.**

“2024 Gartner Technology Adoption Roadmap for Larger
Enterprises Survey,” Gartner, Februar 2024

Methodik für diese Studie

Der diesjährige Kiteworks-Bericht über die Kommunikation sensibler Inhalte basiert auf einer umfassenden Befragung von 572 Fachkräften aus den Bereichen IT, Cybersicherheit sowie Risiko- und Compliance-Management in Unternehmen mit mehr als 1.000 Mitarbeitern. Unsere Analyse berichtet über das Feedback der Befragten für die gesamte Kohorte, vergleicht es mit unseren Umfrageergebnissen aus den Jahren 2023 und 2022 und analysiert es nach verschiedenen demografischen Details.

Vielfalt der Befragten

Die Befragten kamen aus acht Ländern weltweit, wobei die Regionen Nordamerika (34 %), Asien-Pazifik (18 %) und EMEA (48 %) am stärksten vertreten waren. (Abb. 1 und 2). Sie repräsentieren ein breites Spektrum an Unternehmensgrößen: 54 % haben zwischen 1.000 und 10.000 Beschäftigte und 46 % noch mehr (Abb. 3).

Die Kohorte kommt aus einer Vielzahl von Branchen, wobei Unternehmen aus den Bereichen Sicherheit und Verteidigung (15 %), Fertigungsindustrie (12 %), Gesundheitswesen (12 %) und Finanzdienstleistungen (12 %) am stärksten vertreten sind (Abb. 4). Mehr als zwei von zehn Befragten (22 %) arbeiten in der öffentlichen Verwaltung oder im Bildungswesen, ein Viertel im Finanz-, Rechts- und Dienstleistungssektor und 10 % im Energiesektor.

Hinsichtlich der beruflichen Funktion umfasst die Gruppe der Befragten Fachleute auf verschiedenen Ebenen in ihren Unternehmen, wobei 31 % in Führungspositionen und 69 % im mittleren Management tätig sind (Abb. 5). Sie verteilen sich auf die Bereiche Risiko und Compliance (27 %), IT (42 %) und Sicherheit (31 %).

75%

der Weltbevölkerung werden ihre persönlichen Daten bis Ende 2024 durch moderne Datenschutzgesetze geregelt haben.

“Gartner Identifies Top Five Trends in Privacy Through 2024,” Gartner Pressemitteilung, 31. Mai 2022

Insights zu Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

Nachdem wir unsere Befragten vorgestellt haben, möchten wir an dieser Stelle aufzeigen, welche Erkenntnisse wir in diesem Jahr aus den Umfrageergebnissen zu den Themen Messung und Management der Risiken von Cyberangriffen und Datenschutzverletzungen, Datentypen und -klassifizierung, Cybersicherheit, Compliance sowie operative Prozesse gewinnen konnten.

CYBERANGRIFFE UND DATENSCHUTZVERLETZUNGEN

Insight: Die Kommunikation sensibler Inhalte wird zu häufig angegriffen

Böswillige Cyberangriffe stellen nach wie vor eine ernste Bedrohung für sensible Inhalte in allen Branchen dar. So verzeichnete das Identify Theft Resource Center im vergangenen Jahr 3.205 öffentlich gemeldete Datenkompromittierungen, von denen schätzungsweise 353 Millionen Menschen betroffen waren – ein Anstieg um 78 % gegenüber 2022.¹³ Die gute Nachricht ist, dass die Situation für unsere Befragten aus dem Jahr 2024 etwas besser ist als für unsere Kohorte aus dem Jahr 2023. Die schlechte Nachricht ist, dass Unternehmen immer noch häufig von gefährlichen Sicherheitsverletzungen betroffen sind. Fast ein Drittel der Befragten (32 %) gab an, im vergangenen Jahr *sieben oder mehr* böswillige externe Hackerangriffe auf sensible Inhalte erlebt zu haben, verglichen mit 36 % im Vorjahr (Abb. 6). Obwohl mehr Unternehmen (36 %) als im letzten Jahr drei oder weniger Sicherheitsverletzungen meldeten, sind selbst diese Zahlen nicht gerade ideal.

Die Anzahl der Hackerangriffe variiert stark nach Branche ([Abb. 7](#)). In den Bereichen Hochschulwesen, Sicherheit und Verteidigung sowie Öl und Gas waren noch mehr Sicherheitsvorfälle zu verzeichnen - 68% der Befragten gaben vier oder mehr Sicherheitsverletzungen an, verglichen mit 55 % in der Gesamtkohorte. Besorgniserregende Daten lieferte auch der *Sektor der Regierungsbehörden*: 17 % der Befragten gaben an, 10 oder mehr Sicherheitsverletzungen zu verzeichnen, weitere 10 % meldeten 7 bis 9 Sicherheitsverletzungen. Noch alarmierender ist, dass 42% der *Unternehmen im Bereich Sicherheit und Verteidigung*, die mit den sensibelsten Inhalten aller Branchen arbeiten, sieben oder mehr Sicherheitsverletzungen zugaben. Pharma- und Life-Sciences-Unternehmen stehen demgegenüber deutlich besser da: Nur 28 % der Befragten berichteten von vier oder mehr Datenschutzverletzungen.

Unternehmen im asiatisch-pazifischen Raum waren ebenfalls überproportional von Sicherheitsverletzungen betroffen. 72 % der Befragten berichteten von vier oder mehr Vorfällen ([Abb. 8](#)). Da Unternehmen im asiatisch-pazifischen Raum eine höhere Anzahl an externen Parteien haben, mit denen sie sensible Inhalte austauschen (siehe unten), ist es wahrscheinlich, dass weitere Untersuchungen einen Zusammenhang zwischen diesen beiden Problemen aufzeigen werden. Schließlich schnitten Unternehmen mit 20.001 bis 30.000 Mitarbeitern deutlich schlechter ab als andere Unternehmen. Hier meldeten 75 % oder mehr Unternehmen vier oder mehr Datenschutzverletzungen, während der entsprechende Anteil sowohl bei den kleineren als auch bei den größeren Unternehmen deutlich unter 60 % lag ([Abb. 9](#)).

42%

der **Unternehmen im Bereich Sicherheit und Verteidigung** meldeten für das vergangene Jahr **mehr als sieben Datenschutzverletzungen**.



68%

der **Unternehmen im asiatisch-pazifischen Raum** gaben an, im vergangenen Jahr von **mehr als vier Datenpannen** betroffen gewesen zu sein.



32%

der Unternehmen
erlebten im letzten
Jahr **mehr als
sieben externe
Hackerangriffe** auf
sensible Inhalte.

Prozesskosten bei Datenschutzverletzungen

Die Kosten von Datenschutzverletzungen können erheblich sein und umfassen Geldbußen und Strafen für die Nichteinhaltung von Vorschriften, Betriebsunterbrechungen, Produktivitätsverluste und Umsatzeinbußen. Der jährliche Bericht von IBM und dem Ponemon Institute über die Kosten von Datenschutzverletzungen aus dem letzten Jahr beziffert die Kosten einer Datenschutzverletzung auf *4,45 Mio. USD* - eine Zahl, die von Jahr zu Jahr weiter steigt.¹⁴ Und diese Zahl könnte sogar noch zu niedrig sein, da die mit Datenschutzverstößen verbundenen Prozesskosten oft übersehen oder unterschätzt werden. Vor diesem Hintergrund haben wir unsere Umfrage in diesem Jahr um die Frage nach den Kosten für Rechtsstreitigkeiten erweitert - mit interessanten Ergebnissen.

Sechs von zehn Befragten gaben an, dass sie jährlich **mehr als 2 Mio. USD** für Prozesskosten im Zusammenhang mit internen und externen Datenverlusten ausgeben, während 45 % mehr als 3 Mio. USD und ein Viertel **mehr als 5 Mio. USD** ausgeben ([Abb. 10](#)). Je größer das Unternehmen, desto höher die Kosten für Rechtsstreitigkeiten: 39 % der Unternehmen mit mehr als 30.001 Beschäftigten gaben an, dass ihre Rechtskosten mehr als 7 Mio. USD betragen (17 % mit 7 bis 9 Mio. USD und 22 % mit mehr als 10 Mio. USD), und weit über die Hälfte der Unternehmen mit mehr als 15.001 Beschäftigten gaben mehr als 3 Mio. USD aus ([Abb. 11](#)). Der am stärksten betroffene Wirtschaftszweig war der *Hochschulsektor*, in dem 49 % der Befragten angaben, im vergangenen Jahr mehr als 5 Mio. USD ausgegeben zu haben ([Abb. 12](#)). Geografisch gesehen führt *Nordamerika* die Liste an, wo 27 % der Befragten angaben, mehr als 5 Mio. USD ausgegeben zu haben. Eine beunruhigende Feststellung in dem Bericht ist die Tatsache, dass 14 % der Befragten aus der EMEA-Region die Kosten für Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen nicht kennen ([Abb. 13](#)).



24%

der Unternehmen mit über 30.001 Mitarbeitern meldeten, **jährlich mehr als 7 Mio. USD an Prozesskosten für Datenschutzverstöße bezahlt zu haben.**

45%

der Befragten gaben an, **dass die Kosten für Rechtsstreitigkeiten 3 Mio. USD pro Jahr übersteigen, ein Viertel davon bezahlte mehr als 5 Mio. USD.**



DATENTYPEN UND KLASSIFIZIERUNG

Insight: Keine Verfolgung und Kontrolle des gesamten Datenaustauschs

Das ohnehin schon exponentielle Datenwachstum hat sich in den letzten 18 Monaten mit der Einführung der GenKI LLMs (Large Language Models) weiter beschleunigt. Wenn Inhalte eine Anwendung wie E-Mail, File Sharing, SFTP, Managed File Transfer Protocol oder Webformulare verlassen, ist es wichtig, dass Unternehmen den Zugriff auf diese Inhalte verfolgen und kontrollieren können.

Unternehmen müssen wissen, welche Arten von Daten sie haben, wo sie gespeichert sind und wohin sie gesendet und übertragen werden. Um festzustellen, welche unstrukturierten Daten kontrolliert werden müssen, ist ein Klassifizierungssystem erforderlich. Auf die Frage, wie viele ihrer unstrukturierten Daten gekennzeichnet oder klassifiziert sind, gaben *weniger als die Hälfte* der Befragten (48 %) an, dass dies bei 75 % oder mehr ihrer Daten der Fall ist (Abb. 14). Innerhalb der Branchen erreichten 65 % dieses Niveau im Gesundheitswesen, 56 % bei den Finanzdienstleistungen und 55 % im Rechtswesen (Abb. 15).

Die Unternehmen gaben jedoch an, dass nicht alle unstrukturierten Daten gekennzeichnet und klassifiziert werden müssen. 40 % der Unternehmen gaben an, dass 60 % oder mehr der unstrukturierten Daten gekennzeichnet und klassifiziert werden müssen. Je größer ein Unternehmen ist, desto mehr unstrukturierte Daten müssen mit Tags versehen und klassifiziert werden. Dies gilt z. B. für Unternehmen mit mehr als 30.001 Mitarbeitern: 15 % gaben an, dass alle Daten getaggt und klassifiziert werden müssen und weitere 20 % gaben an, dass mehr als 80% der Daten mit Tags versehen und klassifiziert werden müssen ([Abb. 16](#)). Die nordamerikanischen Befragten gaben regional gesehen häufiger an, dass die Daten getaggt und klassifiziert werden müssen. 10 % gaben an, dass alle unstrukturierten Daten gekennzeichnet und klassifiziert werden müssen, und weitere 16 % gaben an, dass 80 % oder mehr der unstrukturierten Daten gekennzeichnet und klassifiziert werden müssen ([Abb. 17](#)). Die meisten Befragten aus Regierungsbehörden gaben an, dass alle Daten gekennzeichnet und klassifiziert werden müssen (24 %), wobei 17 % angaben, dass 80 % oder mehr der Daten gekennzeichnet und klassifiziert werden müssen ([Abb. 18](#)).

40%

der Unternehmen gaben an, dass **mehr als 60 % der unstrukturierten Daten gekennzeichnet und klassifiziert** werden müssen.

Nur **49 %** der Unternehmen meinten, dass mehr als **75 % ihrer unstrukturierten Daten gekennzeichnet und klassifiziert** werden müssen.



CONFIDENTIAL DOCUMENT



TOP SECRET

Bewertung der Risiken einzelner Datentypen

Wie bereits beschrieben, sind sensible Inhalte in den Unternehmen in unterschiedlicher Form vorhanden. Das Risiko einer Datenschutzverletzung ist nicht für alle gleich hoch. Laut der IBM-Studie über die jährlichen Kosten von Datenschutzverletzungen sind *personenbezogene Daten* die kostspieligste und am stärksten gefährdete Datenkategorie. Im Jahr 2023 waren personenbezogene Daten mit 52 % aller Datenschutzverletzungen auch die am häufigsten verletzte Datenkategorie, wie bereits in den beiden Vorjahren.¹⁵ Die Ergebnisse von IBM stimmen mit denen des jüngsten DBIR überein, wonach 50 % aller Datenschutzverletzungen personenbezogene Daten betreffen.

Vergleicht man diese Daten mit den Einstufungen der Befragten, ergeben sich Diskrepanzen. Basierend auf den Forschungsdaten von IBM und Verizon würde man beispielsweise erwarten, dass die Befragten persönliche Daten als wichtigstes inhaltsbezogenes Anliegen nennen würden. Dies war jedoch nicht der Fall. Stattdessen nannten die Befragten *Finanzdokumente* (55 %), *geistiges Eigentum* (44 %) und *juristische Korrespondenz* (44 %) als ihre drei wichtigsten Anliegen ([Abb. 19](#)).

41 % der Befragten aus Regierungsbehörden gaben an, dass **80 % oder mehr** ihrer **unstrukturierten Daten gekennzeichnet und klassifiziert** werden müssen.



Eine gewisse Bestätigung der Daten von IBM und Verizon fand sich in unserer Cross-Analyse von *Patientendaten*, bei der diejenigen, die Patientendaten als eine der drei wichtigsten Datenkategorien nannten, eine höhere Rate an bösartigen Datenschutzverletzungen aufwiesen als diejenigen, die andere Datenkategorien angaben. So gaben 43 % derjenigen, die Patienteninformationen zu den drei wichtigsten Datenarten zählten, an, *mehr als sieben* Datenschutzverletzungen erlebt zu haben (im Vergleich zu 32 % aller Befragten, die von sieben oder mehr Datenschutzverletzungen berichteten) ([Abb. 20](#)). Die am zweithäufigsten von Datenpannen betroffene Datenkategorie war *geistiges Eigentum* (35 % gaben an, von mehr als sieben Datenpannen betroffen gewesen zu sein).

Auffallend ist, dass die Hälfte der nordamerikanischen Befragten GenKI LLMs (Large Language Models) als eines der drei wichtigsten Anliegen nannten, nur knapp hinter Finanzdokumenten ([Abb. 21](#)). Nach Wirtschaftszweigen sind LLMs besonders wichtig in der Öl- und Gasindustrie (62 %), in der pharmazeutischen Industrie (61 %), in Regierungs- (61 %) und Landesbehörden (58 %) sowie in Anwaltskanzleien (58 %).

Es gibt erhebliche Unterschiede zwischen den verschiedenen Datentypen und Branchen in Bezug auf das **höchste Risiko**:



Befragte aus den Bereichen **Energie und Versorgung** sowie **Sicherheit und Verteidigung** nannten häufig **GenKI LLMs** (50%).



Personenbezogene Daten wurden mit 50 % am häufigsten von Unternehmen aus dem **Hochschulwesen** genannt.



Patientendaten wurden am häufigsten von Befragten aus dem **Gesundheitswesen** genannt (58 %).



CUI und FCI wurden aus der **Fertigungsindustrie** mit 79 % am häufigsten genannt.



Juristische Korrespondenz wurde am häufigsten von **Öl- und Gasunternehmen** (62 %) und **Regierungsbehörden** angeführt (61 %).



Details zu Fusionen und **Übernahmen (M&A)** wurden am häufigsten von **Pharma- und Life Sciences-Unternehmen** genannt (40 %).



Diejenigen, die **Patienteninformationen** zu den **drei wichtigsten Datenkategorien** zählten, erlebten häufiger **böswillig verursachte Datenschutzverletzungen** als die Befragten, die andere Datenarten nannten.



COMPLIANCE UND RISIKO- MANAGEMENT

Insight: Compliance und Risikomanagement haben höchste Priorität

Inzwischen scheint das Cybersicherheitsrisiko von Jahr zu Jahr einen größeren Teil des gesamten Risikoportfolios eines Unternehmens ausmacht.

CrowdStrike stellte in seinem jährlichen Gefahrenbericht fest, dass die Zahl der auf eCrime-Websites genannten Opfer im Vergleich zum Vorjahr um 76 % gestiegen ist.¹⁶ In seinem jüngsten DBIR hat Verizon über 30.000 reale Sicherheitsvorfälle analysiert und bestätigt, dass etwa ein Drittel (10.626) Datenschutzverletzungen waren.¹⁷

Da sensible Daten im Mittelpunkt der meisten Datenschutzverstöße stehen, haben Regierungsbehörden und Branchenverbände mit einer Reihe neuer Vorschriften und Standards sowie einer Verschärfung bestehender Vorschriften reagiert. All dies führt zu einem geografischen Flickenteppich, der die Reaktion auf Vorfälle sowie die Audits und Berichte zur Einhaltung der Vorschriften noch komplizierter macht, insbesondere für globale Unternehmen.

Wie in den Vorjahren berichteten die 2024 Befragten von anhaltenden Schwierigkeiten im Bereich Compliance und Risikomanagement. Dies geht aus den Antworten der Befragten auf die zentrale Frage hervor, wie gut ihre Unternehmen das Compliance-Risiko bei der Kommunikation sensibler Inhalte managen (Abb. 22). Nur 11 % gaben an, dass in diesem Bereich keine Verbesserungen erforderlich sind – deutlich weniger als bei den Kohorten 2022 und 2023. Die gute Nachricht ist, dass weniger Befragte (32 %) angeben, dass erhebliche Verbesserungen erforderlich sind.



Die regionalen Unterschiede bei dieser Frage sind gering, aber die Unternehmensgröße spielt eine Rolle. Insbesondere größere Unternehmen sind eher der Ansicht, dass erhebliche Verbesserungen erforderlich sind ([Abb. 23](#)), wobei ein Drittel oder mehr der Unternehmen in jeder Gruppe mit mehr als 15.001 Beschäftigten diese Antwort geben. Dennoch gibt es einige Unterschiede in der Zuversicht hinsichtlich der Einhaltung der gesetzlichen Vorschriften. 29 % der befragten französischen Unternehmen sind der Meinung, dass *keine Verbesserungen* notwendig sind, ein deutlich höherer Prozentsatz als in anderen Ländern - z. B. 5 % in Deutschland, 10 % im Vereinigten Königreich und 13 % in Saudi-Arabien und den VAE ([Abb. 24](#)). Interessant und vielleicht beunruhigend ist, dass 41 % der Befragten aus Regierungsbehörden angaben, dass bei der Verwaltung und Messung der Compliance in Bezug auf die Kommunikation sensibler Inhalte erheblicher Verbesserungsbedarf besteht, mehr als in jedem anderen Wirtschaftszweig (der nächsthöhere Wert liegt im Dienstleistungssektor mit 36 %) ([Abb. 25](#)).

Nur

11 %

der Unternehmen erklärten, dass **keine Verbesserungen** bei der Messung und dem Management der Compliance bei der Kommunikation sensibler Inhalte **erforderlich** seien.





Vorrangige Bereiche für gesetzliche Bestimmungen

Weltweit tätige Unternehmen müssen eine Vielzahl von Datenschutzbestimmungen und Sicherheitsstandards beachten. Bis heute wurden weltweit über 160 Datenschutzgesetze erlassen, und die Zahl steigt weiter. Die Nichteinhaltung dieser Gesetze führt zu Imageschäden, Umsatzeinbußen, Bußgeldern und laufenden Prozesskosten. Infolgedessen gaben 37 % der Befragten im diesjährigen ISACA-Datenschutzbericht an, dass sie nur einigermaßen zuversichtlich sind, und weitere 13 % gaben an, dass sie weniger oder überhaupt nicht zuversichtlich sind, Datenschutz gewährleisten und die Einhaltung neuer Datenschutzgesetze und -vorschriften sicherstellen zu können.¹⁸

Bei der Frage nach den beiden wichtigsten Bereichen, auf die sich die Befragten in Bezug auf Datenschutz und Compliance konzentrieren, dominierten zwei Wahlmöglichkeiten: die Datenschutzgrundverordnung (DSGVO) der EU und die Datenschutzgesetze einzelner US-Bundesstaaten wie der California Consumer Privacy Act (CCPA). Beide wurden von 41 % der Befragten genannt ([Abb. 26](#)).

Es überrascht nicht, dass die DSGVO in der EMEA-Region viel häufiger genannt wurde (57 %), während die Gesetze der US-Bundesstaaten von 63 % der nordamerikanischen Befragten genannt wurden ([Abb. 27](#)). Was die verschiedenen Verantwortungsbereiche betrifft, so messen die Verantwortlichen der Risiko- und Compliance-Abteilungen (52 %) der DSGVO eine größere Bedeutung bei als die Verantwortlichen der IT-Abteilungen (38 %) und der Cybersicherheitsabteilungen (33 %) ([Abb. 28](#)). IT-Manager messen den Datenschutzgesetzen der US-Bundesstaaten (52 %) im Vergleich zu Risiko- und Compliance-Managern (25 %) und Cybersicherheits-Managern (40 %) die größte Bedeutung bei. Gleichzeitig messen Cybersicherheitsbeauftragte (35 %) dem CMMC 2.0 mehr Bedeutung bei als IT- (22 %) und Risikomanagement-Verantwortliche (18 %). HIPAA – ein US-spezifisches Gesetz – wurde von 38 % der nordamerikanischen Befragten genannt, ironischerweise aber von einem höheren Prozentsatz (43 %) der Befragten im asiatisch-pazifischen Raum.

Betrachtet man die Einhaltung der Vorschriften aus der Sicht der Industrie, so gibt es einige besorgniserregende Risikolücken. Beispielsweise gaben nur 38 % der Auftragnehmer im Bereich Sicherheit und Verteidigung an, dass die Einhaltung der CMMC-Vorschriften eine ihrer beiden höchsten Prioritäten ist. Da CMMC 2.0 nun schrittweise eingeführt wird, scheint dies ein ernsthaftes Risiko zu sein – nämlich, dass Sicherheits- und Verteidigungsunternehmen und Subunternehmer, die die Vorschriften nicht einhalten, Aufträge vom DoD verlieren.



US DATA
PRIVACY
LAWS



DSGVO
Europäische Union

Die **beiden wichtigsten** von den Befragten genannten **gesetzlichen Vorgaben**, waren die **DSGVO** und die **neuen US-Datenschutzgesetze** (bisher 18 verabschiedet).



Schwerpunktbereiche für Validierungen und Zertifizierungen

Was die Validierung und Zertifizierung im Gegensatz zu den Vorschriften betrifft, so wurden zwei Standards am häufigsten unter den beiden höchsten Prioritäten der Befragten genannt ([Abb. 29](#)): die von der Internationalen Organisation für Normung (ISO; 53 %) und die vom National Institute of Standards and Technology (NIST 800-171; 42 %) veröffentlichten Standards. Da die 110 Kontrollen von NIST 800-171 mit denen des CMMC 2.0 Level 2 übereinstimmen, ist diese hohe Priorisierung vielversprechend, insbesondere im Hinblick auf die schrittweise Einführung von CMMC 2.0, die derzeit im Gange ist. ISO 27001, 27017 und 27018 wurden in allen Regionen und in den meisten Branchen am häufigsten genannt, darunter 59 % in der EMEA-Region, 67 % in der Pharmaindustrie und 69 % in der Kommunalverwaltung ([Abb. 30](#) und [31](#)).

59%

der Befragten in der EMEA-Region nannten **ISO 27001, 27017 und 27018** als eine der **beiden wichtigsten Sicherheitsvalidierungen und -zertifizierungen** (19 % mehr als in der Asien-Pazifik-Region und 22 % mehr als in Nordamerika).

ISO 27018

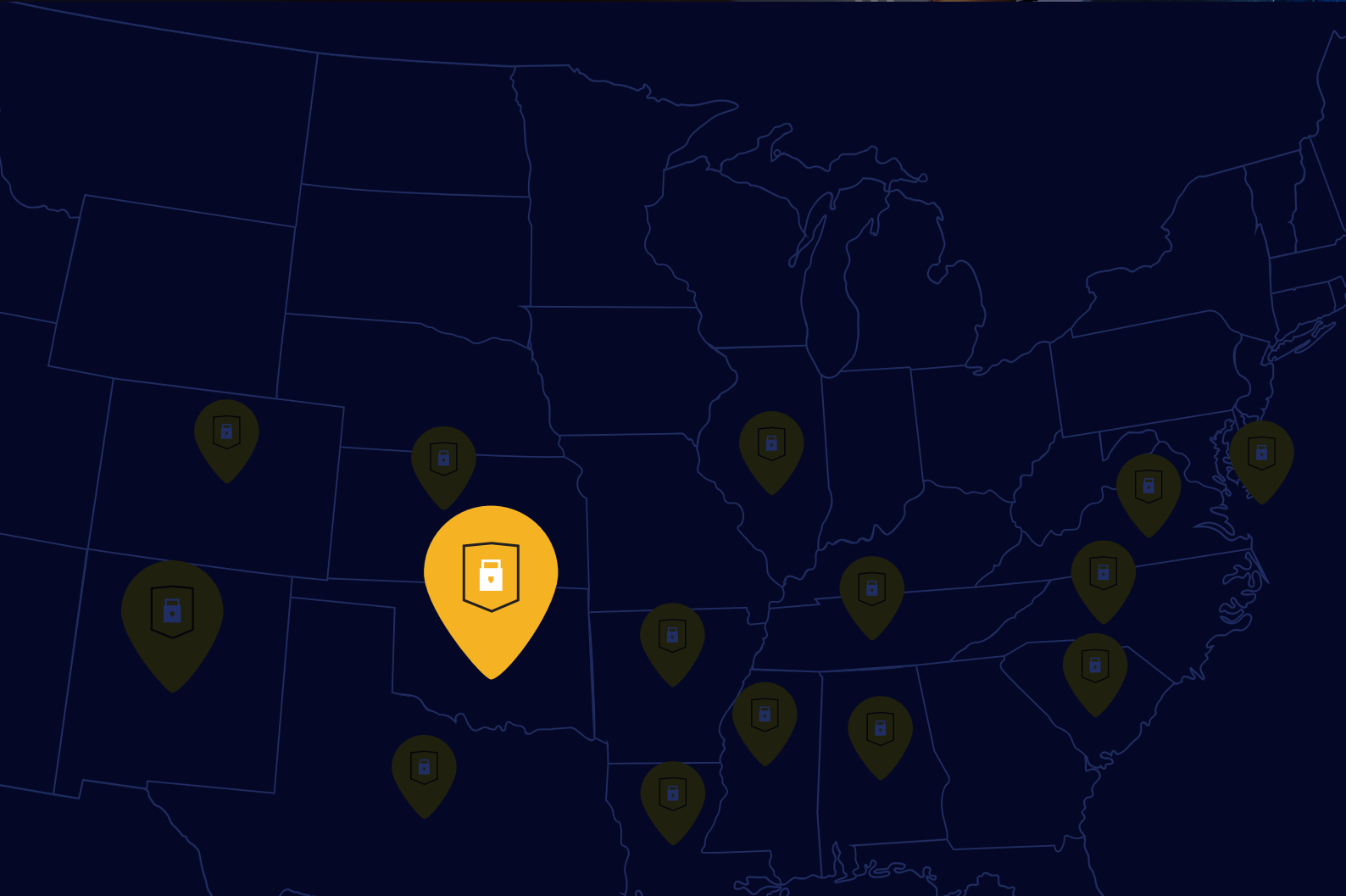
ISO 27017

ISO 27018

ISO 27001

ISO 27001





63%

der nordamerikanischen Befragten nannten die **Datenschutzgesetze der US-Bundesstaaten** als eines der beiden größten Compliance-Probleme.

Nur **38 %** der Sicherheits- und Verteidigungsunternehmen nannten **CMMC 2.0** als eines ihrer beiden größten Probleme bei der Einhaltung der Vorschriften.



Da ein beträchtlicher Anteil der Befragten im asiatisch-pazifischen Raum aus Australien stammt, ist es logisch, dass das Information Security Registered Assessors Program (IRAP) von mehr Unternehmen im asiatisch-pazifischen Raum als in den beiden anderen Regionen gewählt wurde (45 %). Interessanterweise wurde die NIS 2-Richtlinie nur von 20 % der Unternehmen in der EMEA-Region als erste oder zweite Priorität genannt (jedoch mehr als in Nordamerika mit 8 % und im asiatisch-pazifischen Raum mit 4 %). Man könnte annehmen, dass die Einhaltung der NIS 2-Richtlinie angesichts der Frist für die Umsetzung der Richtlinie in nationales Recht am 17. Oktober 2024 eine höhere Priorität hätte. In unseren drei Haupttätigkeitsbereichen wurde NIS 2 am wenigsten von Risiko- und Compliance-Verantwortlichen (19 %) im Vergleich zu den Verantwortlichen für IT (31 %) und Cybersicherheit (33 %) berücksichtigt. Nordamerikanische Unternehmen haben sich häufiger als andere Regionen für die Einhaltung von SOC 2 Type II entschieden (41 %).

Nach Branchen wurde SOC 2 Type II am häufigsten von Dienstleistungsunternehmen gewählt (47 %). ISO 27001, 27017 und 27018 wurden am häufigsten von Pharma- und Life Science-Unternehmen gewählt (67 %). Unternehmen aus dem Bereich Sicherheit und Verteidigung waren mit 44 % Spitzenreiter bei FedRAMP Moderate. Unternehmen aus dem Rechtswesen wählten am häufigsten IRAP (50 %).

ISO 27018 ISO 27017 ISO 27018 ISO 27017
ISO 27018 ISO 27001 ISO 27018 ISO 27018

ISO 27001, 27017, und 27018 wurden von den Befragten am häufigsten als wichtigste Cybersicherheitsstandards genannt.

ISO 27001 Standard

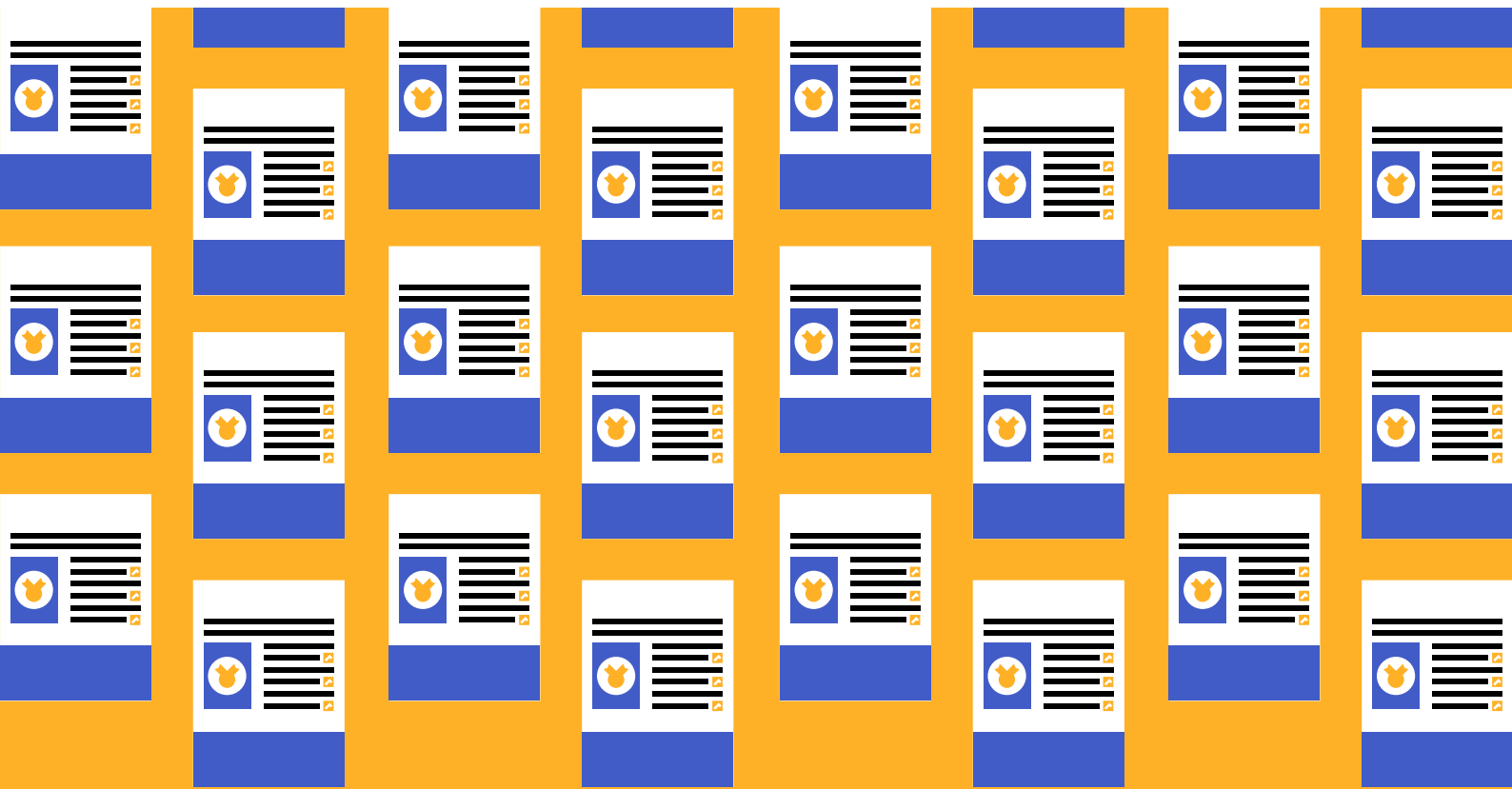


CERTIFIED



Herausforderungen beim Compliance-Reporting

Unabhängig von den spezifischen Vorschriften, Validierungen und Zertifizierungen, die ein Unternehmen einhalten muss, bleibt die Dokumentation der Compliance eine große Herausforderung. Unternehmen kämpfen mit dem externen Versand und der Weitergabe sensibler Daten. 57 % geben an, dass sie den Austausch nicht nachverfolgen, kontrollieren und dokumentieren können (Abb. 32). Ein Grund dafür ist die Vielzahl der Anforderungen, mit denen die Unternehmen konfrontiert sind, was zu Komplexität führt und erhebliche personelle und zeitliche Ressourcen in Anspruch nimmt. Auf die Frage, wie oft sie detaillierte Audit-Protokolle für Compliance-Berichte erstellen müssen, gaben 72 % der Befragten an, dass sie dies fünfmal oder öfter pro Jahr tun müssen (Abb. 33). Bei mehr als einem Drittel der Befragten (34 %) ist dies achtmal oder öfter der Fall.



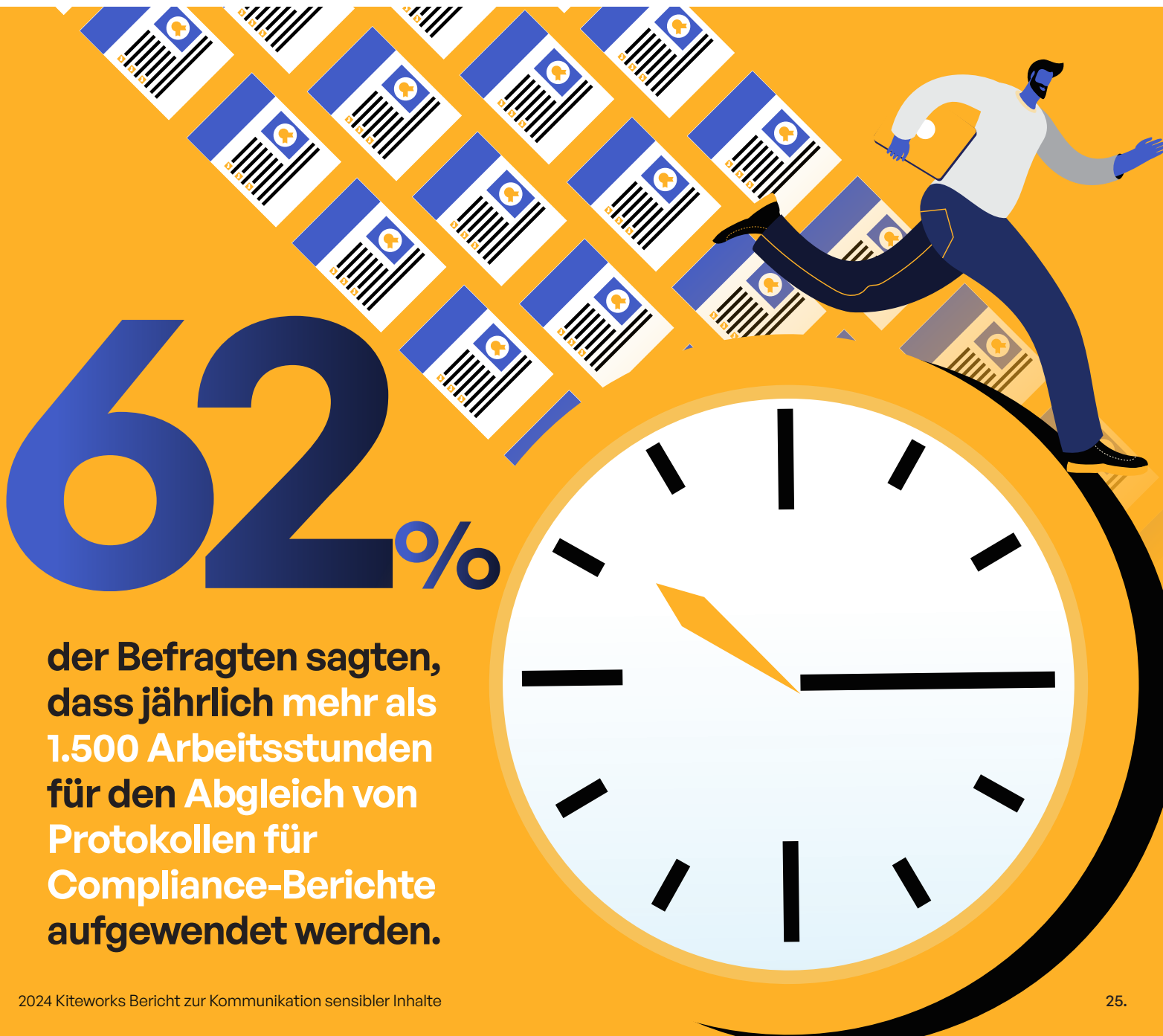
89%

der Unternehmen
müssen acht oder
mehr detaillierte
Compliance-Berichte
jährlich erstellen.



Die Unterschiede zwischen den Regionen und den Unternehmensgrößen waren bei dieser Frage nicht sehr groß ([Abb. 34](#) und [35](#)). Nordamerikanische Unternehmen und kleinere Unternehmen haben tendenziell etwas weniger Protokolle. Unternehmen mit mehr als 30.001 Mitarbeitern haben mehr Audit-Protokolle (19 % haben 9) als andere Unternehmensgrößen. Die Branchen mit der höchsten Anzahl an Audit-Protokollen pro Jahr sind Dienstleistungen, Sicherheit und Verteidigung sowie Regierungsbehörden mit 78 %, 77 % bzw. 72 %. Die geringste Anzahl an Audit-Protokollen haben Rechtswesen/Anwaltskanzleien mit 15 % oder weniger, die fünf Protokolle oder mehr haben ([Abb. 36](#)).

Die Compliance-Berichte erfordern einen hohen Zeitaufwand der Mitarbeiter, da immer wieder detaillierte Protokolle in die Berichte eingefügt werden müssen. Von allen Befragten gaben 63 % an, dass *mehr als 1.500 Arbeitsstunden* pro Jahr für diese Aufgabe benötigt werden ([Abb. 37](#)). Bei Unternehmen mit mehr als 15.001 Mitarbeitern steigt die Stundenzahl deutlich an. Ein Drittel der Unternehmen mit mehr als 30.001 Beschäftigten gibt an, mehr als 2.500 Stunden zu investieren ([Abb. 38](#)). Die Hälfte der Befragten aus dem Öl- und Gassektor und fast die Hälfte der Befragten aus dem Hochschulsektor wenden mehr als 2.000 Stunden pro Jahr auf - die mit Abstand höchsten Werte aller Branchen ([Abb. 39](#)).



CYBERSICHERHEIT UND RISIKO- MANAGEMENT

Insight: Der Schutz der Kommunikation sensibler Inhalte bleibt eine große Herausforderung

Für die Sicherheitsteams stehen sensible Inhalte im Mittelpunkt dessen, was sie in den IT-Systemen ihrer Unternehmen schützen müssen. Die Teilnehmer unserer Umfrage im Jahr 2024 geben deutlich seltener an, dass ihr Content Security Management nicht verbessert werden muss, als ihre Kollegen im Jahr 2023 (Abb. 40). In diesem Jahr sind es nur noch 11 %, aber auch der Anteil derer, die eine deutliche Verbesserung für notwendig halten, ist zurückgegangen. Es bleibt also mehr als die Hälfte (56 %), die eine gewisse Verbesserung für notwendig halten. Vielleicht können wir uns damit trösten, dass die Unternehmen zwar Fortschritte machen, aber gleichzeitig realistischer sind, was die Notwendigkeit weiterer Verbesserungen angeht.

Diese Prozentsätze waren jedoch in den verschiedenen Gruppen nicht einheitlich. 30 % oder mehr der Befragten in Saudi-Arabien, den Vereinigten Arabischen Emiraten, Nordamerika und im asiatisch-pazifischen Raum gaben an, dass erhebliche Verbesserungen erforderlich sind (Abb. 41). Gleiches gilt für Dienstleistungen (47 %), Finanzdienstleistungen (43 %), Öl und Gas (42 %), Regierungsbehörden (41 %), Fertigungsindustrie (36 %) und das Gesundheitswesen (34 %) (Abb. 42 und 43).

56%

der Befragten gaben an, dass die **Messung und das Management der Sicherheit der Kommunikation sensibler Inhalte** im Jahr 2024 verbessert werden muss (gegenüber 37 % im Jahr 2023).



Fortschritte in Richtung Zero Trust

Zero Trust in Unternehmen spiegelt eine signifikante Akzeptanz und Integration über verschiedene Sicherheitsebenen hinweg wider. Zero-Trust-Prinzipien auf Netzwerkebene werden durch Mikrosegmentierung und strenge Zugangskontrollen durchgesetzt, um die laterale Ausbreitung von Bedrohungen zu minimieren. Endgerätesicherheit im Rahmen von Zero Trust beinhaltet die Installation von Advanced Threat Protections und Endpoint Detection and Response (EDR), um sicherzustellen, dass alle Geräte, die auf das Netzwerk zugreifen, kontinuierlich authentifiziert und überwacht werden. Für das Identitäts- und Zugriffsmanagement sind die Multi-Faktor-Authentifizierung (MFA) und das Privileged Access Management (PAM) wichtige Komponenten, die sicherstellen, dass der Zugriff der Anwender streng kontrolliert und kontinuierlich überprüft wird. Auf der Inhaltsebene setzen Unternehmen Datenverschlüsselung und Echtzeitüberwachung ein, um sensible Informationen zu schützen. Obwohl Unternehmen Zero Trust eine hohe Priorität einräumen, berichtet fast die Hälfte (48 %) von Schwierigkeiten bei der Integration von Zero Trust in On-Premises- und Cloud-Umgebungen.¹⁹

Unser Interesse für diesen Bericht konzentriert sich natürlich auf die Ebene der Sicherheit von Inhalten ([Abb. 44](#)). Unsere erste Beobachtung ist der bedauerliche Anteil von 45 % der Unternehmen, die *noch kein* Zero Trust für Content Security erreicht haben. Zweitens gibt es einige demografische Regionen, in denen die Ergebnisse noch schlechter sind. Nur 35 % der Befragten im Vereinigten Königreich und 39 % im Nahen Osten und im asiatisch-pazifischen Raum haben dieses Ziel erreicht ([Abb. 45](#)). Nach Branchen betrachtet, liegen die Landesbehörden (21 %), die Öl- und Gasindustrie (33 %) und die Pharma- und Life-Sciences-Branche (39 %) beim Zero-Trust-Schutz von Inhalten zurück ([Abb. 46](#)).



Mehr Sicherheit für den Schutz sensibler Inhalte

Von den Unternehmen, die angaben, keine erweiterten Sicherheitsfunktionen für die Kommunikation sensibler Inhalte zu verwenden, gab ein wesentlich höherer Prozentsatz (36 %) an, nicht zu wissen, wie viele Datenschutzverletzungen ihr Unternehmen zu beklagen hatte, als von den Unternehmen, die angaben, erweiterte Sicherheitsfunktionen für einige oder alle Inhalte zu verwenden (jeweils 8 %) ([Abb. 47](#)). Dies deutet auf eine erhebliche Risikolücke hin. Über alle Branchensegmente hinweg zeigen die Ergebnisse, dass die größten Herausforderungen im Rechtswesen (55 % nutzen sie teilweise oder gar nicht), in der Kommunalverwaltung (50 %), in den Regierungsbehörden (48 %) und im Gesundheitswesen (44 %) bestehen. Dies steht im Gegensatz zu den 41 % der globalen Kohorte, die dies tun. Zu den Sektoren mit den besten Ergebnissen gehören Dienstleistungen (71 % nutzen sie immer), die Landesbehörden (71 %) und das Hochschulwesen (65 %) ([Abb. 48](#)).



Nachverfolgung, Klassifizierung und Kontrolle des Zugriffs auf sensible Inhalte

Wenn Inhalte eine Anwendung wie E-Mail, File Sharing, SFTP, Managed File Transfer Protocol oder Webformulare verlassen, ist es wichtig, dass Unternehmen den Zugriff auf diese Inhalte verfolgen und kontrollieren können. Während nur 16 % der Befragten in der Lage sind, dies jedes Mal zu tun, gaben 45 % an, dass sie in etwa drei Viertel der Fälle dazu in der Lage sind (Abb. 49). Dieser Anteil ist in einigen Segmenten noch höher: 70 % für Nordamerika, 79 % für die Fertigungsindustrie und 73 % für das Gesundheitswesen (Abb. 50 und 51). Weniger gut schneiden dagegen das Hochschulwesen (31 %) sowie die Öl- und Gasindustrie (34 %) ab.

Um festzustellen, welche unstrukturierten Daten kontrolliert werden sollten, muss ein Klassifizierungssystem vorhanden sein. Auf die Frage, wie viele ihrer unstrukturierten Daten mit Tags versehen oder klassifiziert sind, gaben *weniger als die Hälfte* der Befragten (48 %) an, dass dies bei 75 % oder mehr ihrer Daten der Fall ist (Abb. 14). In Nordamerika ist die Situation mit 56 % etwas besser (Abb. 52). Unter den Branchen haben 65 % im Gesundheitswesen, 56 % bei den Finanzdienstleistungen und 55 % im Rechtswesen dieses Niveau erreicht (Abb. 53).

Nur

16%

der Unternehmen können den Zugriff auf *alle* Inhalte nachverfolgen und kontrollieren, wenn diese eine Anwendung verlassen.

65%

der Befragten aus dem Gesundheitswesen gaben an, über 75 % ihrer unstrukturierten Daten zu taggen und zu klassifizieren (der höchste Wert aller Branchen).



Sicherheitstools für sensible Inhalte

Alle Unternehmen verfügen über eine Reihe von Sicherheitstools für ihre Netzwerke, Endgeräte und Cloud-Anwendungen. Ob diese auch zum Schutz der internen und externen Kommunikation sensibler Inhalte eingesetzt werden, ist eine andere Frage.

In Bezug auf die Nutzung von Funktionen wie Multi-Faktor-Authentifizierung, Verschlüsselung, Governance-Tracking und -Kontrollen für diese Kommunikation sind die Ergebnisse gemischt (Abb. 54). Fast 6 von 10 (59 %) geben an, dass diese Schutzmaßnahmen für die externe Kommunikation sensibler Inhalte immer vorhanden sind. Bei fast allen anderen sind sie manchmal vorhanden. Fast sechs von 10 (59 %) geben an, dass diese Schutzmaßnahmen bei der externen Kommunikation sensibler Inhalte immer vorhanden sind. Fast alle anderen sagen, dass sie manchmal vorhanden sind. In Nordamerika sind die Sicherheitsvorkehrungen am höchsten: 67 % der Befragten geben an, dass dies immer der Fall ist, gegenüber 57 % im asiatisch-pazifischen Raum und 53 % in der EMEA-Region.

Die Fähigkeit, die Sicherheit der Kommunikation sensibler Inhalte zu messen und zu verwalten, ist nach wie vor ein wichtiges Anliegen der Unternehmen: Nur 11 % der Befragten gaben an, dass keine Verbesserungen erforderlich seien, gegenüber 26 % in der Vorjahresumfrage (Abb. 55). Ein höherer Prozentsatz der Unternehmen hat in diesem Jahr *einigen Verbesserungsbedarf* festgestellt (56 % vs. 37 % im Vorjahr).

Während die Zahlen für die gesamte Kohorte gleich sind, gibt es interessante Unterschiede, wenn die Frage nach verschiedenen Gruppen analysiert wird. Für die interne Kommunikation gaben 71 % der staatlichen Behörden und Dienstleistungsunternehmen an, diese Tools immer zu verwenden (Abb. 56). Zwei Drittel (67 %) der nordamerikanischen Befragten gaben dies an, während es in der EMEA-Region nur 53 % waren (aber 63 % im Vereinigten Königreich) (Abb. 57). Interessant ist, dass Anwaltskanzleien (45 %) bei der internen Kommunikation am schlechtesten abschneiden. Bei der externen Kommunikation schnitten die Pharma- und Life-Sciences-Branche (78 %) und der Hochschulsektor (72 %) sowie nordamerikanische Unternehmen (69 %) am besten ab (Abb. 56).

56%



der Unternehmen gaben an, dass die Art und Weise, wie sie die Sicherheit der Kommunikation sensibler Inhalte messen und verwalten **verbesserungsbedürftig ist – 33 % mehr als im Vorjahr.**

Insights zu Datenschutz und Compliance bei der Kommunikation sensibler Inhalte

Operative Prozesse: Es braucht ein "Dorf" - und eine Menge Zeit - um Datensicherheit und Compliance zu managen

OPERATIVE PROZESSE

Insight: Es braucht ein "Dorf" – und eine Menge Zeit – um Datensicherheit und Compliance zu managen

Viele der oben beschriebenen Herausforderungen - Datenschutzverletzungen, Compliance- und Sicherheitsprobleme - werden durch die Komplexität der operativen Prozesse in den meisten Unternehmen noch verschärft. Angesichts der wachsenden Zahl von Kommunikationstools und der Unfähigkeit der meisten Unternehmen, manuelle Prozesse abzuschaffen, ist es unvermeidlich, dass Sicherheits- und Compliance-Probleme durch das Raster fallen.

Multiplikation durch externe Parteien und die damit verbundenen Risiken

Die meisten Unternehmen tauschen im Tagesgeschäft große Mengen sensibler Daten mit Hunderten oder gar Tausenden externer Parteien aus. Das Risiko im Zusammenhang mit externen Parteien war für Unternehmen aller Branchen noch nie so hoch wie heute, und die Notwendigkeit des Austauschs sensibler Inhalte verschärft die Bedrohung.

Als wir die Kohorte 2024 baten zu schätzen, wie viele externe Parteien sensible Inhalte von ihren Unternehmen erhalten, schätzten zwei Drittel (66 %) mehr als 1.000 (Abb. 58). Von den größten Unternehmen mit mehr als 30.001 Mitarbeitern tauschen 33 % Inhalte mit mehr als 5.000 externen Parteien aus (Abb. 59). 77 % der Unternehmen im asiatisch-pazifischen Raum tauschen sensible Daten mit 1.000 externen Parteien aus, 66 % in Nordamerika und 63 % in EMEA (Abb. 60).

Regierungsbehörden tauschen wesentlich häufiger sensible Inhalte aus als die meisten anderen Wirtschaftszweige (28 % teilen Daten mit mehr als 5.000 externen Parteien) (Abb. 61). Auch im Hochschulbereich werden viele Daten mit externen Parteien ausgetauscht. 47 % der Befragten gaben an, dass sie dies mit mehr als 2.500 externen Parteien tun.

Sobald sensible Inhalte das Unternehmen verlassen, geben 39 % der Unternehmen an, dass sie nur in der Lage sind, 50 % oder weniger der Zugriffe nachzuverfolgen und zu kontrollieren. Die EMEA-Region stellt hier die größte Herausforderung dar. 46 % geben an, dass sie in der Lage sind, den Zugriff auf 50 % oder weniger der sensiblen Inhalte zu verfolgen und zu kontrollieren, sobald diese das Unternehmen verlassen (Abb. 62). Zu den Unternehmen mit dem höchsten Risiko aufgrund mangelnder Nachverfolgbarkeit und Kontrolle gehören Kommunalverwaltungen (54 % geben zu, dass sie nicht in der Lage sind, sensible Inhalte nachzuverfolgen und zu kontrollieren, sobald diese ihre Organisation verlassen) sowie Pharma- und Life Science-Unternehmen (50 % können sensible Inhalte außerhalb ihrer Unternehmen nicht nachverfolgen und kontrollieren) (Abb. 63).

Ein Vergleich des Auftretens von Datenschutzverletzungen mit der Anzahl externer Parteien, mit denen Unternehmen sensible Inhalte austauschen, zeigt ein deutlich höheres Risiko (Abb. 64). Beispielsweise hatten 35 % derjenigen, die angaben, sensible Inhalte mit mehr als 5.000 externen Parteien auszutauschen, im letzten Jahr mehr als 10 Datenschutzverletzungen zu verzeichnen. 50 % derjenigen, die sensible Inhalte mit 2.500 bis 4.999 externen Parteien austauschen, hatten mehr als sieben Datenschutzverletzungen zu verzeichnen. Ähnliches gilt für die Kosten von Rechtsstreitigkeiten (Abb. 65). Von denjenigen, die sensible Daten mit 5.000 oder mehr externen Parteien austauschen, gab die Hälfte mehr als 5 Mio. USD für Prozesskosten aus. 44 % derjenigen, die sensible Inhalte mit 2.500 bis 4.999 externen Parteien austauschen, gaben ebenfalls mehr als 5 Mio. USD aus.



35%

derjenigen,
die angaben,
sensible Inhalte
mit über **5.000**
externen Parteien
auszutauschen,
erlebten mehr als
10 Datenschutz-
verletzungen
im vergangenen
Jahr.

Verbreitung der Kommunikationstools und Risiken

Es gibt eine Vielzahl von Kommunikationstools für den Versand und die gemeinsame Nutzung sensibler Inhalte: E-Mail, File Sharing, Managed File Transfer, SFTP (Secure File Transfer Protocol), Webformulare und andere. Das Bestreben, Risiken zu minimieren, Kosten zu senken und die betriebliche Effizienz zu steigern, dürfte zu einer Konsolidierung der Tools für die Kommunikation von Inhalten geführt haben: Im Jahr 2023 gab die Hälfte der Befragten an, sechs oder mehr Tools für die Kommunikation von Inhalten zu verwenden, im Vergleich zu 32 % in diesem Jahr ([Abb. 66](#)). Nordamerika hat mit 59 % der Befragten, die fünf oder mehr Instrumente nutzen, den höchsten Verbreitungsgrad, verglichen mit 50 % in EMEA und 52 % im Asien-Pazifik-Raum ([Abb. 67](#)). Erstaunliche 77 % der nordamerikanischen Unternehmen verwenden vier oder mehr Tools, und diese Zahl liegt bei 80 % oder mehr in den Bereichen Finanzdienstleistungen, Rechtswesen, Dienstleistungen sowie Öl und Gas ([Abb. 68](#)).

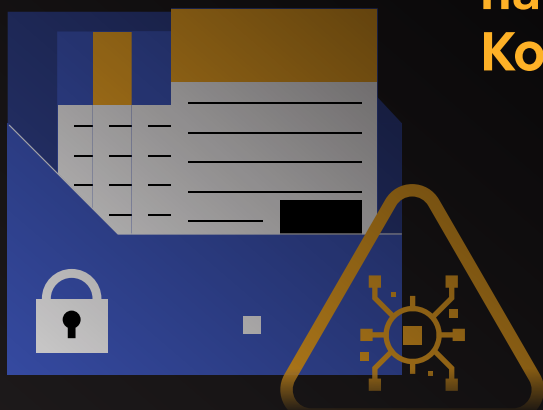
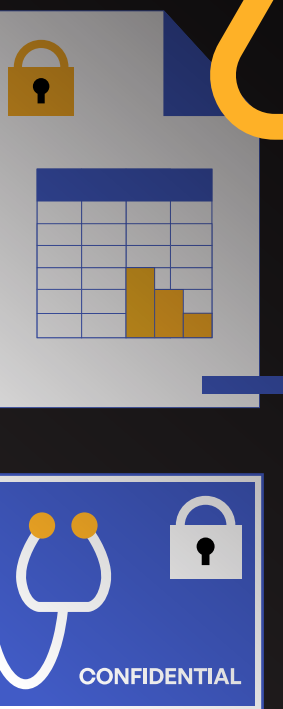
Eine Cross-Analyse der oben genannten Punkte zeigt, dass Unternehmen mit einer höheren Rate an Datenschutzverletzungen mehr Kommunikationstools im Einsatz haben ([Abb. 69](#)). Beispielsweise hatten 32 % der Unternehmen mit zehn oder mehr Datenschutzverletzungen mehr als sieben Kommunikationstools, und 42 % der Unternehmen mit sechs Kommunikationstools hatten sieben bis neun Datenschutzverletzungen. Diese Zahlen sind dramatisch höher als die durchschnittliche Anzahl von Datenschutzverletzungen bei allen Befragten: Nur 9 % berichteten über 10 Datenpannen (im Vergleich zu 32 % mit sieben oder mehr Kommunikationstools) und nur 23 % berichteten über sieben bis neun Datenschutzverletzungen ([Abb. 6](#)). Dies entspricht einer 3,55-fach höheren Rate bei den Befragten mit 10 oder mehr Kommunikationstools und einer 2-fach höheren Rate bei den Befragten mit 7 bis 9 Tools. Das Gleiche gilt für die Kosten, die den Unternehmen durch Rechtsstreitigkeiten aufgrund von Datenschutzverletzungen entstanden sind: 26 % der Unternehmen, die angaben, im letzten Jahr mehr als 7 Mio. USD gezahlt zu haben, verfügten über mehr als sieben Kommunikationstools (3,25-mal höher als der Durchschnitt von 8 %) ([Abb. 70](#)).



32%

der Befragten, die mehr als 10 Datenpannen zu verzeichnen hatten, haben mehr als sieben Kommunikationstools.

Je mehr Kommunikationstools ein Unternehmen einsetzt, desto mehr Datenpannen gibt es und desto höher sind die Kosten für Rechtsstreitigkeiten.



38%

der nordamerikanischen Befragten gaben an, **mehr als sechs Kommunikationstools** zu nutzen (mehr als in den anderen Regionen).

Zwei Drittel der Unternehmen **tauschen sensible Inhalte mit mehr als 1.000 externen Parteien** aus.

Protokollabgleich, der sich summiert

Der Abgleich von Protokollen für die Kommunikation sensibler Inhalte für Audit-Berichte ist für viele Befragte eine zeitaufwändige Aufgabe. 48 % gaben an, dass sie mehr als 11 Protokolle konsolidieren müssen, 14 % sogar mehr als 20 Protokolle. Nicht zu wissen, welche Protokolle abzugleichen sind, stellt an sich schon ein Risiko dar. 8 % gaben an, nicht zu wissen, wie viele Protokolle sie haben ([Abb. 71](#)).

Größere Unternehmen gaben an, dass sie eine größere Anzahl von Audit-Protokollen konsolidieren müssen; so konsolidieren 34 % der Unternehmen mit mehr als 30.001 Beschäftigten mehr als 20 Audit-Protokolle (im Vergleich zu 14 % der Unternehmen mit 20.001 bis 25.000 Beschäftigten und 11 % der Unternehmen mit 25.001 bis 30.000 Beschäftigten) ([Abb. 72](#)).

34%

der Unternehmen mit mehr als 30.001 Beschäftigten gaben an, mehr als 20 Protokolle von Kommunikationstools abgleichen zu müssen.

Der Abgleich von Protokollen kostet wertvolle Zeit und Ressourcen. 20 % der Befragten gaben an, dass dies mehr als 40 Stunden pro Monat in Anspruch nimmt, und weitere 40 % gaben an, dass dies mehr als 25 Stunden pro Monat in Anspruch nimmt ([Abb. 73](#)). Mit zunehmender Unternehmensgröße steigt auch der Aufwand für die Erfassung der Protokolle. 24 % der Unternehmen mit mehr als 30.001 Beschäftigten gaben an, mehr als 40 Stunden pro Monat aufzuwenden ([Abb. 74](#)). Weitere 9 % der Unternehmen mit mehr als 30.001 Mitarbeitern gaben an, dass es nicht möglich ist, ihre Protokolle zu erfassen, was auf ein erhebliches Sicherheits- und Compliance-Risiko hindeutet. In Bezug auf die Branche ([Abb. 75](#)), sind Anwaltskanzleien das größte Segment, welches einräumt, die Protokolle nicht abgleichen zu können (10 %). Hochschulen sind führend, wenn es um die Zeit geht, die für die Konsolidierung der Protokolle aufgewendet wird - 30 % wenden 40 Stunden oder mehr pro Monat auf.

Unter allen Branchen gaben mehr Befragte aus Regierungsbehörden (34 %) an, dass sie mehr als 20 Protokolle von Kommunikationstools konsolidieren müssen.

Dateigrößenbeschränkungen und Risiken

Die Beschränkung der Dateigröße ist eine Herausforderung für viele Tools zum Austausch von Inhalten. Die Frustration von Mitarbeitern, die einfach nur ihre Arbeit erledigen wollen, kann manchmal dazu führen, dass sie nicht autorisierte File-Sharing-Dienste für Verbraucher nutzen, um die Beschränkungen zu umgehen. Aber selbst für die Nutzer, die sich an die Regeln halten, können die daraus resultierenden Workarounds einen erheblichen Zeitaufwand bedeuten.

Abgesehen von SFTP (27 %) müssen *mehr als drei von zehn* Unternehmen aufgrund von Dateigrößenbeschränkungen für E-Mail, File Sharing und Managed File Transfer mehr als 50 Mal pro Monat auf Workarounds zurückgreifen ([Abb. 76](#)). Etwa 10 % gaben an, dass sie dies mehr als 100 Mal im Monat tun müssen (10 % für E-Mail, 11 % für File Sharing, 8 % für SFTP und 11 % für Managed File Transfer). Mehr als die Hälfte der Befragten nutzt diese vier Kommunikationskanäle mehr als 25 Mal pro Monat. Nach Regionen betrachtet ist die Häufigkeit in Nordamerika höher als in EMEA und im asiatisch-pazifischen Raum; die Zahl derer, die mehr als 100 Mal pro Monat auf Workarounds zurückgreifen müssen, ist für alle Kommunikationswege mehr als doppelt so hoch ([Abb. 77](#)).

30⁺%

der Unternehmen
müssen **50 Mal pro Monat**
Workarounds aufgrund
von **Dateigrößen-**
beschränkungen für
E-Mail, File Sharing,
Managed File
Transfer und SFTP
implementieren.

Schlüsselfaktoren für das Risikomanagement bei der Kommunikation sensibler Inhalte

Wahrscheinlich sind den Lesern bereits einige der Probleme bekannt, die sich aus der Verwendung mehrerer Tools für die Kommunikation sensibler Inhalte ergeben - die Risiken und Herausforderungen in Bezug auf Sicherheit und Compliance, der Mangel an Transparenz über alle Datentypen hinweg und die ineffizienten manuellen Prozesse. Um herauszufinden, wie die Umfrageteilnehmer mit dieser Komplexität umgehen, haben wir sie gebeten, die zwei wichtigsten Faktoren für die Vereinheitlichung und den Schutz ihrer Kommunikation mit sensiblen Inhalten zu nennen ([Abb. 78](#)). Die am häufigsten genannte Antwort (56 %) war der *Schutz von geistigem Eigentum und Betriebsgeheimnissen*, dicht gefolgt von der *Vermeidung von Rechtsstreitigkeiten* (51 %) und *Gesetzesverstößen* (48 %).

Interessant sind die Unterschiede in der Bedeutung von Rechtsstreitigkeiten je nach beruflicher Funktion ([Abb. 79](#)). Diese wurden von 79 % der IT-Experten und 61 % der Mitglieder von Sicherheitsteams genannt, aber nur von 39 % der Beschäftigten im Bereich Risiko und Compliance. Befragte aus den Bereichen Recht (75 %), Öl und Gas (75 %) und Regierungsbehörden (69 %) äußerten sich besonders besorgt über die Preisgabe geistigen Eigentums ([Abb. 80](#)).

Auch regional gab es interessante Unterschiede ([Abb. 81](#)). Die Befragten aus dem *asiatisch-pazifischen Raum* nannten die Vermeidung von schädlichen Auswirkungen auf die Marke als wichtigsten Faktor (79 %), gefolgt von der Vermeidung langwieriger und kostspieliger Rechtsstreitigkeiten (61 %). In der *EMEA-Region* war die Verhinderung des Abflusses vertraulichen geistigen Eigentums und von Geschäftsgeheimnissen der wichtigste Faktor (62 %), gefolgt von der Vermeidung langwieriger und teurer Rechtsstreitigkeiten (51 %). Die *nordamerikanischen Befragten* nannten an erster Stelle die Vermeidung von Betriebsunterbrechungen und Umsatzeinbußen (57 %), gefolgt von der Verhinderung der Preisgabe von vertraulichem geistigem Eigentum und Geschäftsgeheimnissen (51 %).

Die wichtigsten Gründe für die Vereinheitlichung und den Schutz der Kommunikation sensibler Inhalte waren **der Schutz des geistigen Eigentums und von Betriebsgeheimnissen (56 %)** sowie die **Vermeidung von Rechtsstreitigkeiten (51 %)** und **Verstößen gegen gesetzliche Bestimmungen (48 %)**.

Fazit

Die Ergebnisse des diesjährigen Berichts über Datenschutz und Compliance bei der Kommunikation sensibler Inhalte unterstreichen, wie wichtig es für Unternehmen ist, *proaktive Maßnahmen* zum Schutz ihrer sensiblen Inhalte zu ergreifen. Eine wichtige Erkenntnis ist die *Konsolidierung von Kommunikationstools* auf einer einzigen Plattform. Durch die Verringerung der Anzahl unterschiedlicher Tools für die Kommunikation von Inhalten können Unternehmen das Risiko von Datenschutzverletzungen erheblich reduzieren und die betriebliche Effizienz verbessern. Unternehmen mit einer geringeren Anzahl von Kommunikationstools verzeichnen weniger Datenschutzverletzungen, was auf einen Zusammenhang zwischen Toolkonsolidierung und verbesserter Sicherheit hindeutet.

Der Bericht weist auch auf die erheblichen Risiken hin, die mit *nicht gekennzeichneten und nicht klassifizierten Daten* verbunden sind. Unternehmen, die es versäumen, solide Systeme zur Kennzeichnung und Klassifizierung von Daten zu implementieren, sind einem höheren Risiko von Datenschutzverletzungen ausgesetzt, da sie nicht die erforderliche Transparenz und Kontrolle über ihre sensiblen Inhalte haben. Das exponentielle Datenwachstum, das durch die Einführung von GenKI noch beschleunigt wird, macht es für Unternehmen zwingend erforderlich, der Datenklassifizierung Priorität einzuräumen, um diese Risiken wirksam zu mindern.

Die Implementierung von *Zero-Trust-Prinzipien und erweiterten Sicherheitsfunktionen* ist entscheidend für die Verbesserung der Sicherheit bei der Kommunikation sensibler Inhalte. Die Ergebnisse des Berichts offenbaren erhebliche Sicherheitslücken und die Notwendigkeit eines strikten, inhaltsdefinierten Zero Trust, der attributbasierte Zugriffskontrollen, umfassende Verschlüsselung, Echtzeitüberwachung und die Verhinderung von Datenverlusten umfasst. Unsere Ergebnisse zeigen, dass die Lücken in bestimmten Branchen, Regionen und Ländern größer sind als in anderen.

Die Daten zeigen auch, dass der Austausch sensibler Inhalte mit *externen Parteien* mit *erheblichen Risiken* verbunden ist: Mit der Anzahl der externen Parteien, mit denen die Befragten sensible Inhalte austauschen, steigen die Anzahl der Datenschutzverletzungen und die Prozesskosten. Unternehmen müssen daher sicherstellen, dass sie über umfassende Kontrollmechanismen und erweiterte Sicherheitsfunktionen verfügen, um die mit externen Parteien verbundenen Risiken zu minimieren.

In diesem Zusammenhang ist eine abschließende Bemerkung zu den *Kosten von Datenschutzverletzungen* und insbesondere zu den damit verbundenen Kosten für Rechtsstreitigkeiten angebracht. Die diesjährige Umfrage hat gezeigt, dass vielen Unternehmen erhebliche Prozesskosten entstehen, die in den herkömmlichen Kostenschätzungen für Datenschutzverletzungen oft nicht berücksichtigt werden. Reputationsschäden, Umsatzeinbußen und gestörte Betriebsabläufe sind nur einige der Folgen von Datenschutzverletzungen. Bußgelder und Strafen für die Nichteinhaltung von Vorschriften sowie langwierige Rechtsstreitigkeiten wirken sich oft über lange Zeiträume aus. Dies unterstreicht die Bedeutung der Prüfung und Auswahl von Tools für die Kommunikation sensibler Inhalte, die Sicherheitsstandards wie FedRAMP, ISO 27001, SOC 2 Type II, NIST CSF 2.0 und andere erfüllen.

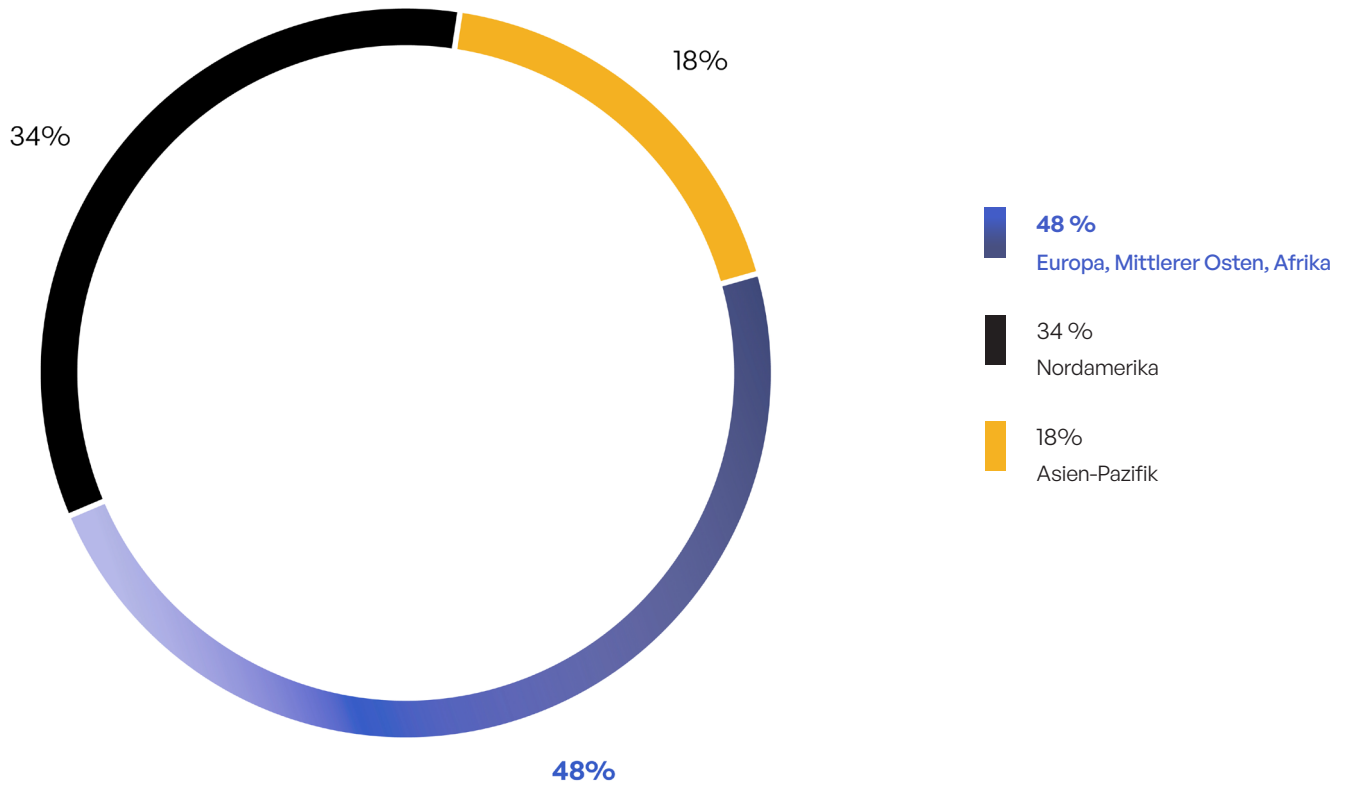


Abb. 1: Regionale Verteilung.

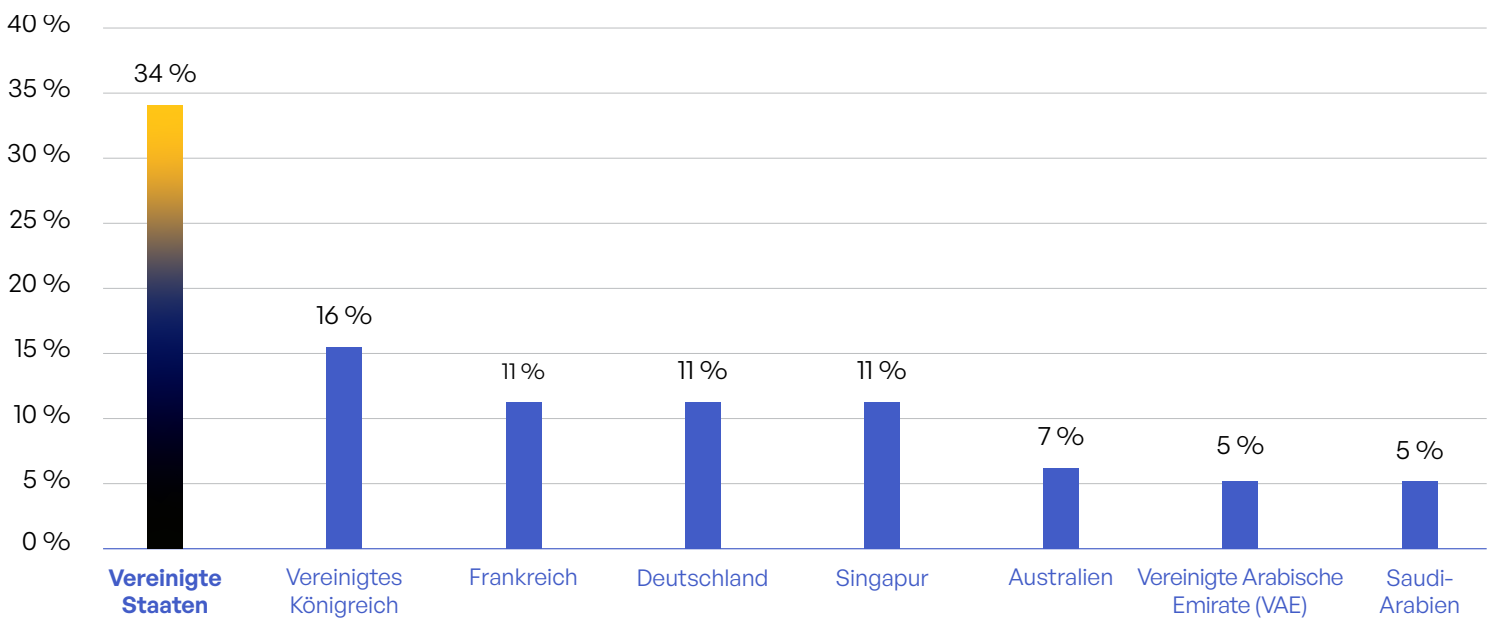


Abb. 2: Verteilung nach Ländern.

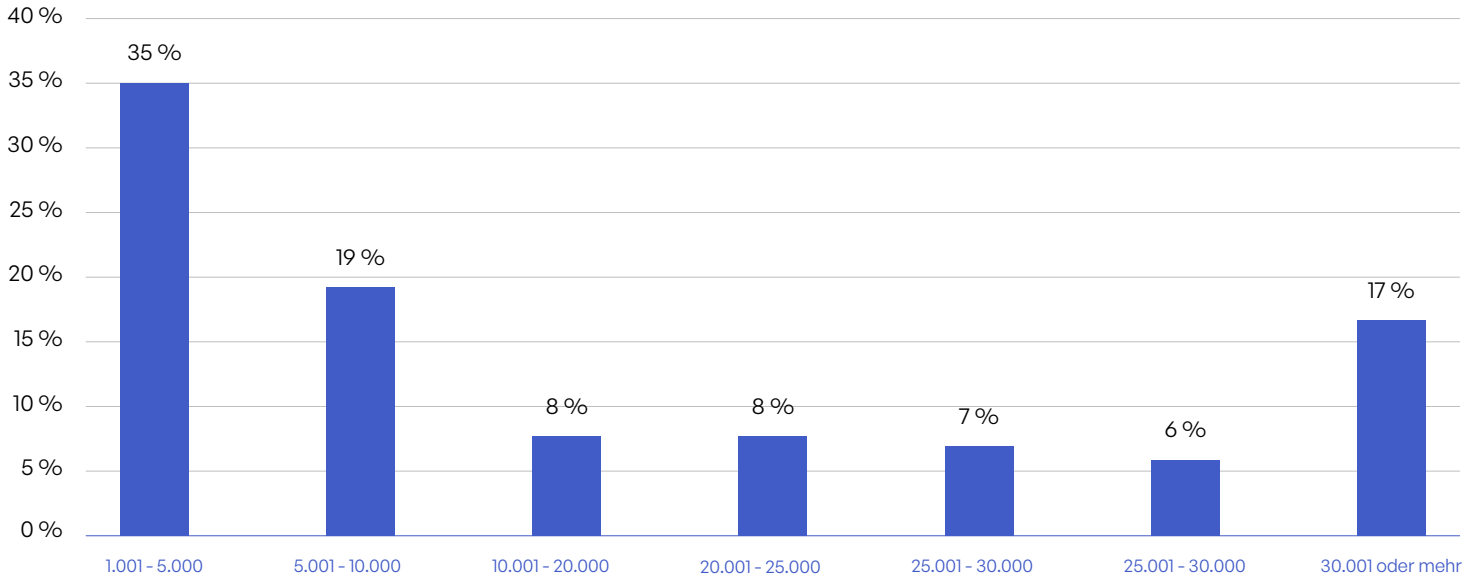


Abb. 3: Unternehmensgröße.

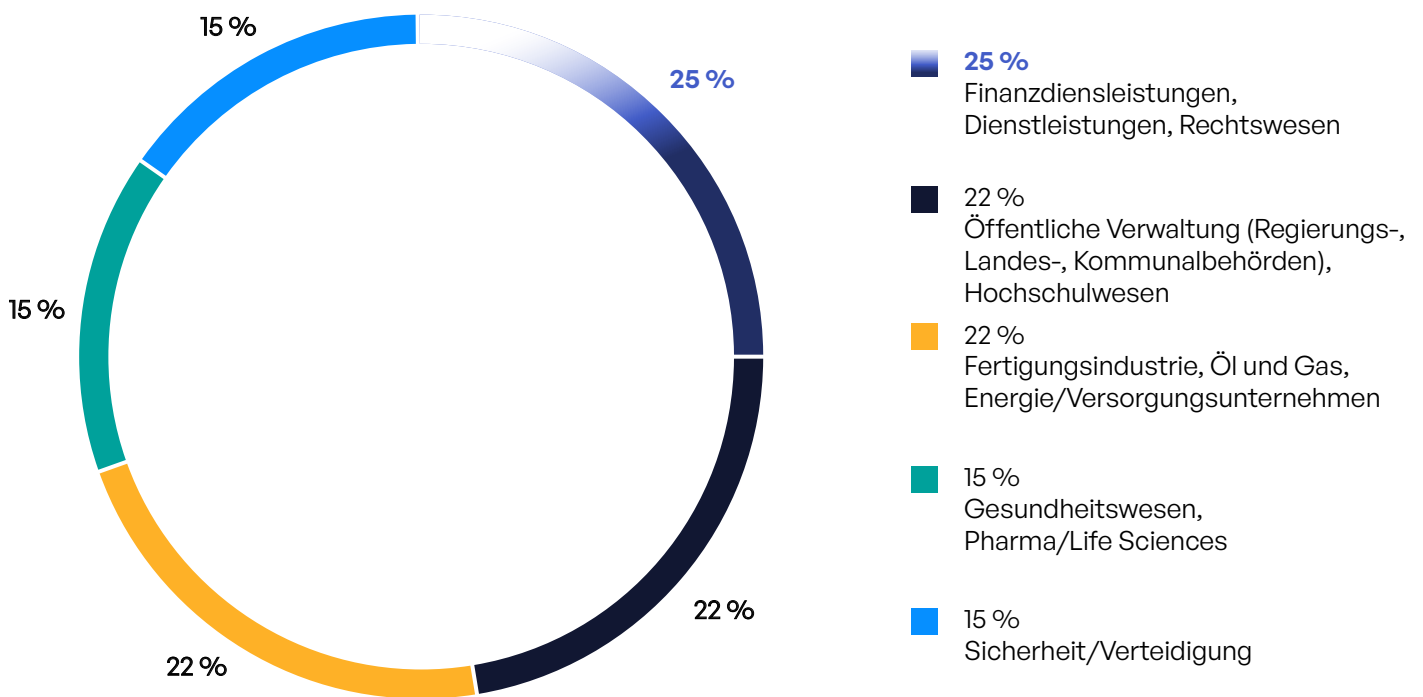


Abb. 4: Verteilung nach Branchen.

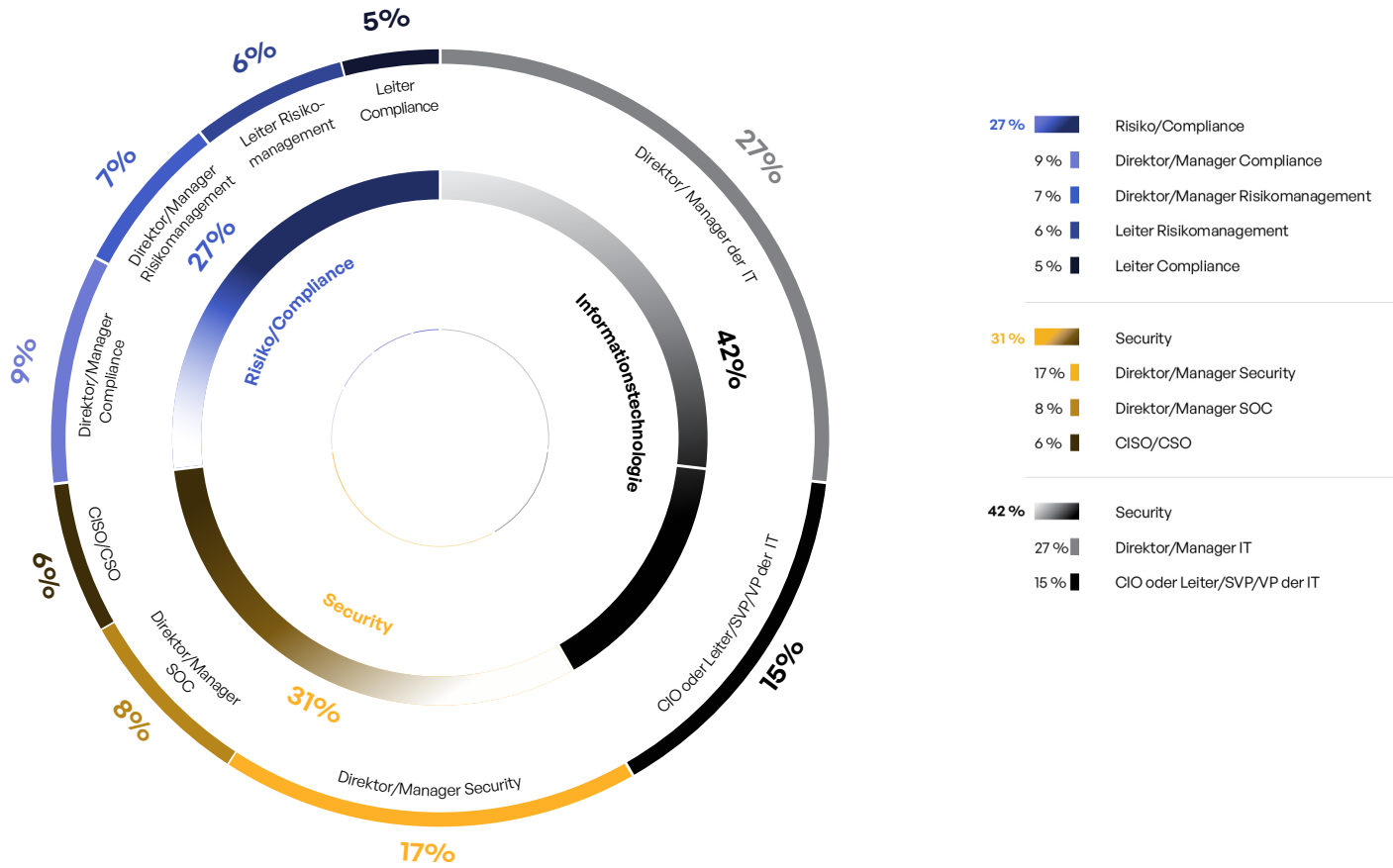


Abb. 5: Job-Funktionen/Verantwortlichkeiten.

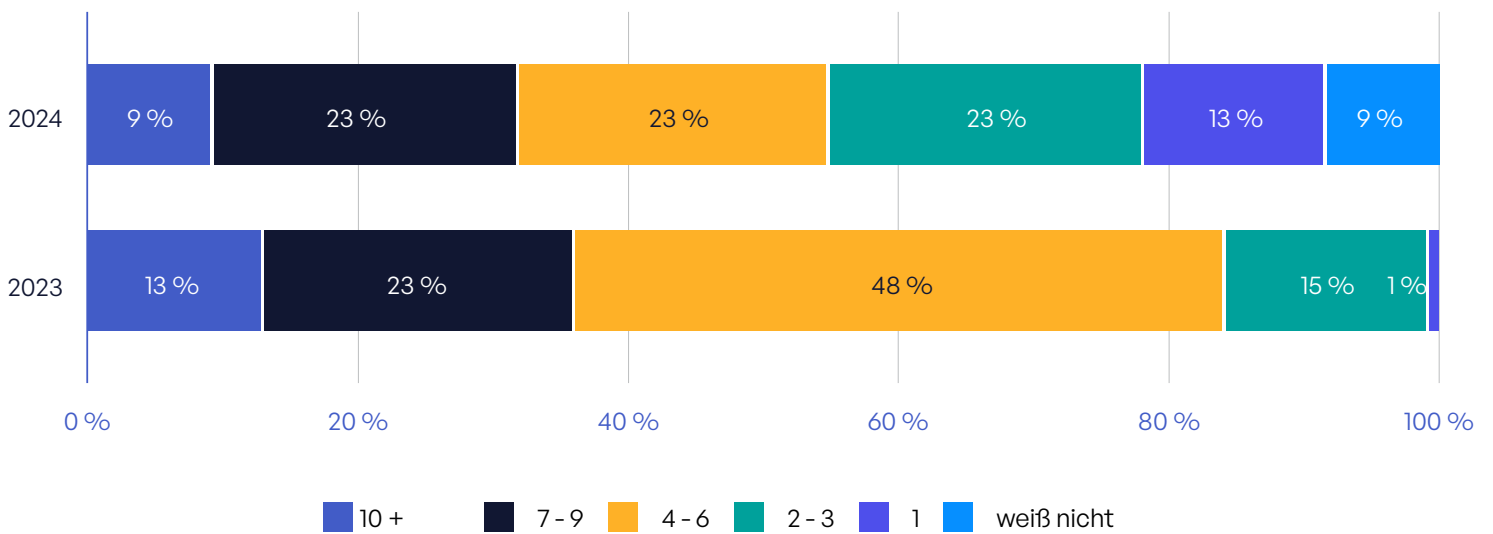


Abb. 6: Externe Hackerangriffe auf sensible Inhalte im vergangenen Jahr.

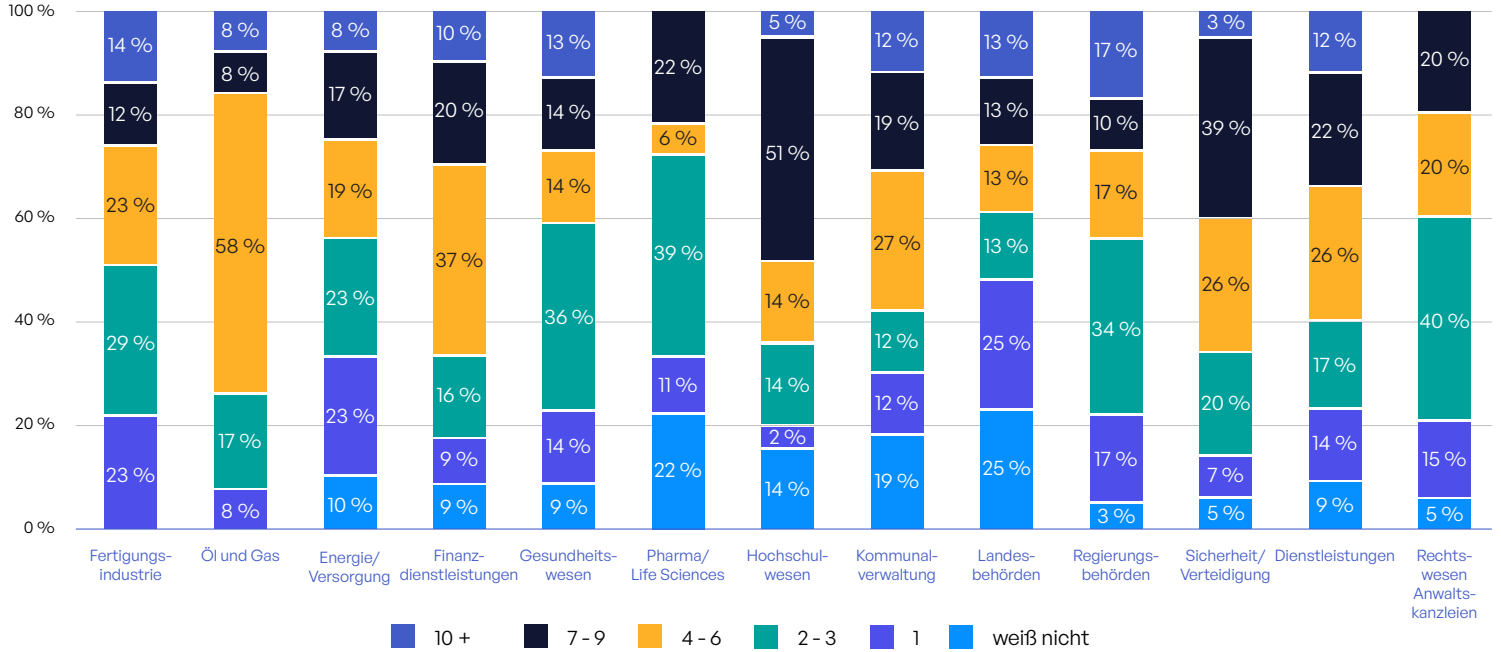


Abb. 7: Externe Hackerangriffe nach Branche.

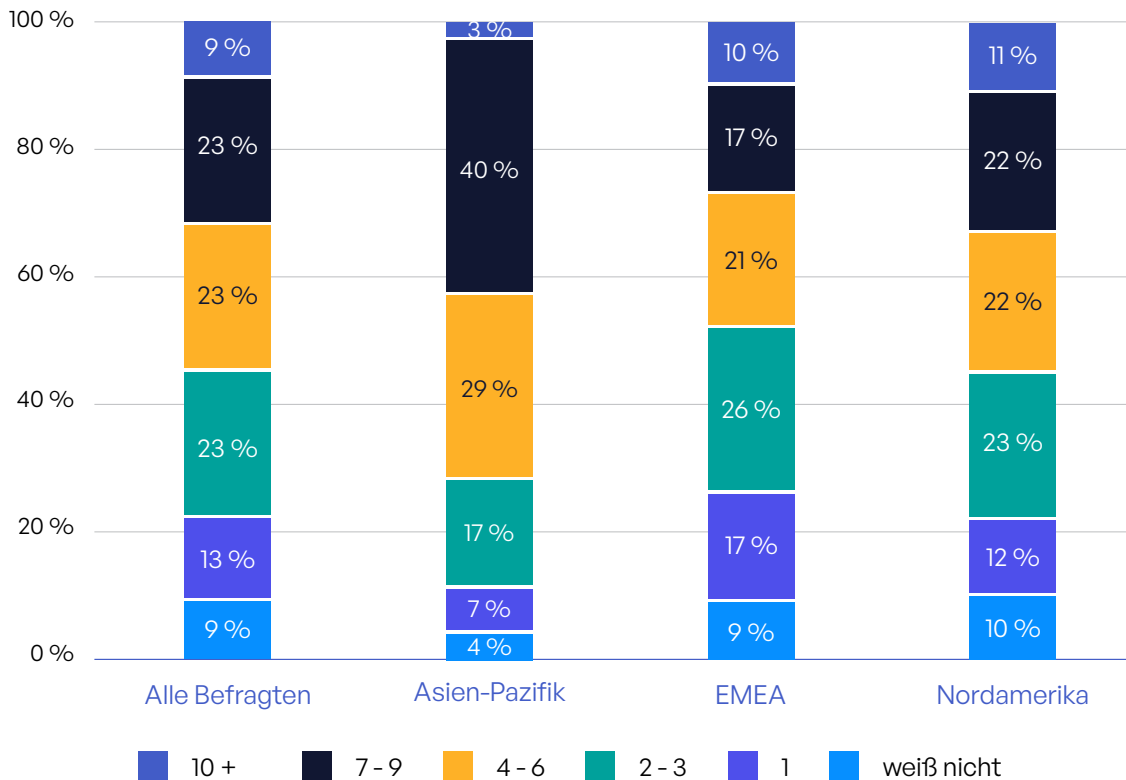


Abb. 8: Externe Hackerangriffe nach Region.

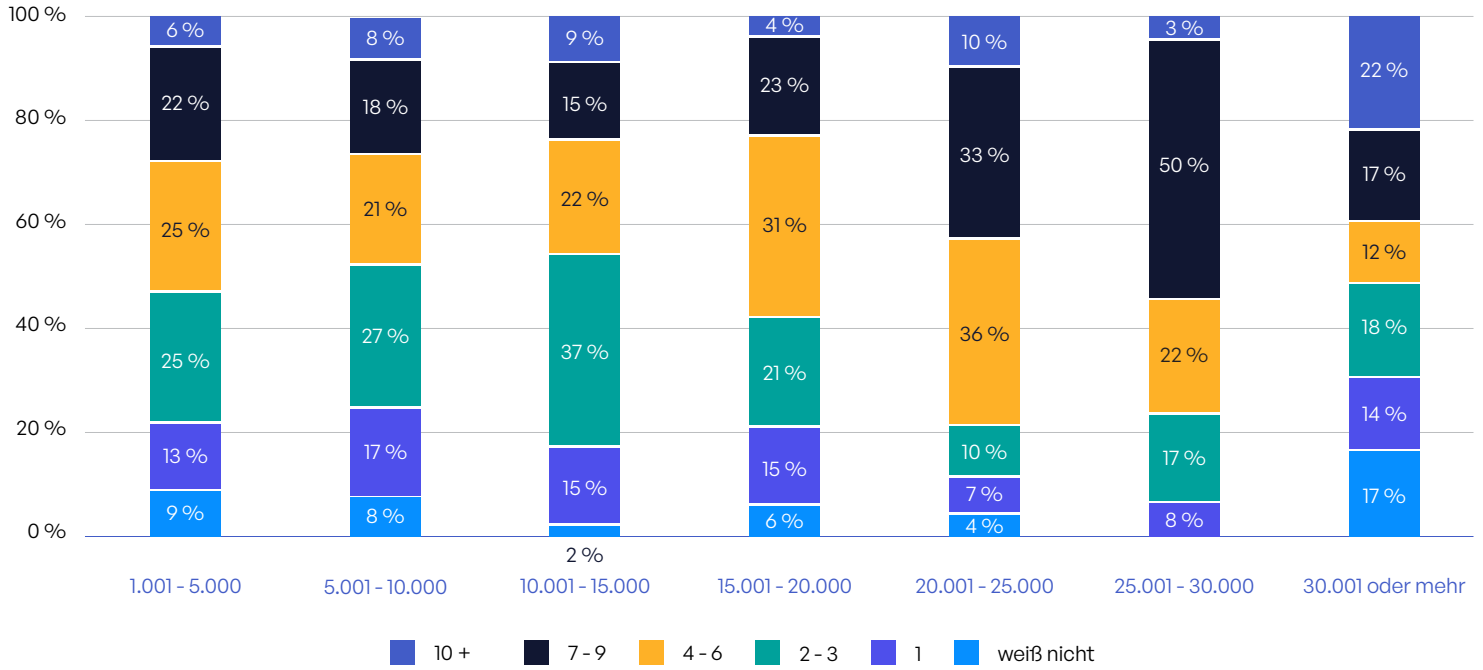


Abb. 9: Externe Hackerangriffe nach Unternehmensgröße.

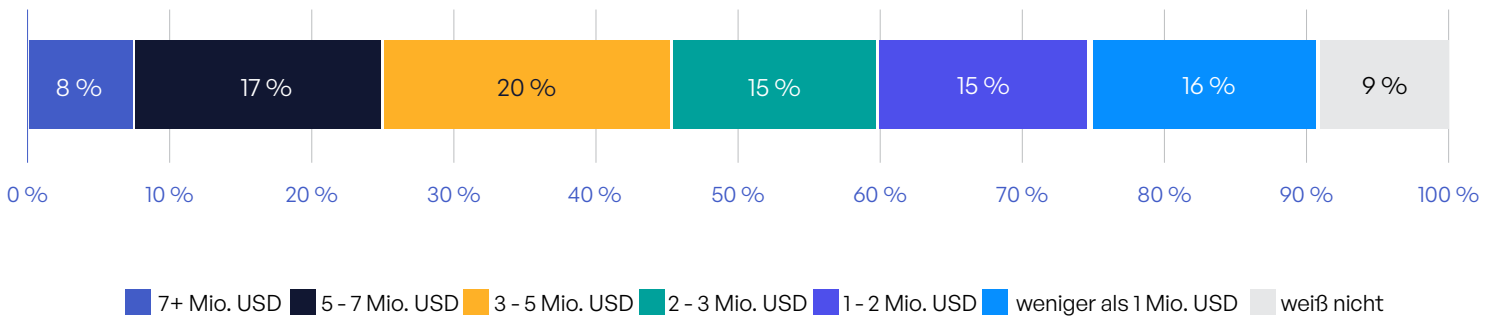


Abb. 10: Jährliche Prozesskosten im Zusammenhang mit Datenschutzverletzungen.

ERGEBNISSE DER UMFRAGE

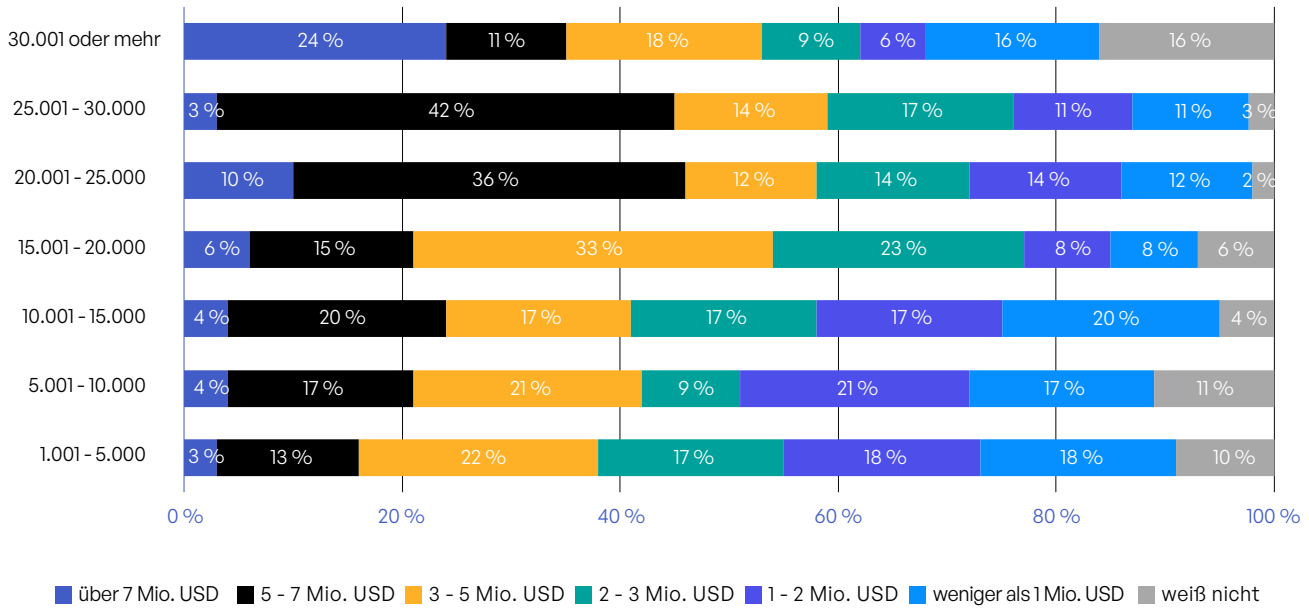


Abb. 11: Jährliche Prozesskosten im Zusammenhang mit Datenschutzverletzungen nach Unternehmensgröße.

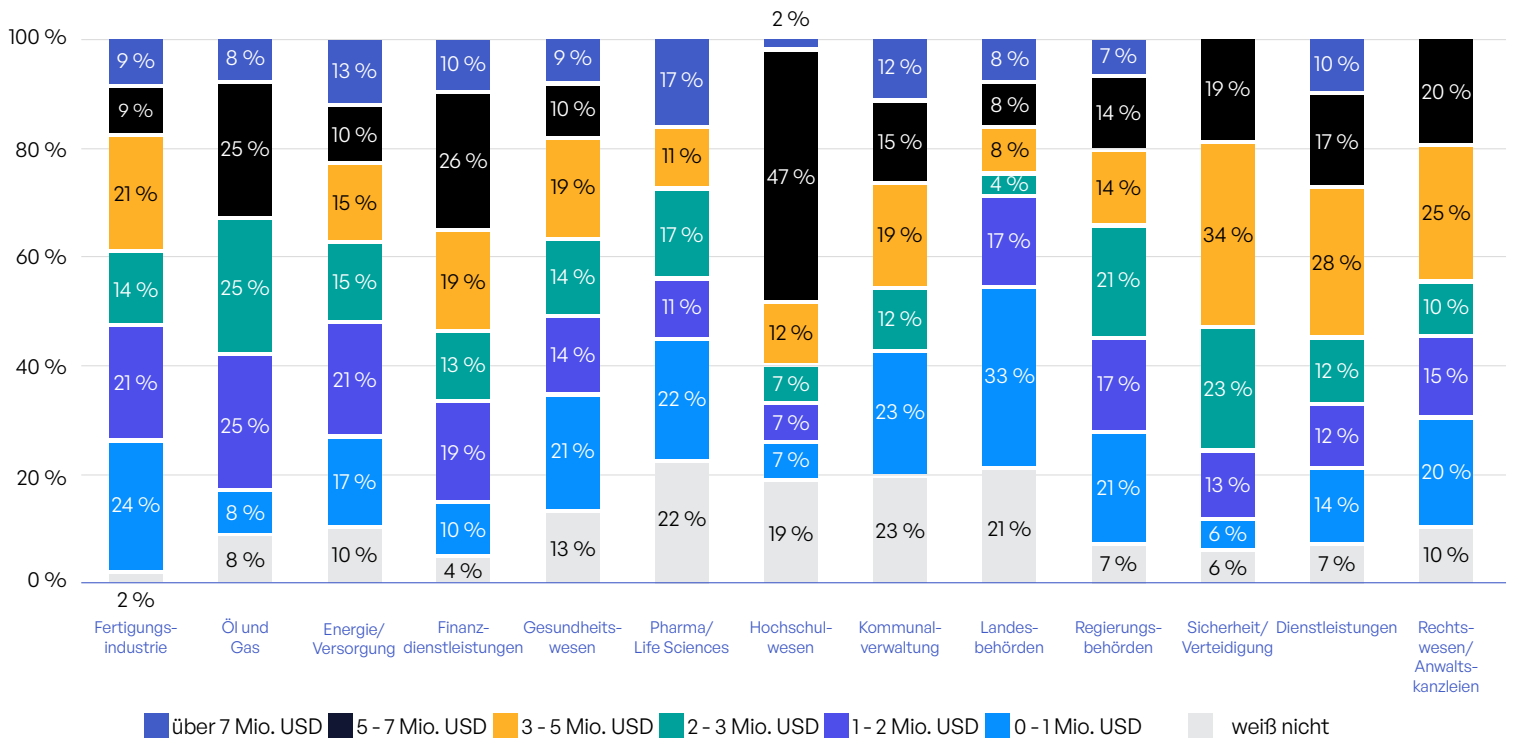


Abb. 12: Kosten im Zusammenhang mit Datenschutzverletzungen nach Branchen.

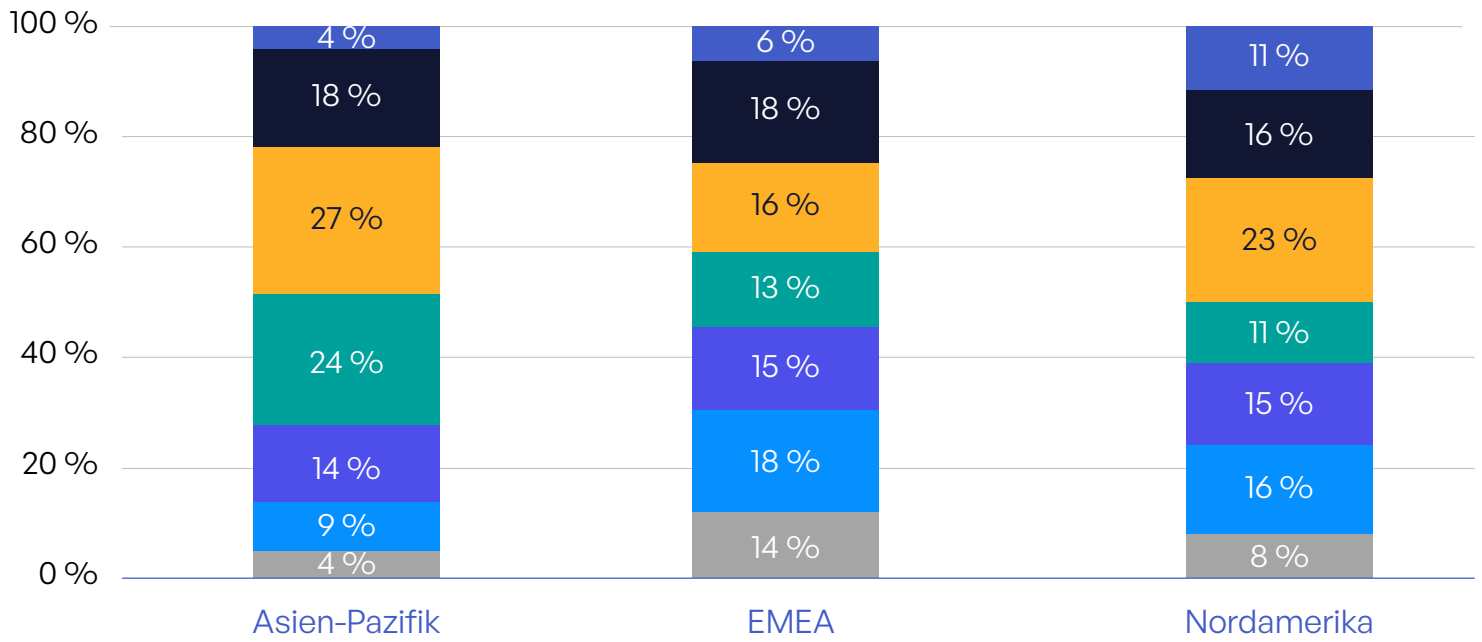


Abb. 13: Prozesskosten nach Regionen.

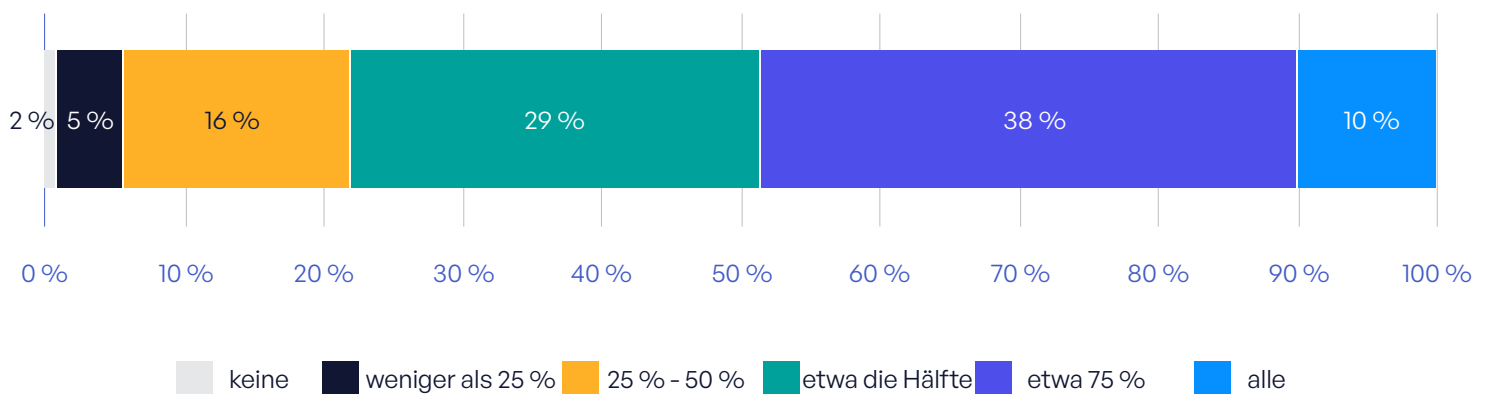


Abb. 14: Unstrukturierte Daten, die getaggt/klassifiziert sind.

ERGEBNISSE DER UMFRAGE

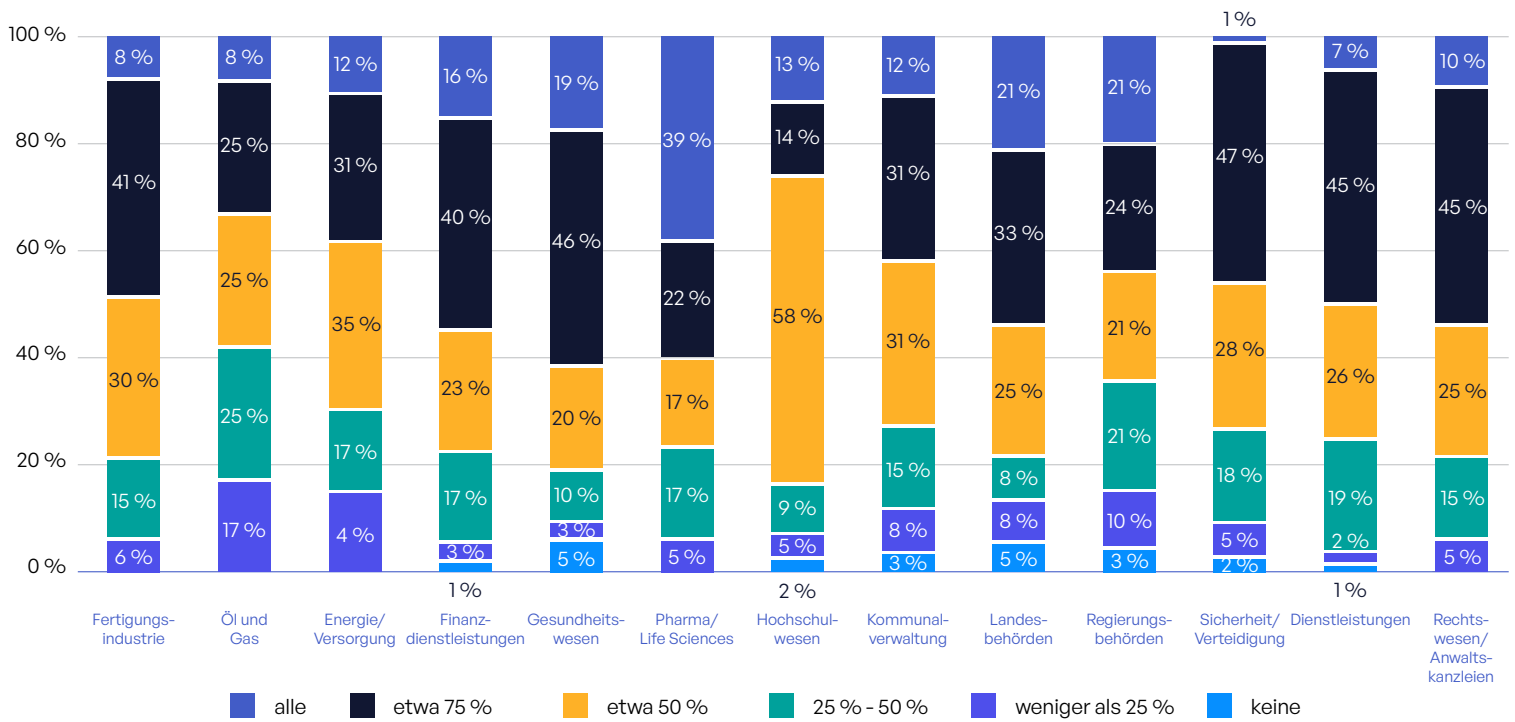


Abb. 15: Klassifizierung und Kennzeichnung unstrukturierter Daten nach Branchen.

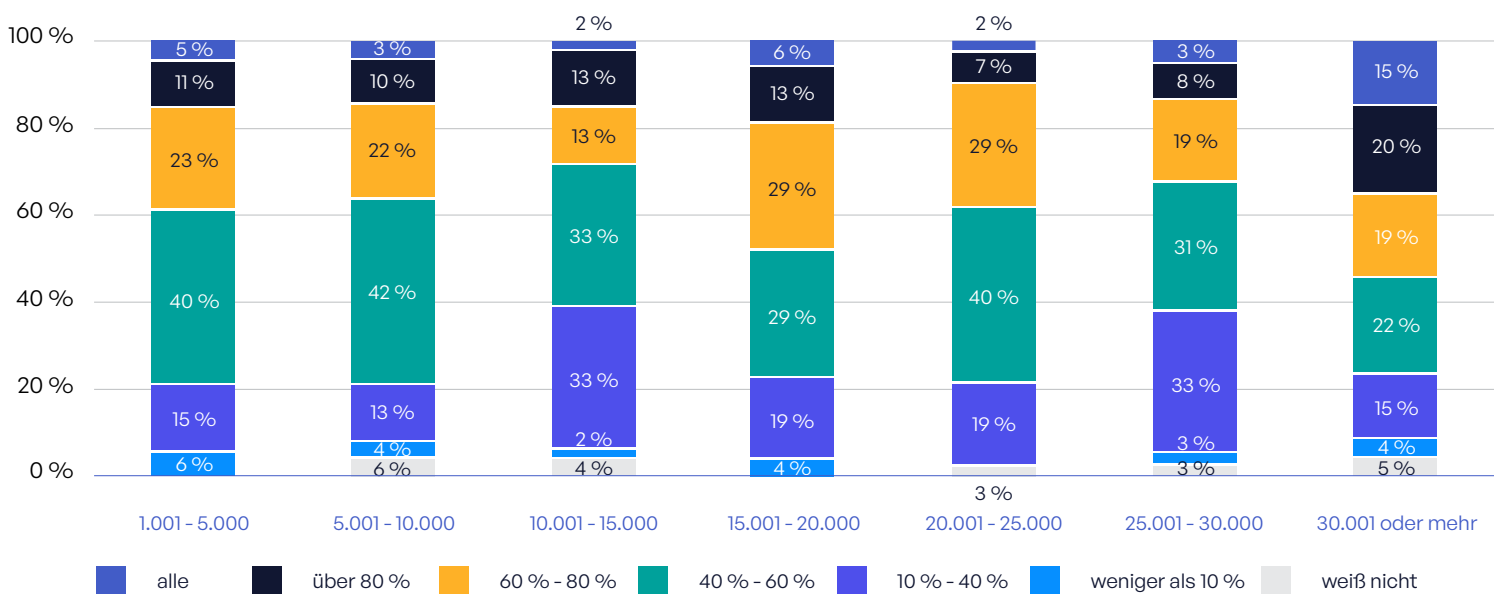


Abb. 16: Gekennzeichnete und klassifizierte unstrukturierte Daten nach Unternehmensgröße.

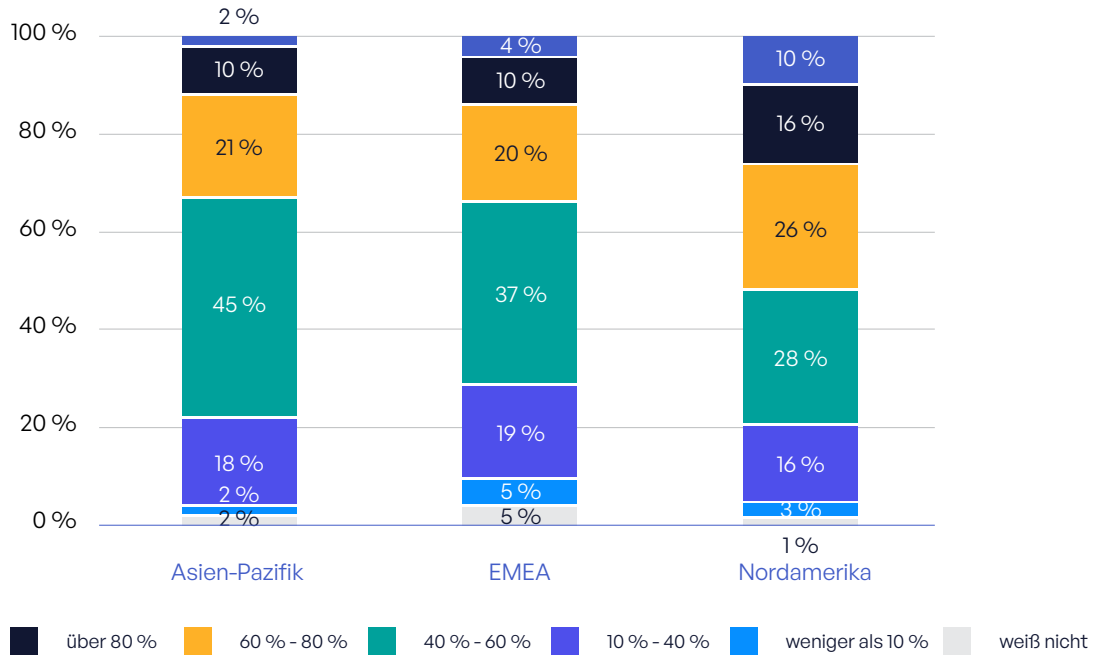


Abb. 17: Gekennzeichnete und klassifizierte unstrukturierte Daten nach Region.

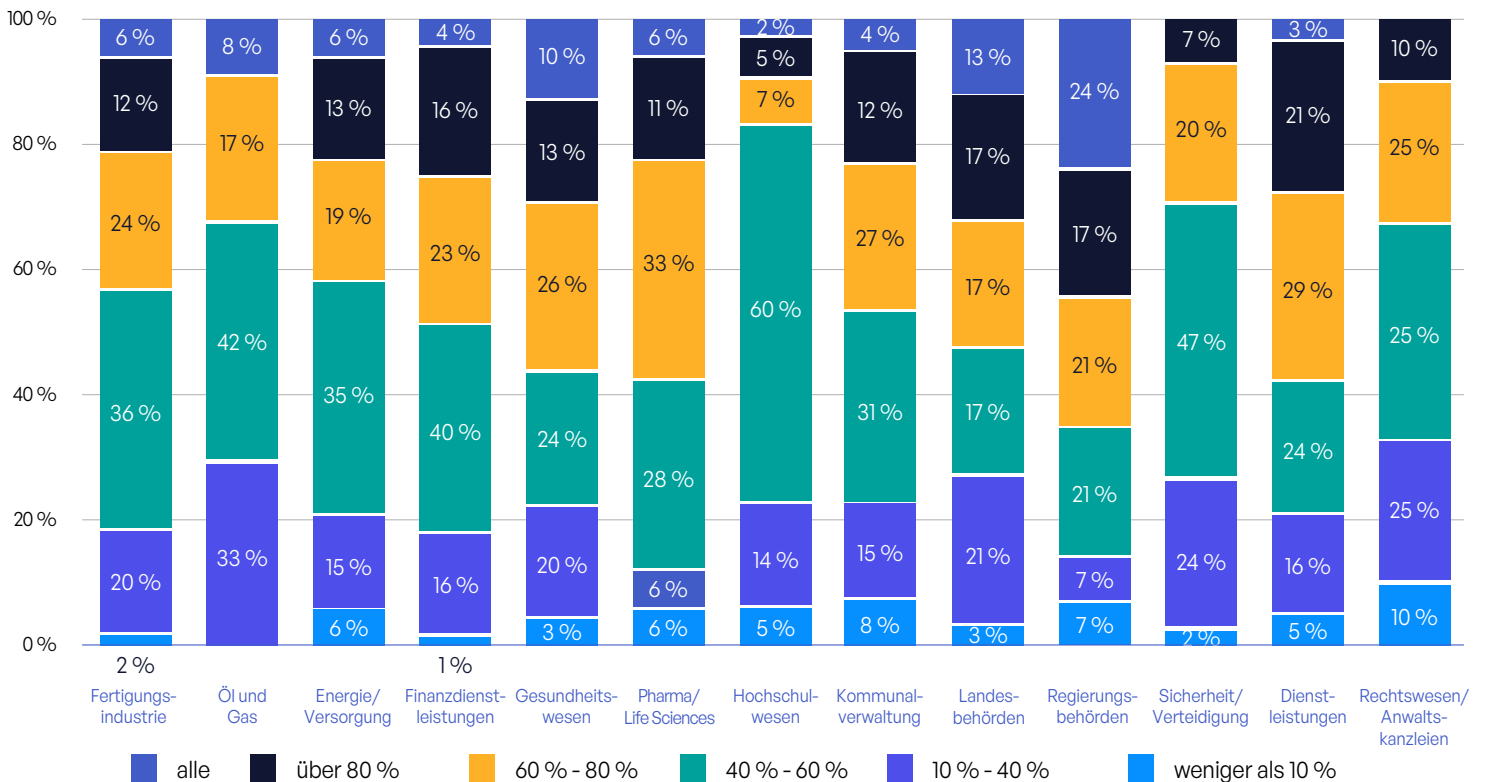


Abb. 18: Gekennzeichnete und klassifizierte unstrukturierte Daten nach Branchen.

ERGEBNISSE DER UMFRAGE

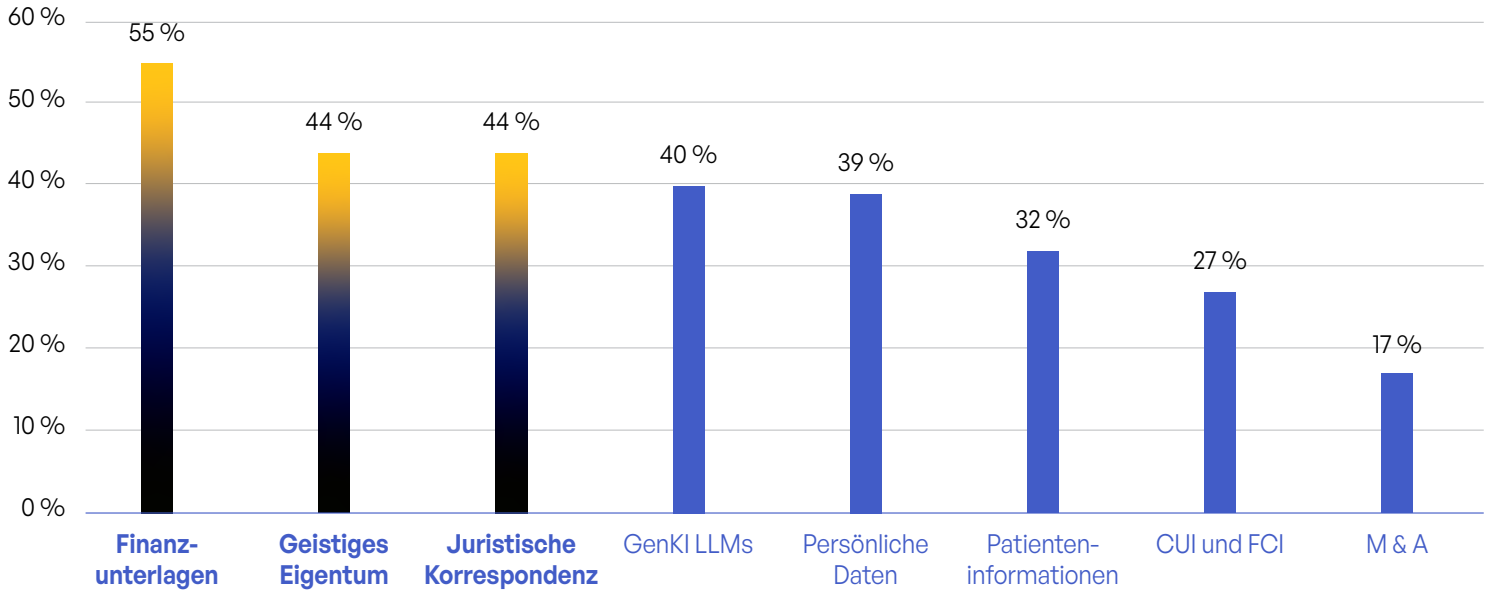


Abb. 19: Die drei wichtigsten Datenarten.

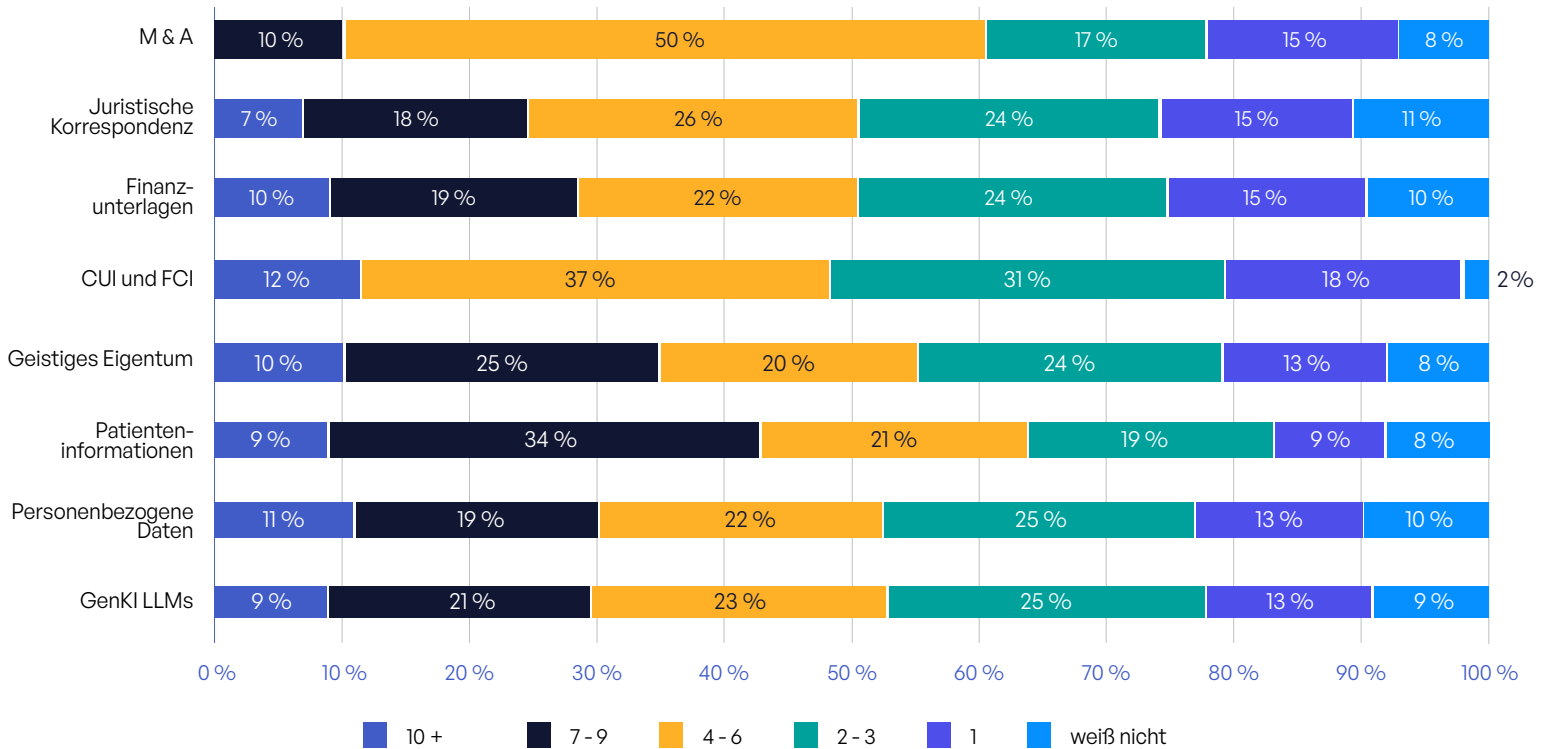


Abb. 20: Datenarten und Datenschutzverletzungen.

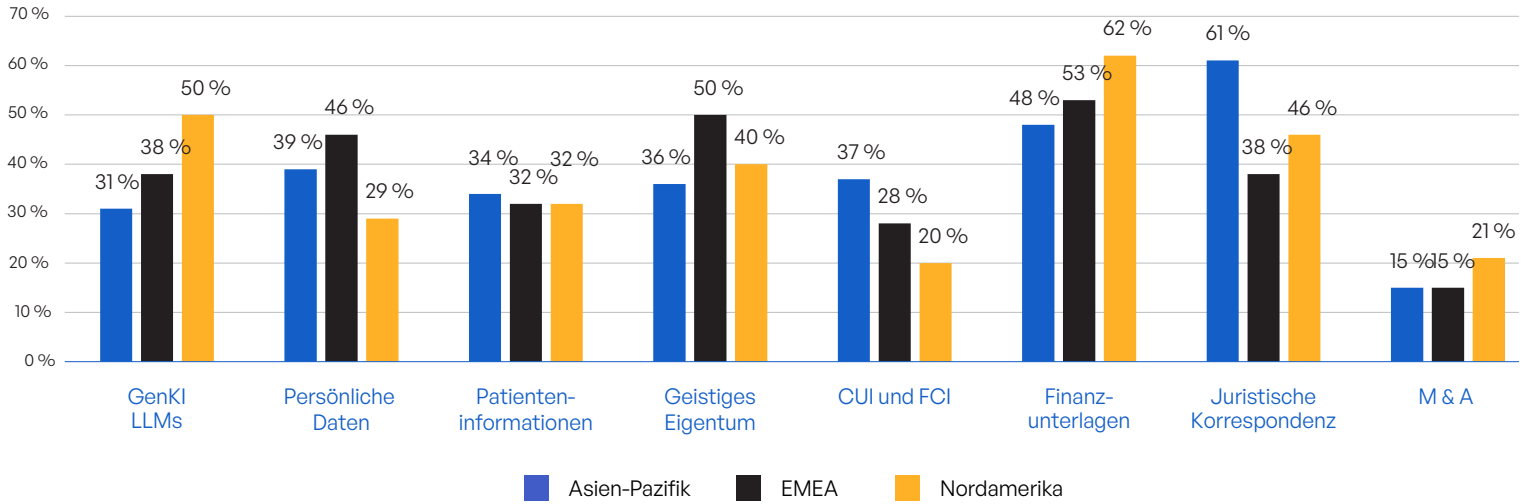


Abb. 21: Die wichtigsten Datenarten nach Regionen.

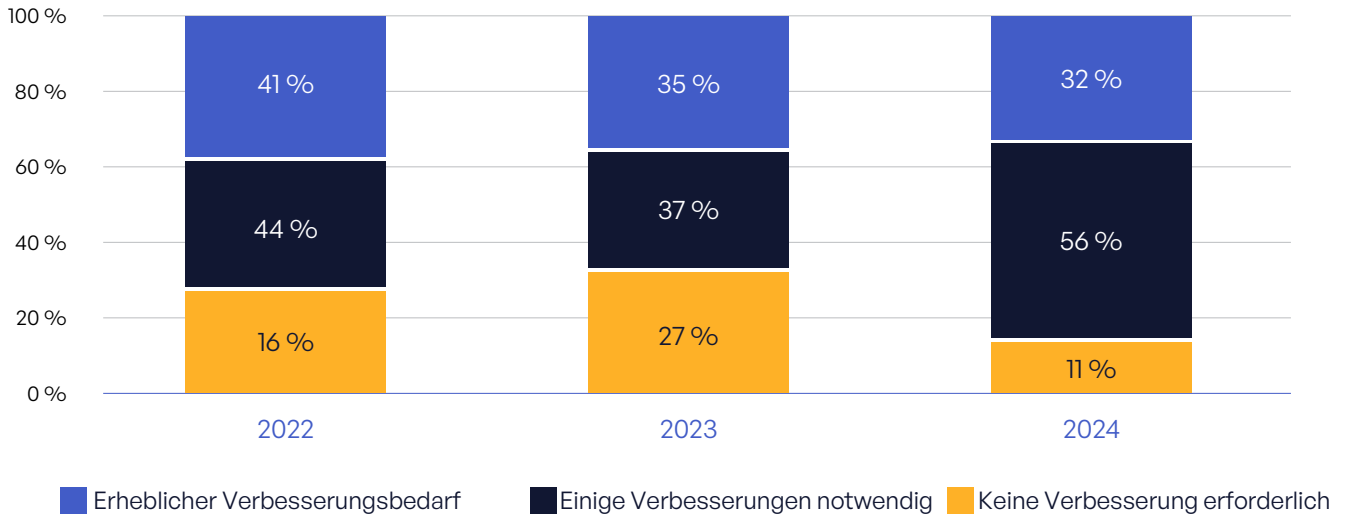


Abb. 22: Verbesserungsbedarf bei der Messung und Verwaltung von Compliance-Risiken bei der Kommunikation sensibler Inhalte.

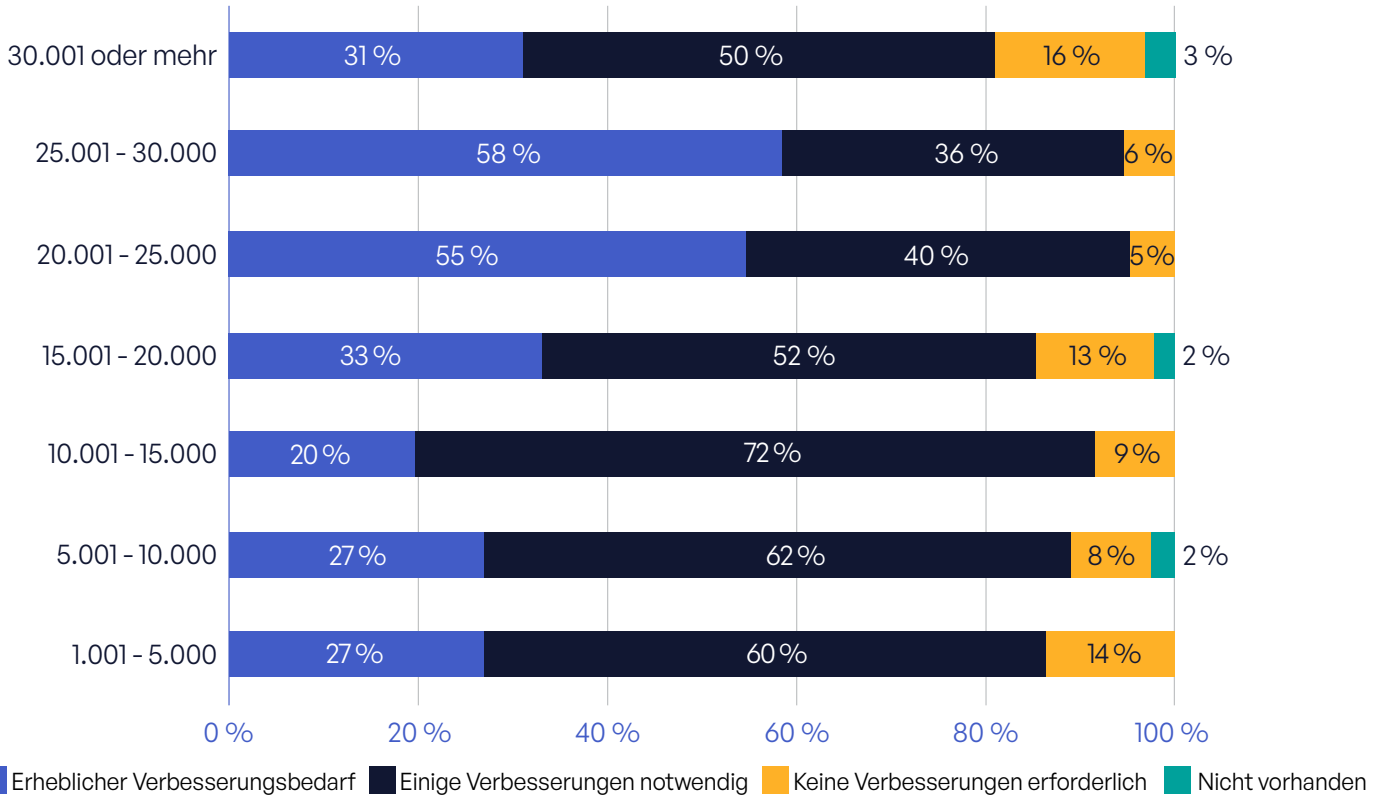


Abb. 23: Verbesserungsbedarf bei der Messung und dem Management des Risikos bei der Kommunikation sensibler Inhalte nach Unternehmensgröße.

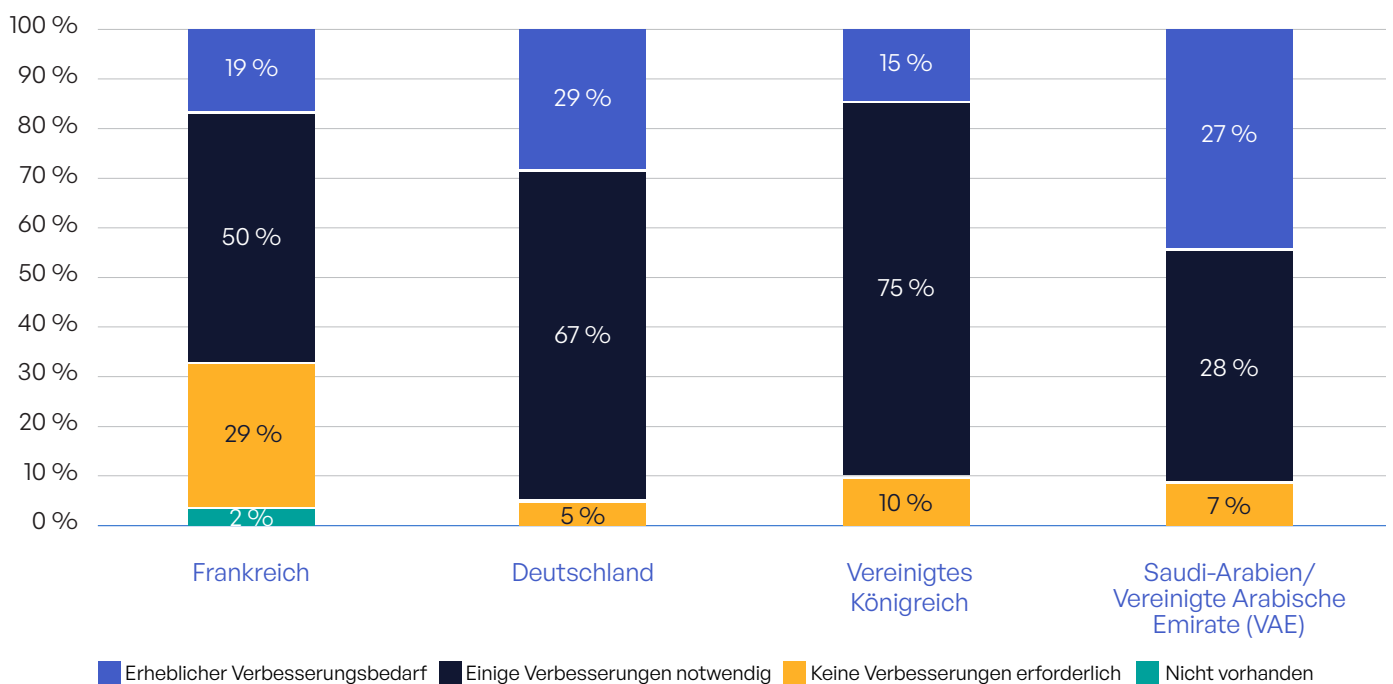


Abb. 24: Verbesserungsbedarf beim Management von Compliance-Risiken bei der Kommunikation sensibler Inhalte nach Ländern.

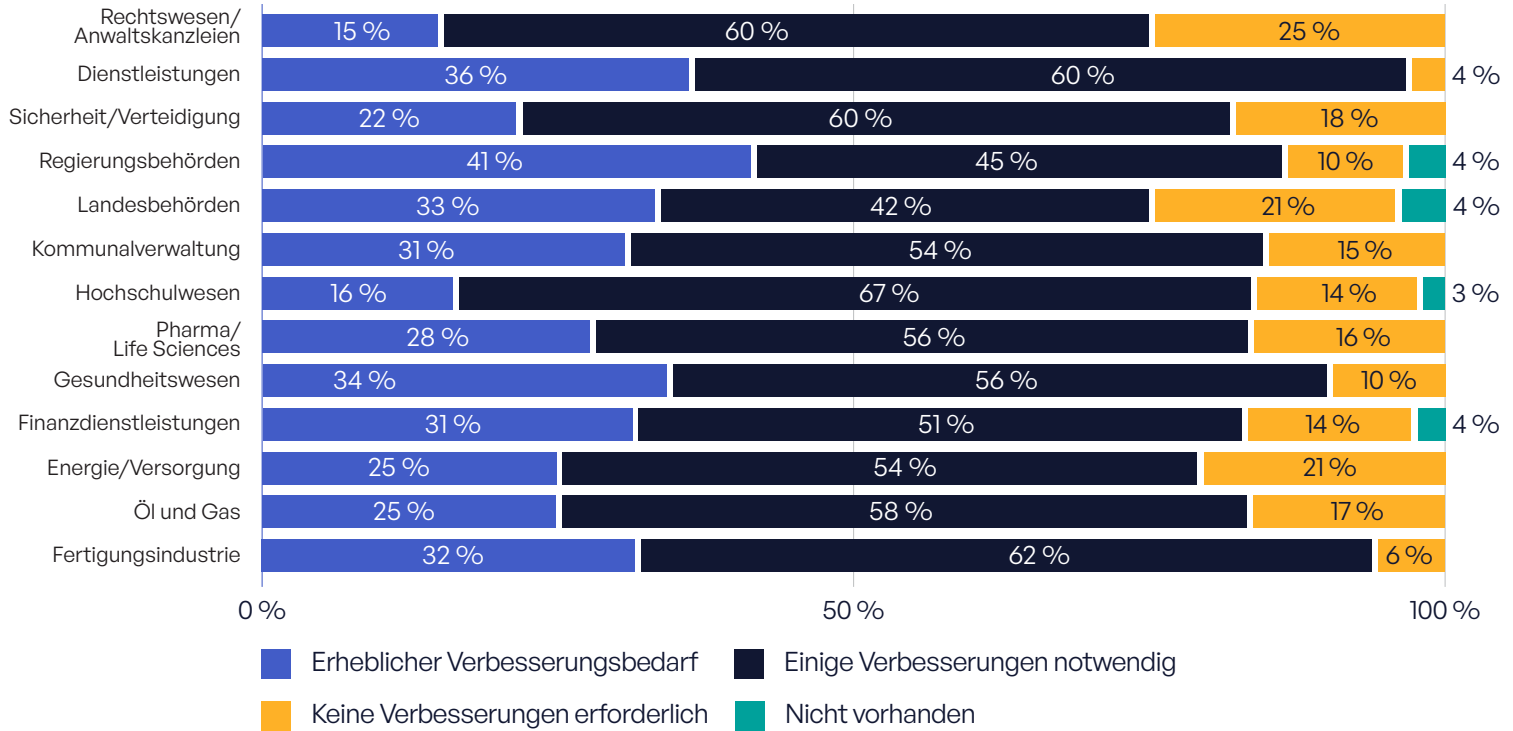


Abb. 25: Verbesserungsbedarf beim Management von Compliance-Risiken bei der Kommunikation sensibler Inhalte nach Branchen.

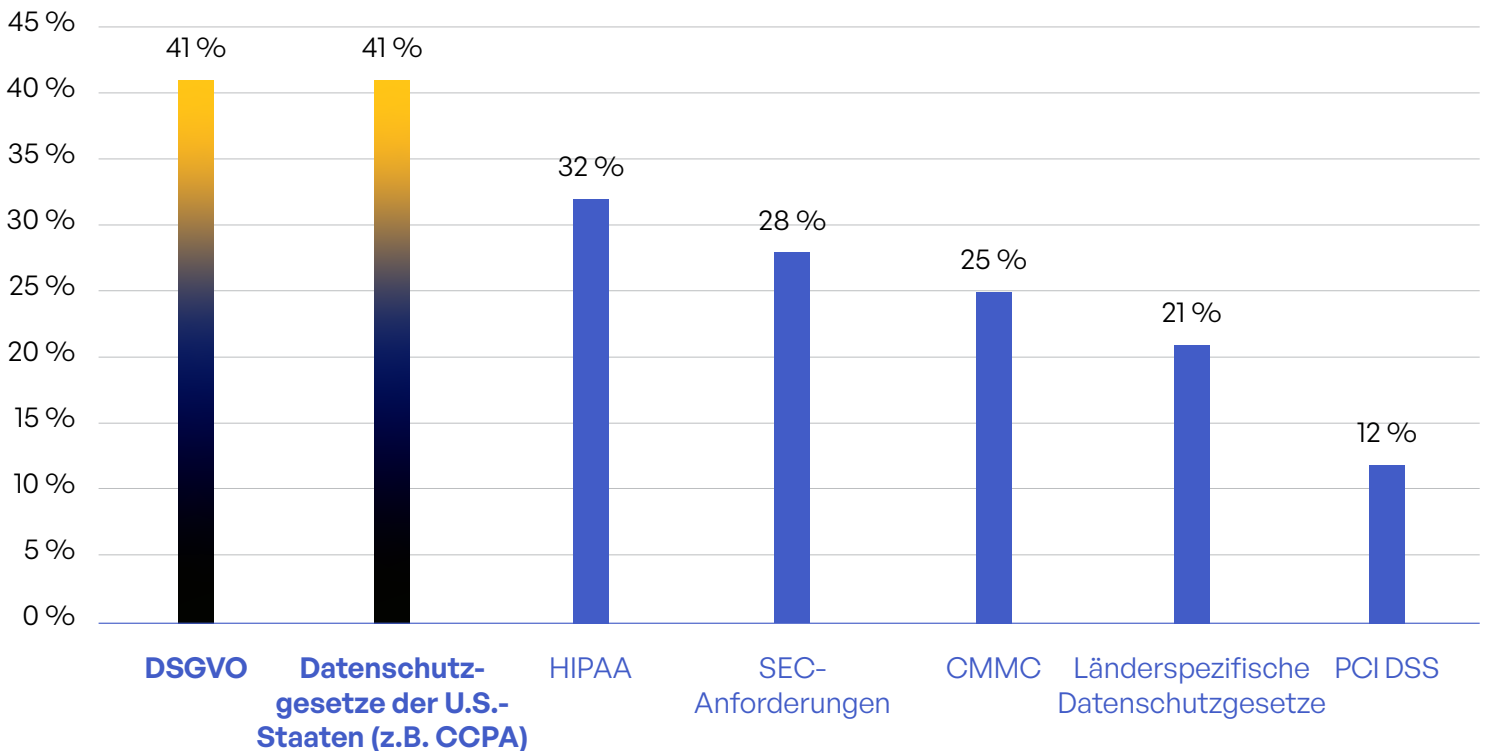


Abb. 26: Schwerpunktbereiche für Datenschutz und Compliance.

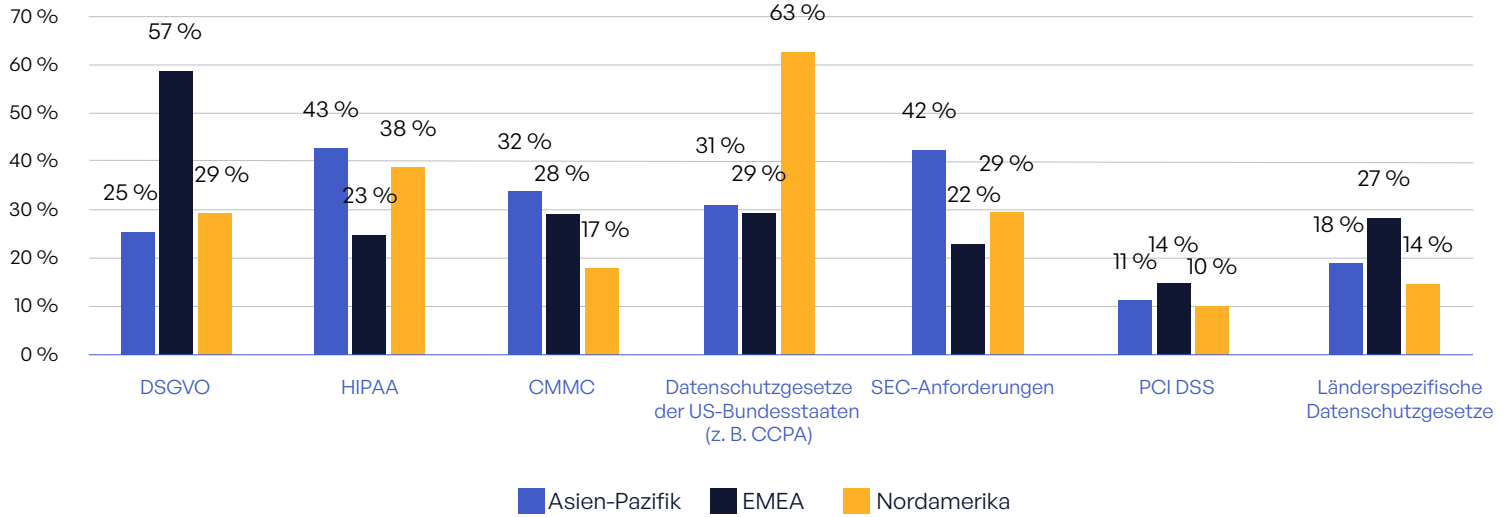


Abb. 27: Wichtigste Prioritäten im Bereich Datenschutz und Compliance nach Regionen.

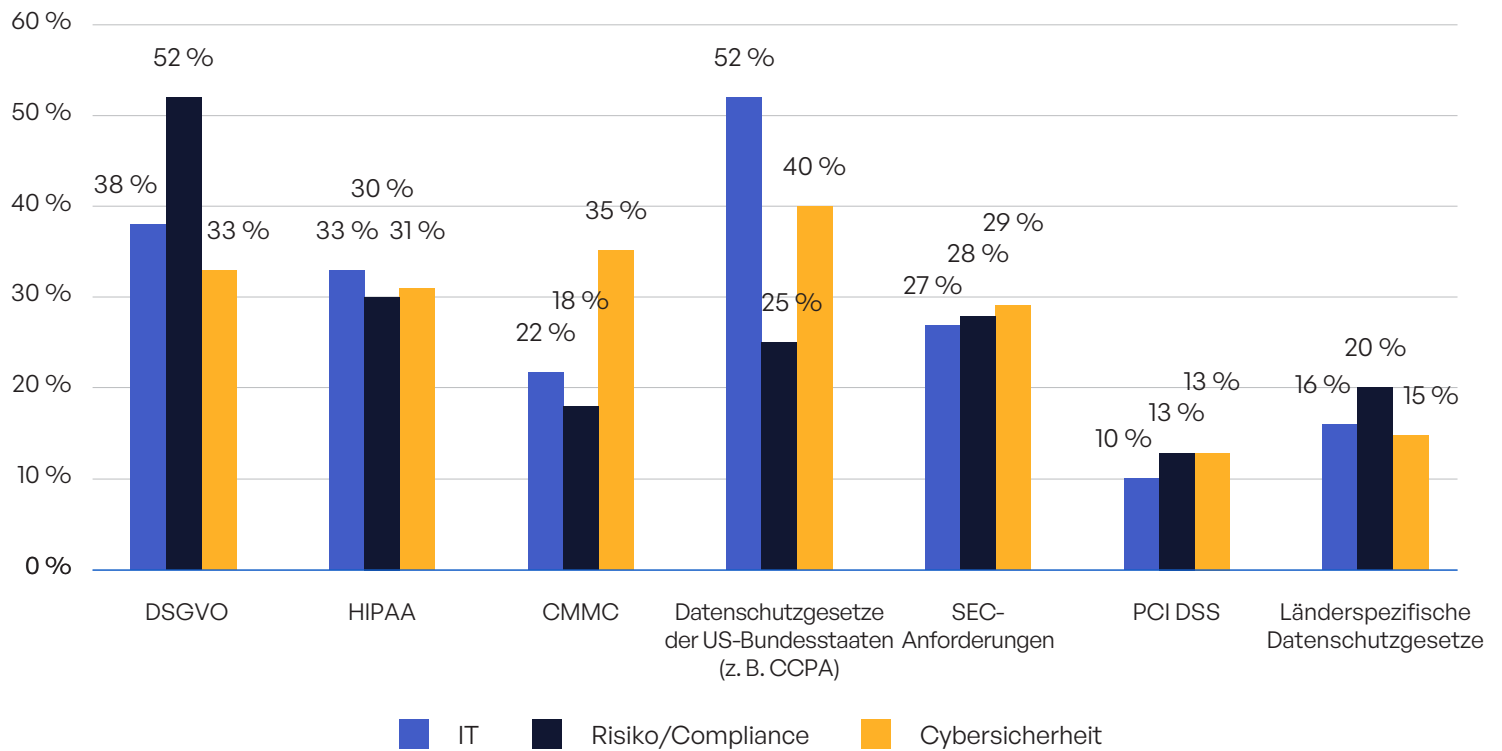


Abb. 28: Wichtigste Prioritäten im Bereich Datenschutz und Compliance nach Job-Funktionen.

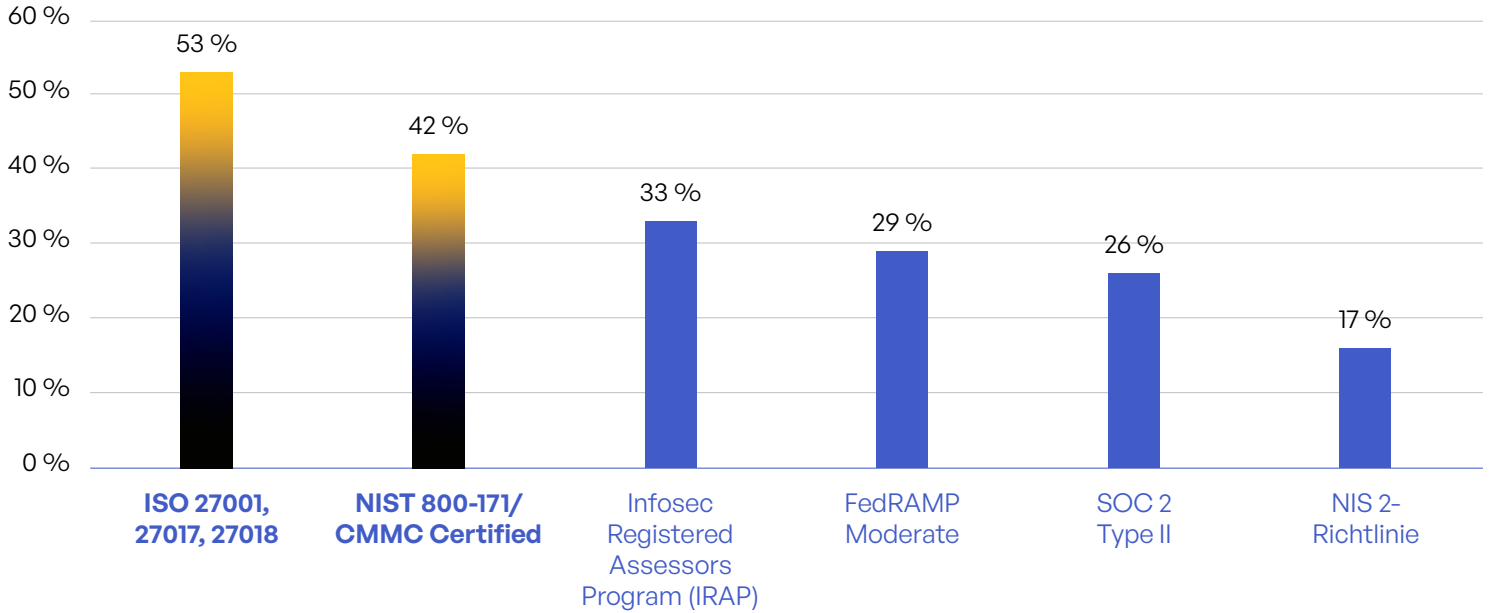


Abb. 29: Wichtigste Zertifizierungen und Validierungen im Bereich Sicherheit (Top 2 Prioritäten).

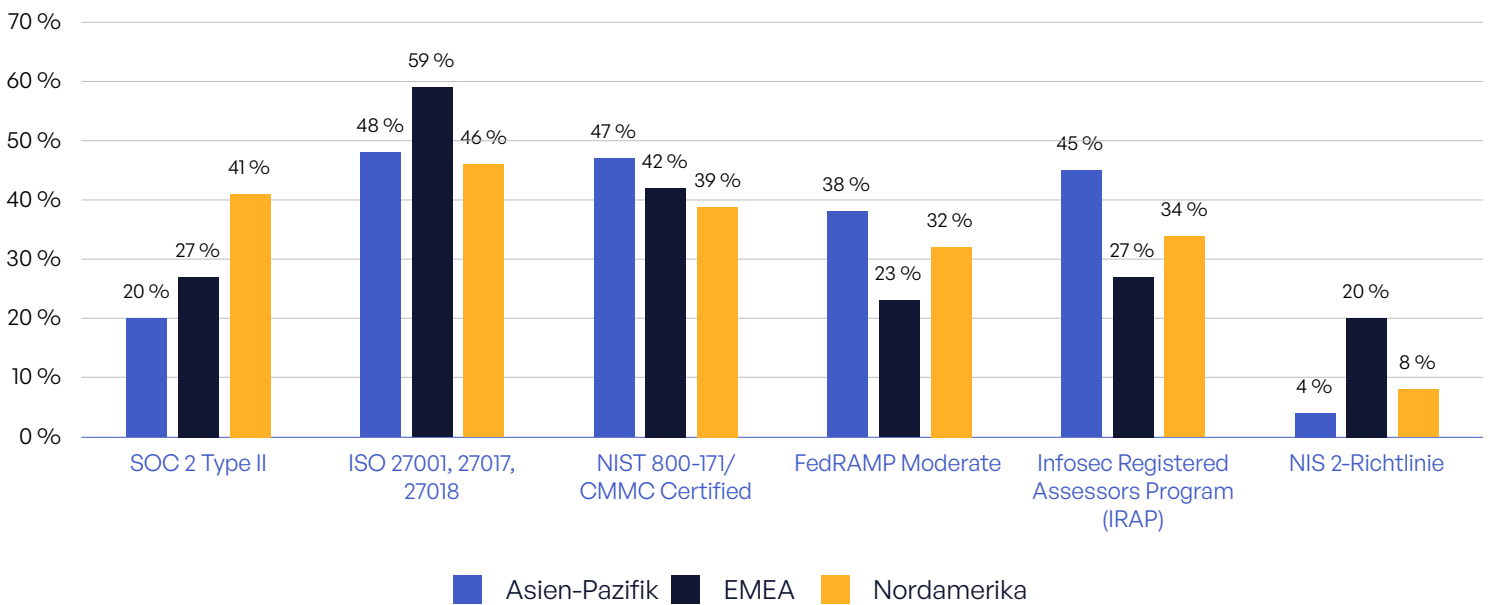


Abb. 30: Wichtigste Prioritäten in Bezug auf die Sicherheitsstandards nach Regionen.

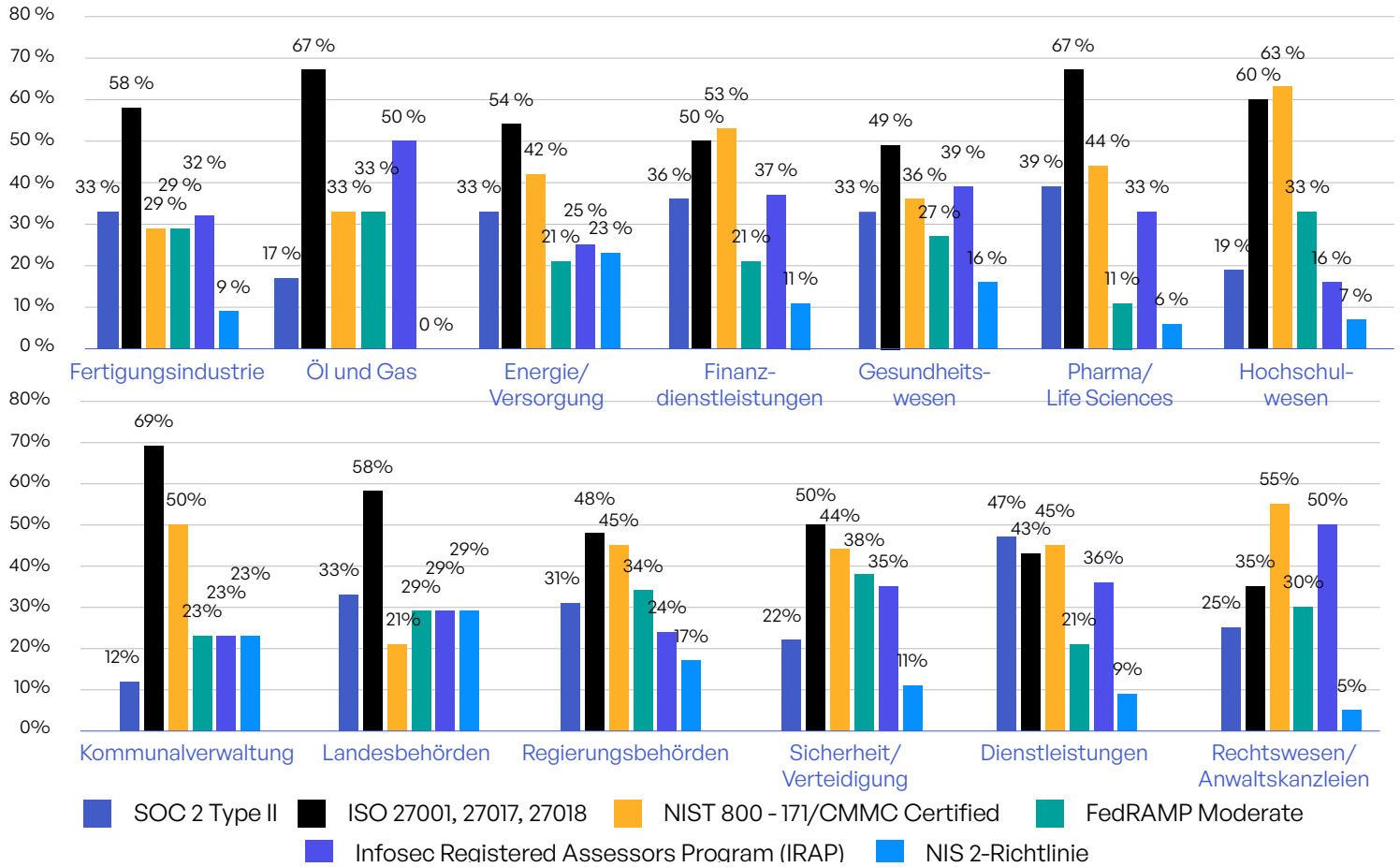


Abb. 31: Wichtigste Prioritäten bei den Sicherheitsstandards nach Branchen.

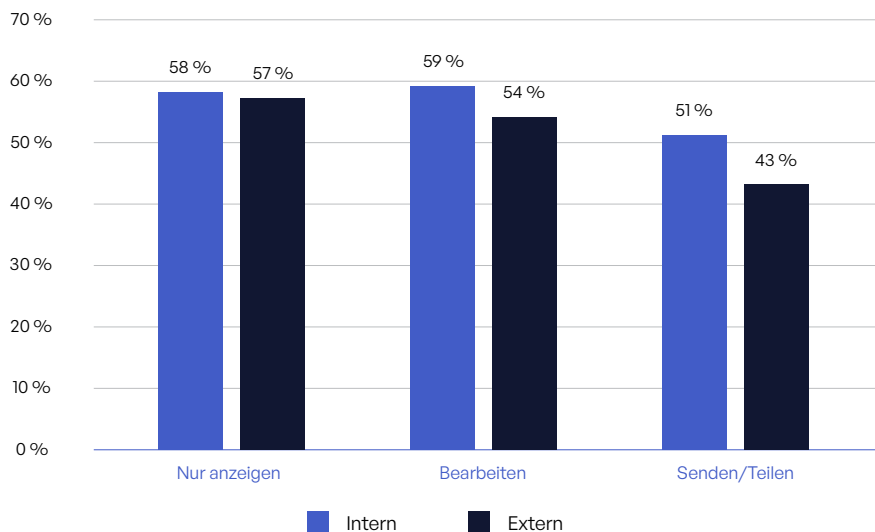


Abb. 32: Nachverfolgung, Kontrolle und Dokumentation der Freigabe und des Versands sensibler Inhalte.

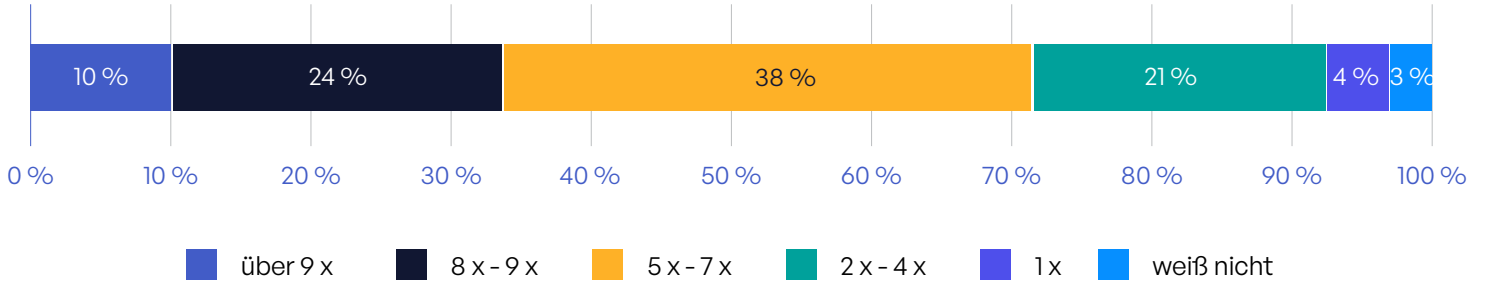


Abb. 33: Jährlicher Bedarf an Audit-Protokollen für Compliance.

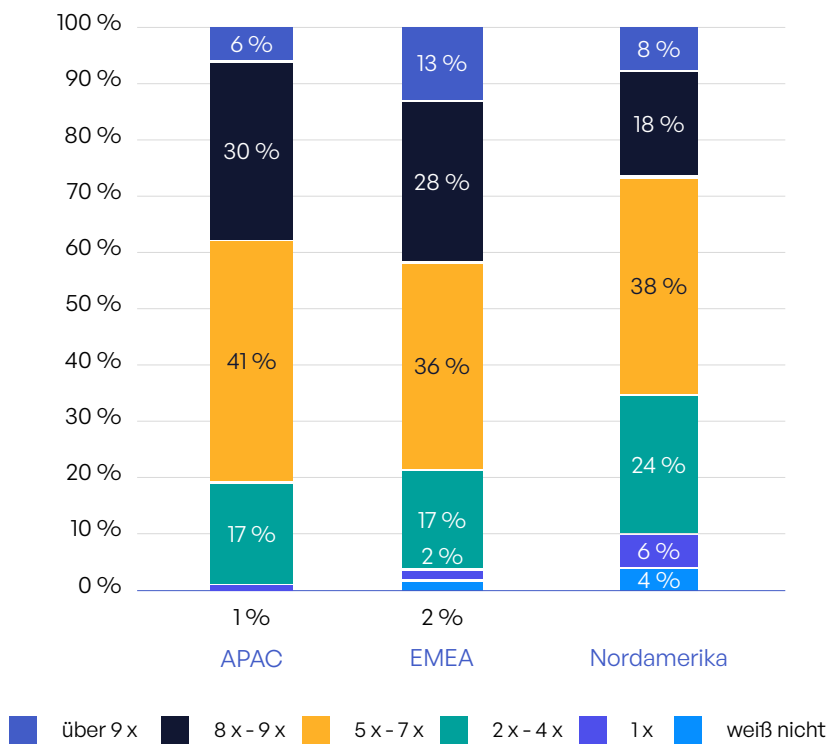


Abb. 34: Jährlicher Bedarf an Audit-Protokollen nach Region.

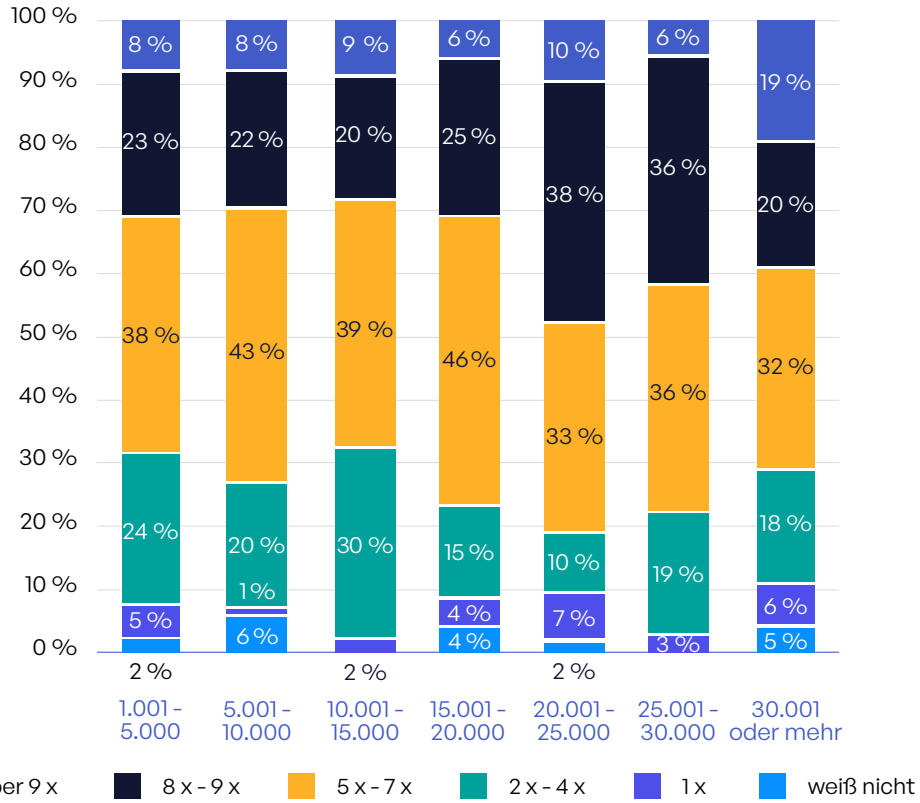


Abb. 35: Jährlicher Bedarf an Audit-Protokollen für Compliance nach Unternehmensgröße.

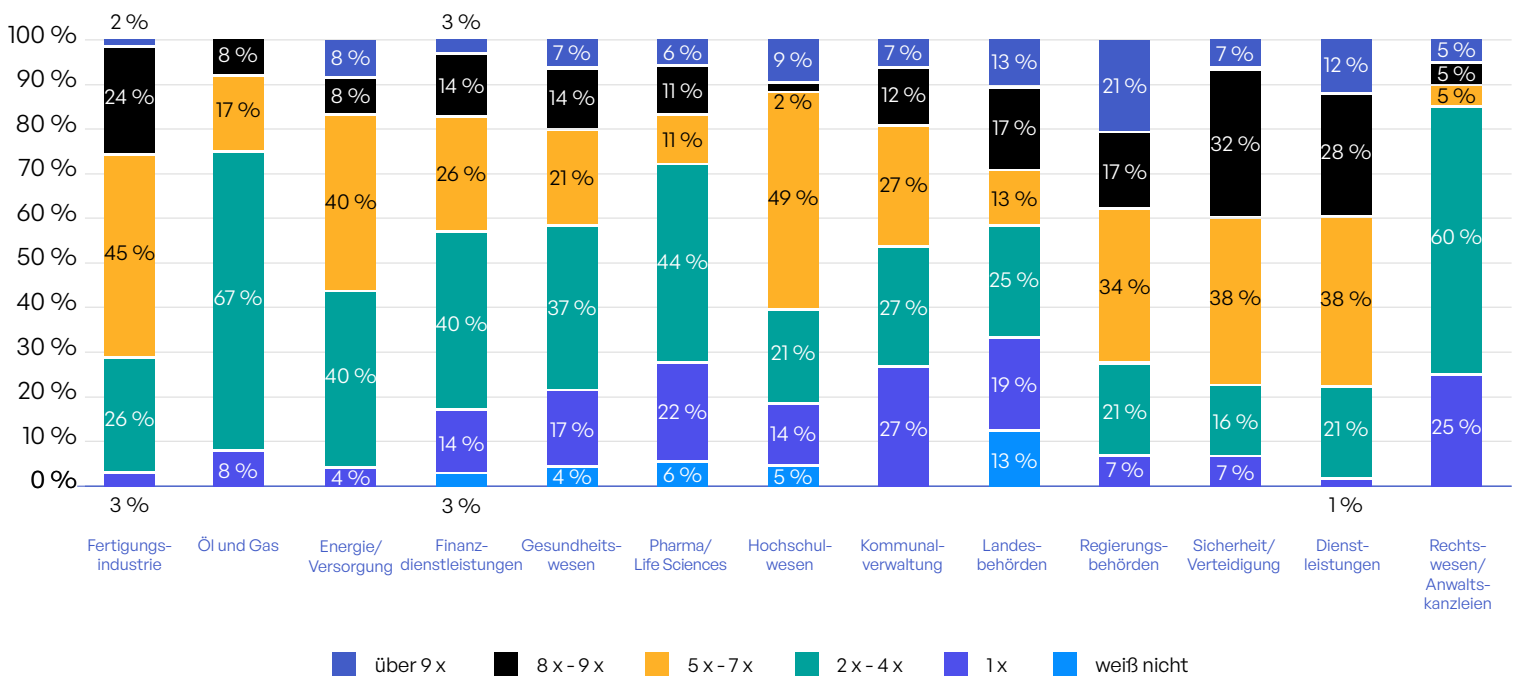


Abb. 36: Jährlicher Bedarf an Audit-Protokollen für Compliance nach Branche.

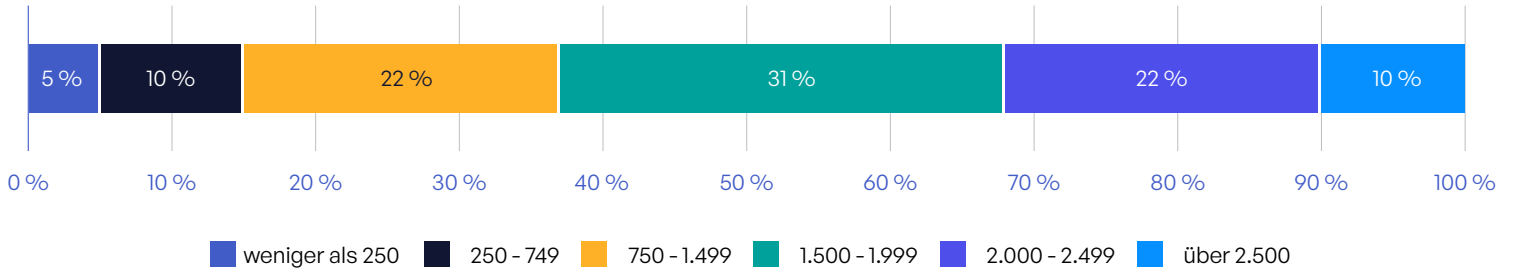


Abb. 37: Jährlicher Aufwand an Arbeitsstunden für Compliance-Audit-Berichte.

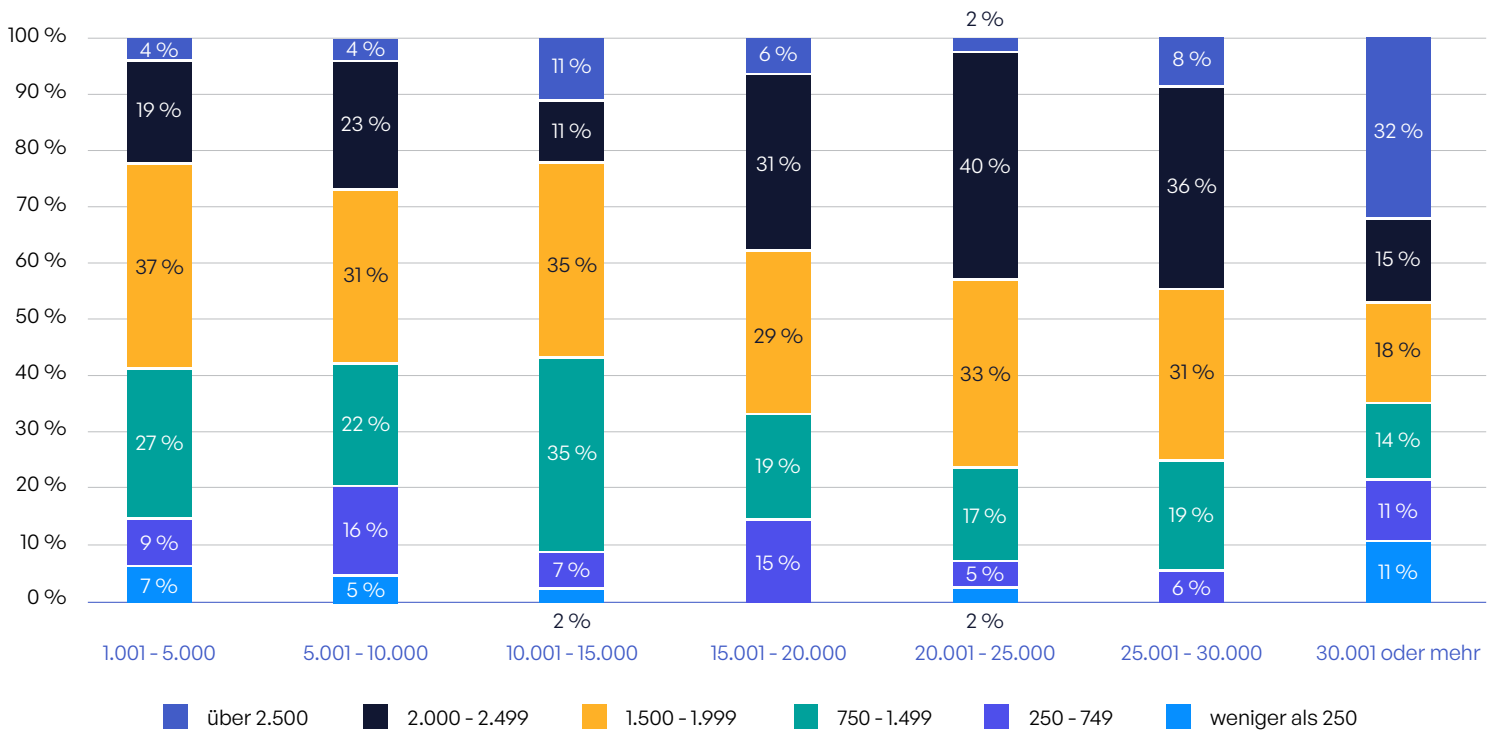


Abb. 38: Jährlicher Aufwand an Arbeitsstunden für die Erstellung von Compliance-Berichten nach Unternehmensgröße.

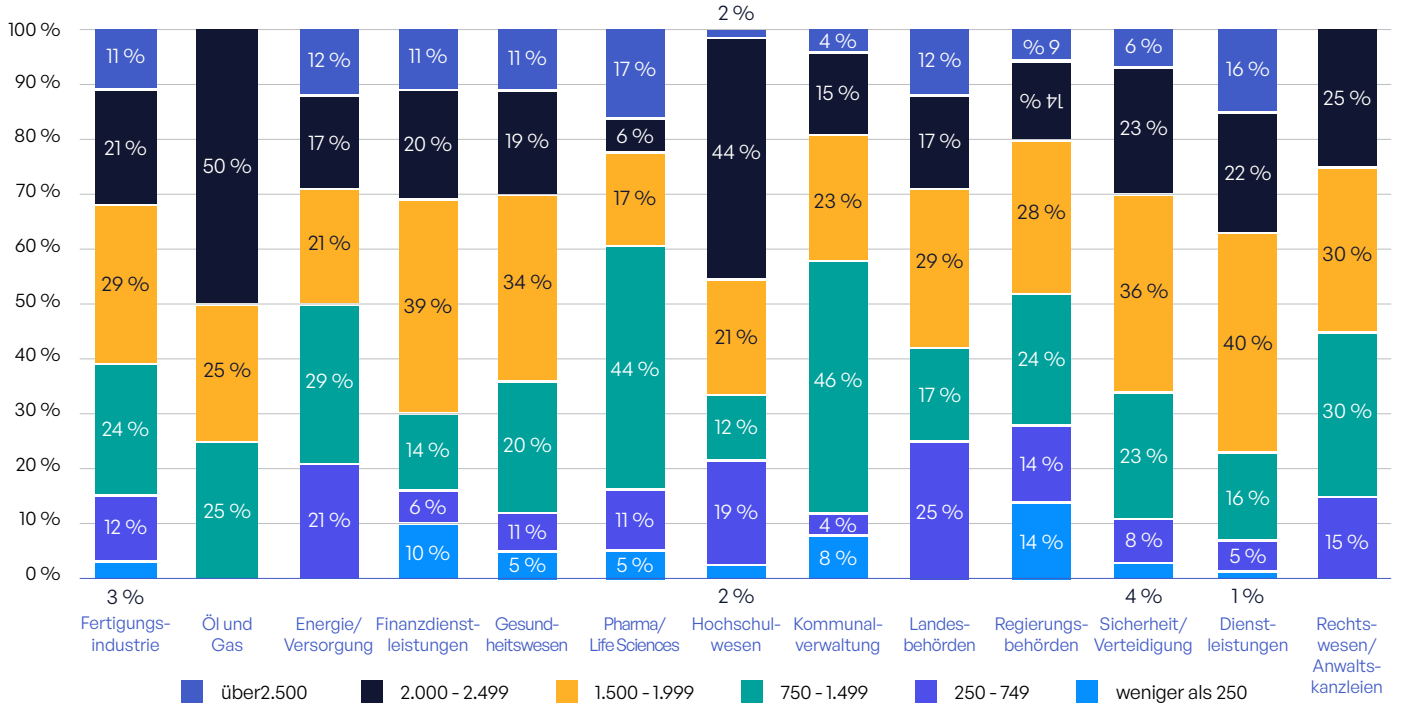


Abb. 39: Jährlicher Aufwand an Arbeitsstunden für die Erstellung von Compliance-Berichten nach Branchen.

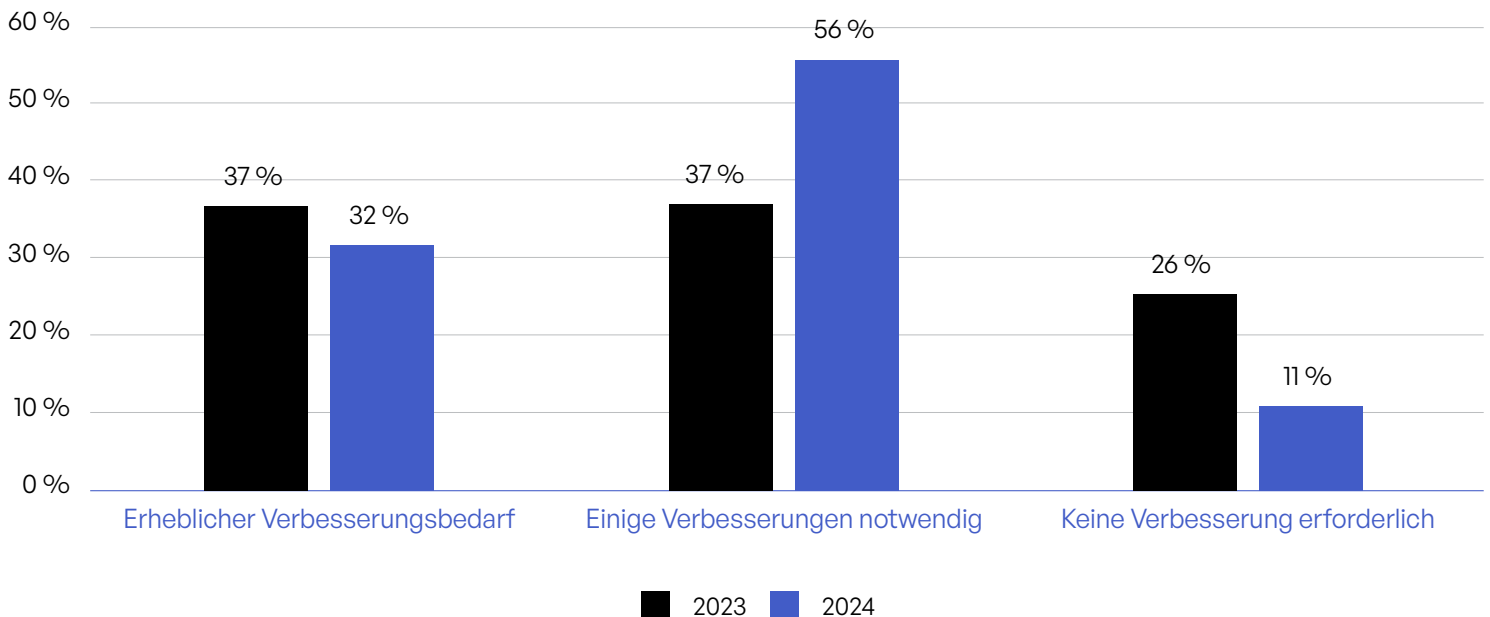


Abb. 40: Verbesserungsbedarf beim Management der Sicherheit sensibler Inhalte.

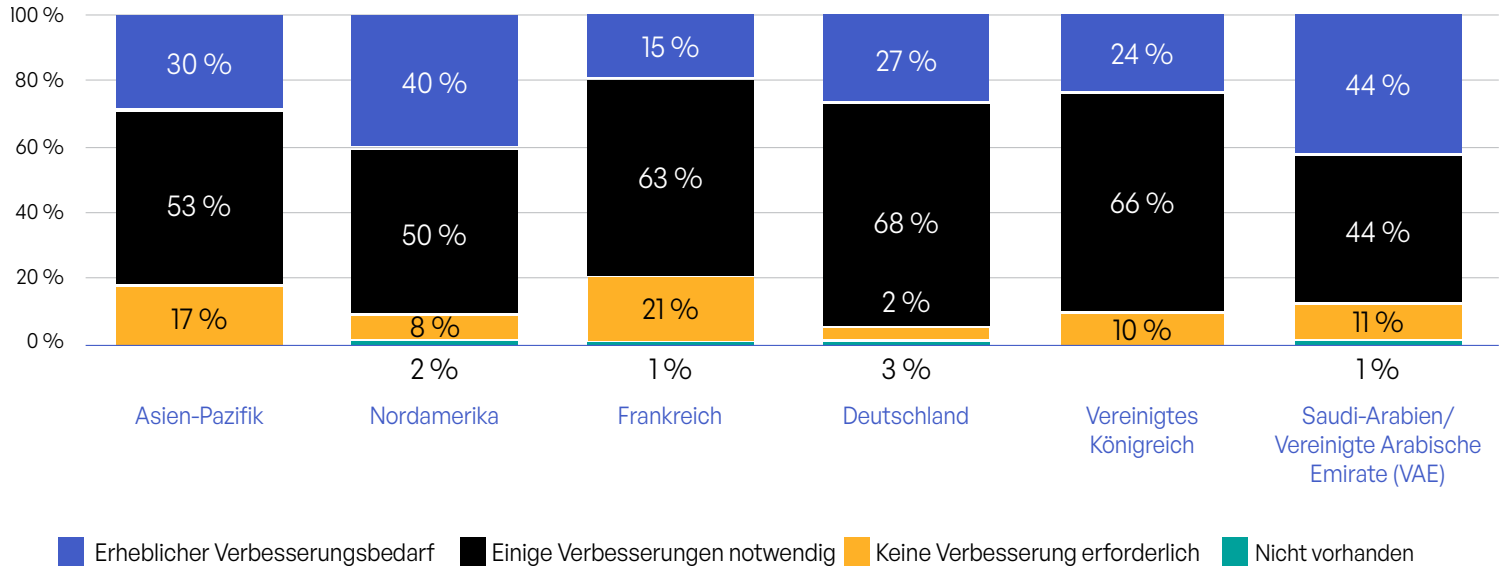


Abb. 41: Verbesserungsbedarf beim Management der Sicherheit sensibler Inhalte in verschiedenen Regionen und EMEA-Ländern.

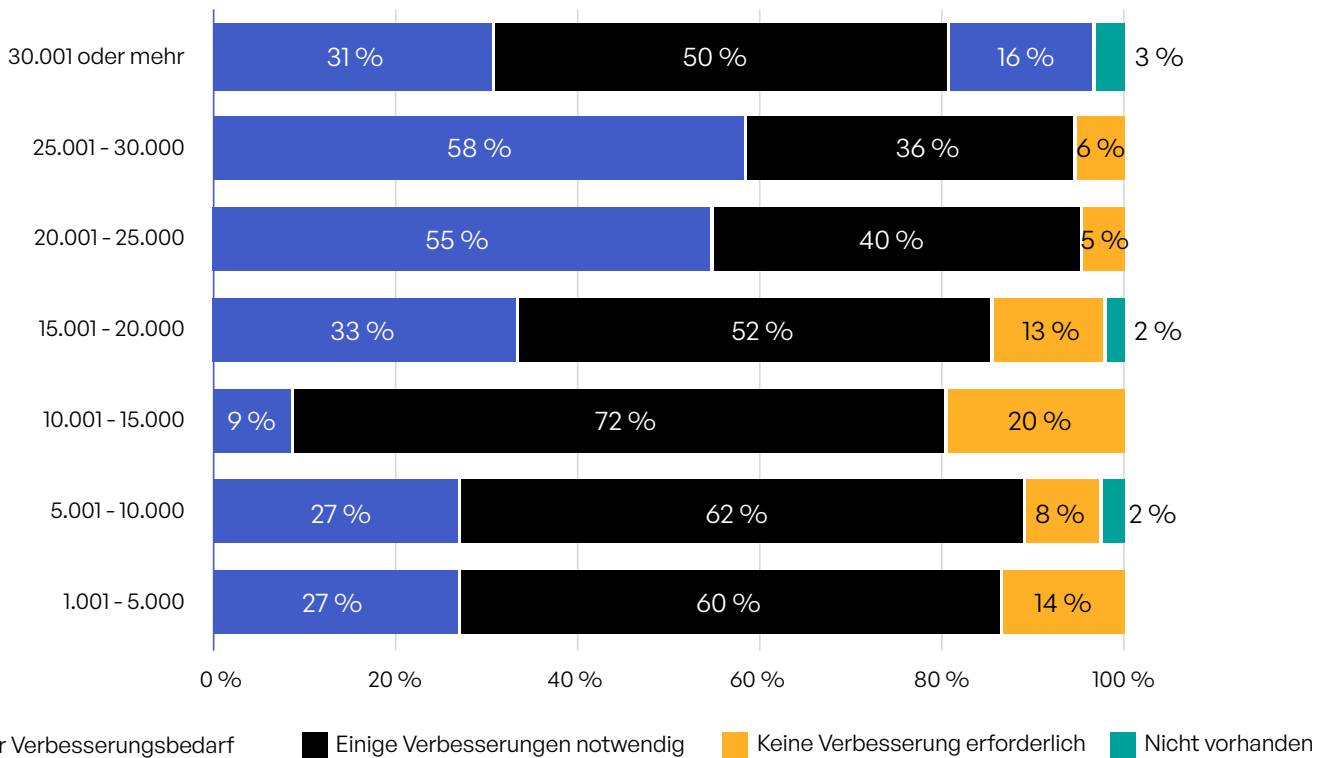


Abb. 42: Verbesserungsbedarf bei der Sicherheit sensibler Inhalte nach Unternehmensgröße.

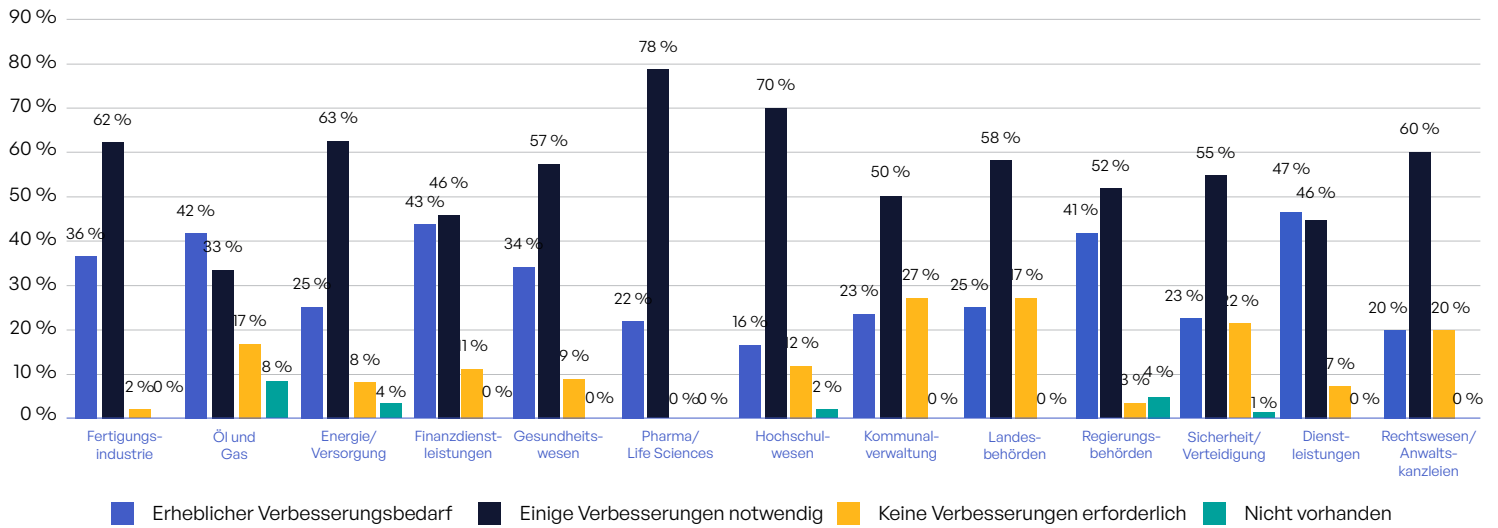


Abb. 43: Verbesserungsbedarf bei der Sicherheit sensibler Inhalte nach Branchen.

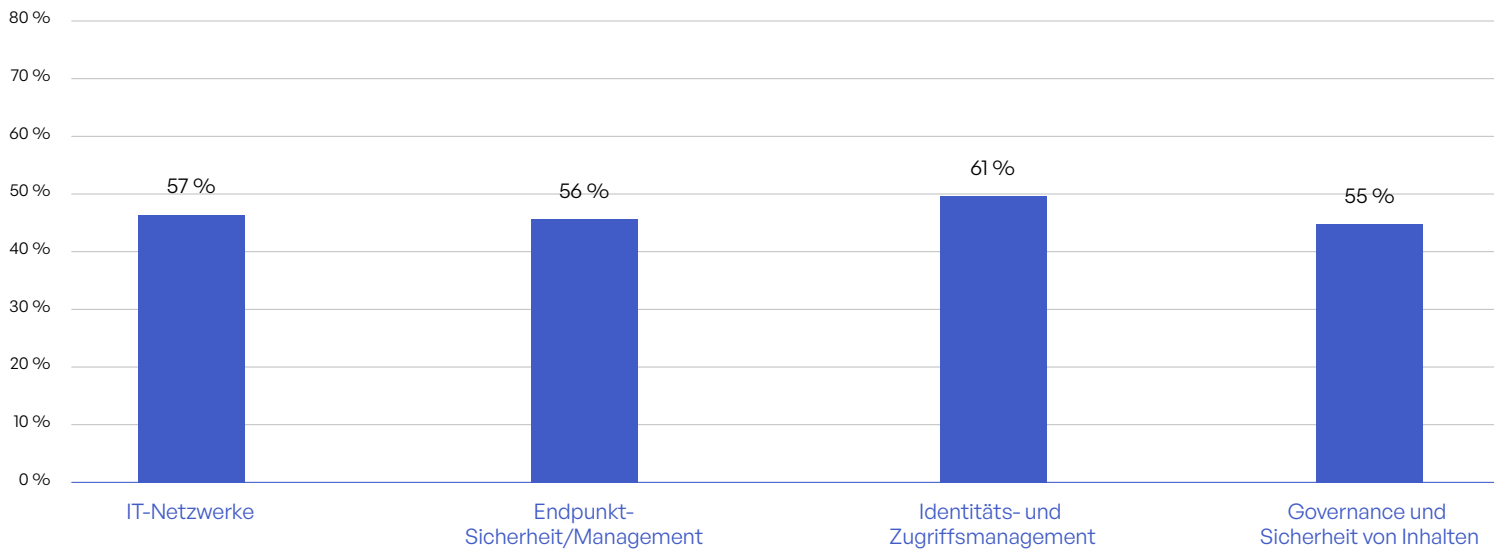


Abb. 44: Bereiche, in denen Zero Trust erreicht wurde.

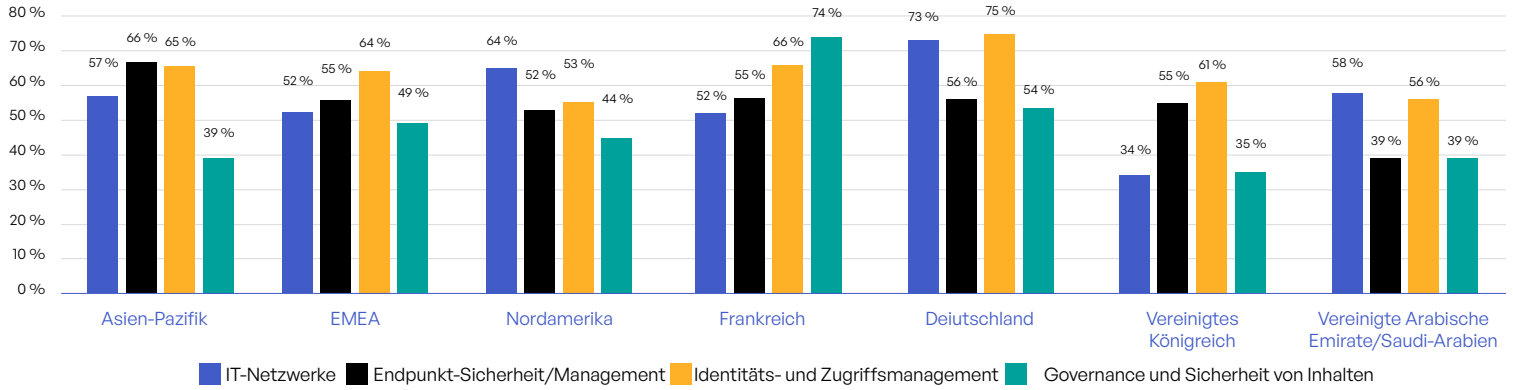


Abb. 45: Zero Trust nach Regionen und EMEA-Ländern.

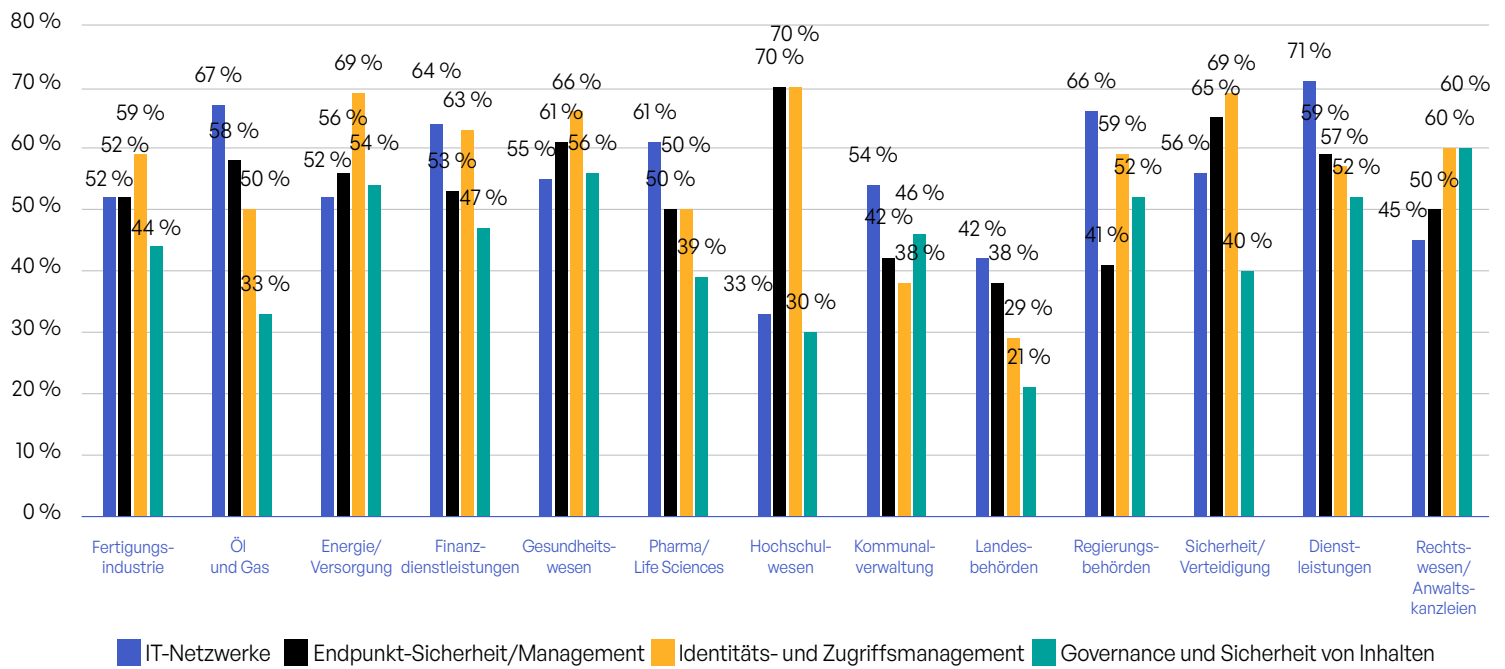


Abb. 46: Bereiche, in denen Zero Trust erreicht wurde, nach Branchen.

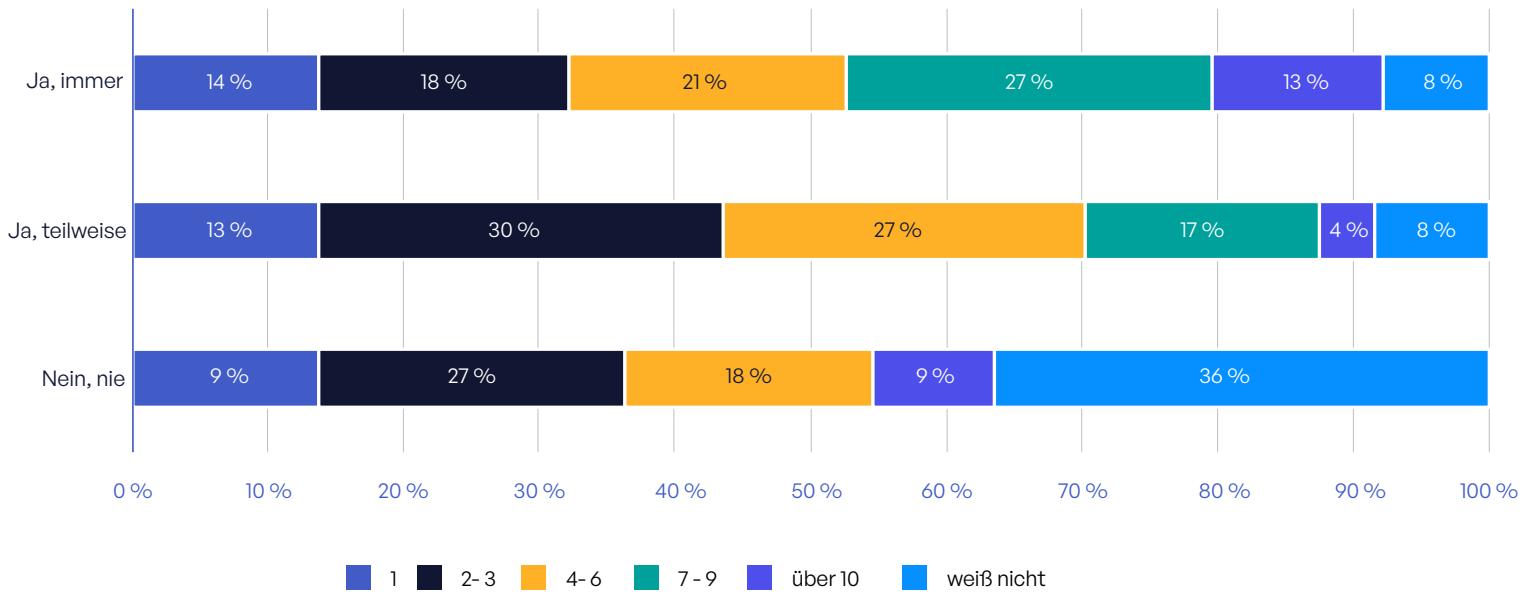


Abb. 47: Erweiterte Sicherheit bei der Kommunikation sensibler Inhalte und Anzahl der Datenschutzverletzungen.

	Fertigungsindustrie	Öl und Gas	Energie/Versorgung	Finanzdienstleistungen	Gesundheitswesen	Pharma/Life Sciences	Hochschulwesen	Kommunalverwaltung	Landesbehörden	Regierungsbehörden	Sicherheit/Verteidigung	Dienstleistungen	Rechtswesen/Anwaltskanzleien
Ja, immer	58 %	58 %	58 %	60 %	56 %	61 %	65 %	50 %	71 %	52 %	55 %	71 %	45 %
Ja, teilweise	42 %	42 %	40 %	36 %	44 %	39 %	28 %	50 %	25 %	45 %	45 %	28 %	50 %
Nein, nie	0 %	0 %	2 %	4 %	0 %	0 %	7 %	0 %	4 %	3 %	0 %	2 %	5 %

Abb. 48: Einsatz erweiterter Sicherheit für die Kommunikation sensibler Inhalte nach Branchen.

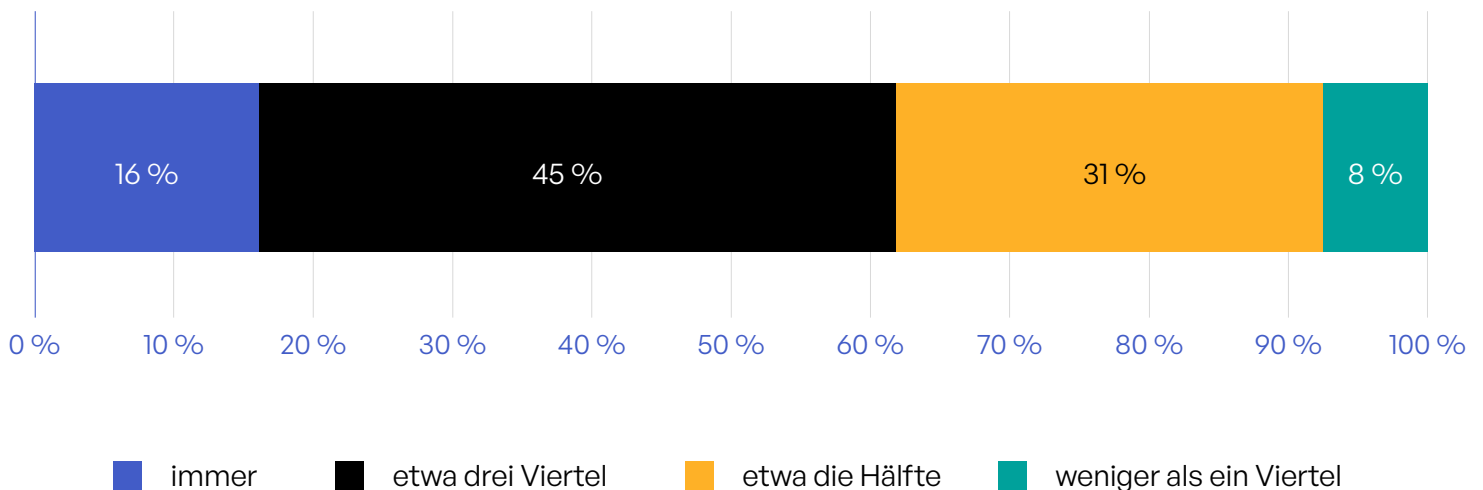


Abb. 49: Nachverfolgung und Kontrolle sensibler Inhalte nach Verlassen einer Anwendung.

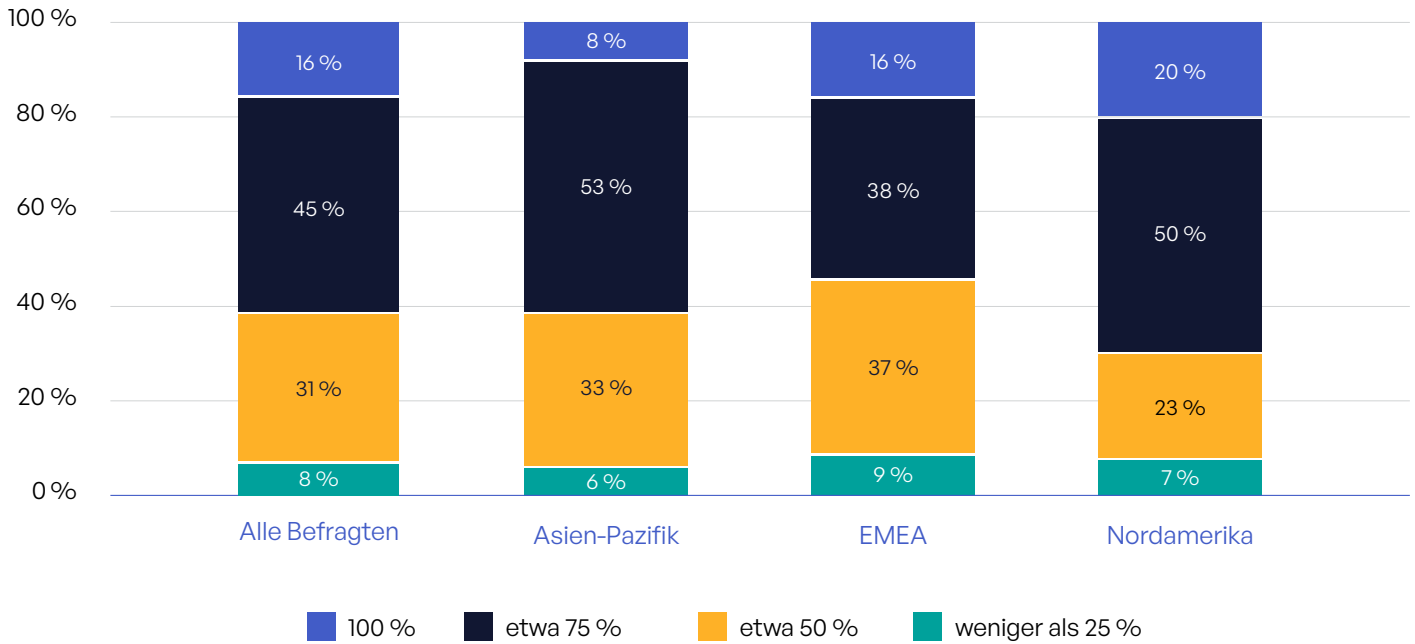


Abb. 50: Wie oft Unternehmen den Zugriff auf Kommunikation mit sensiblen Inhalten nachverfolgen und kontrollieren können nach Region.

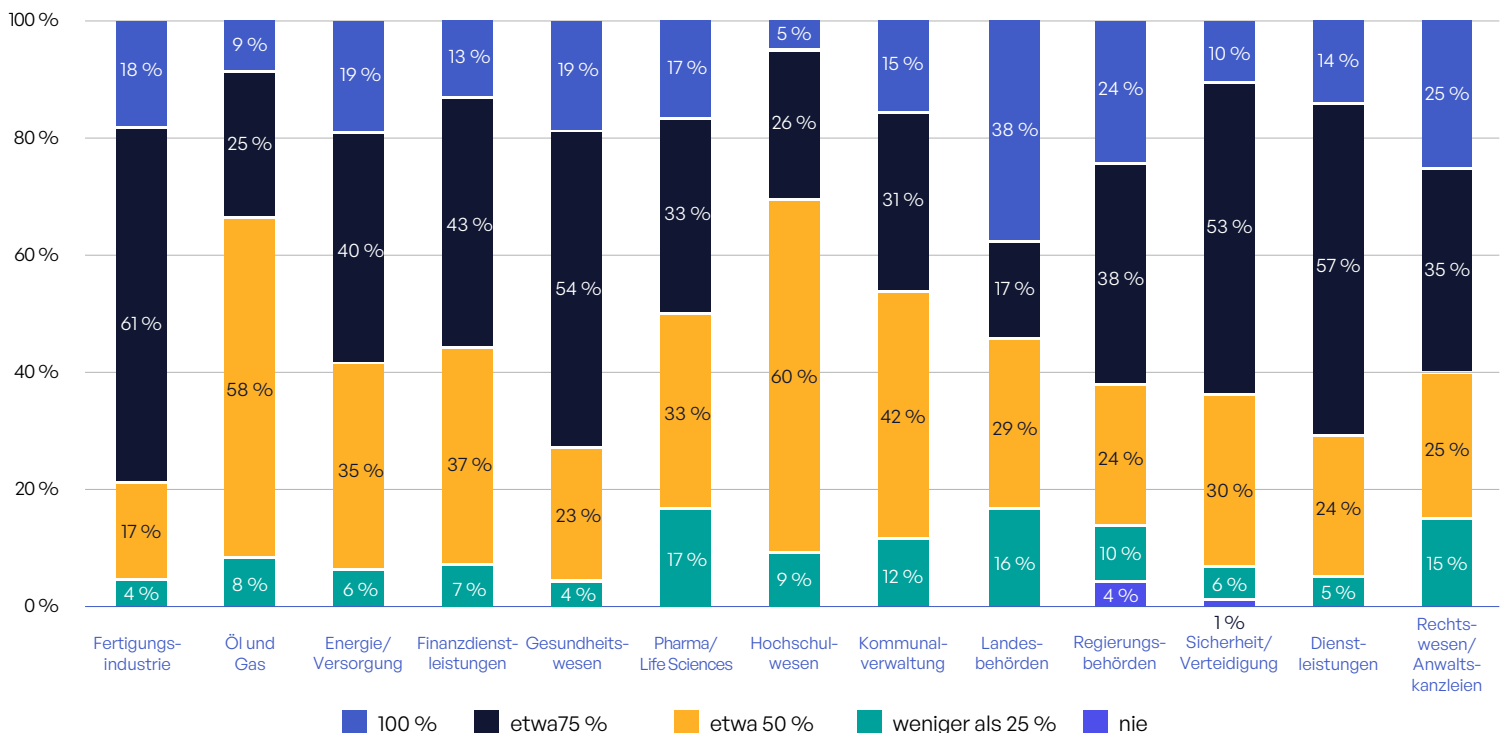


Abb. 51: Wie oft Unternehmen den Zugriff auf Kommunikation mit sensiblen Inhalten nachverfolgen und kontrollieren können nach Branchen.

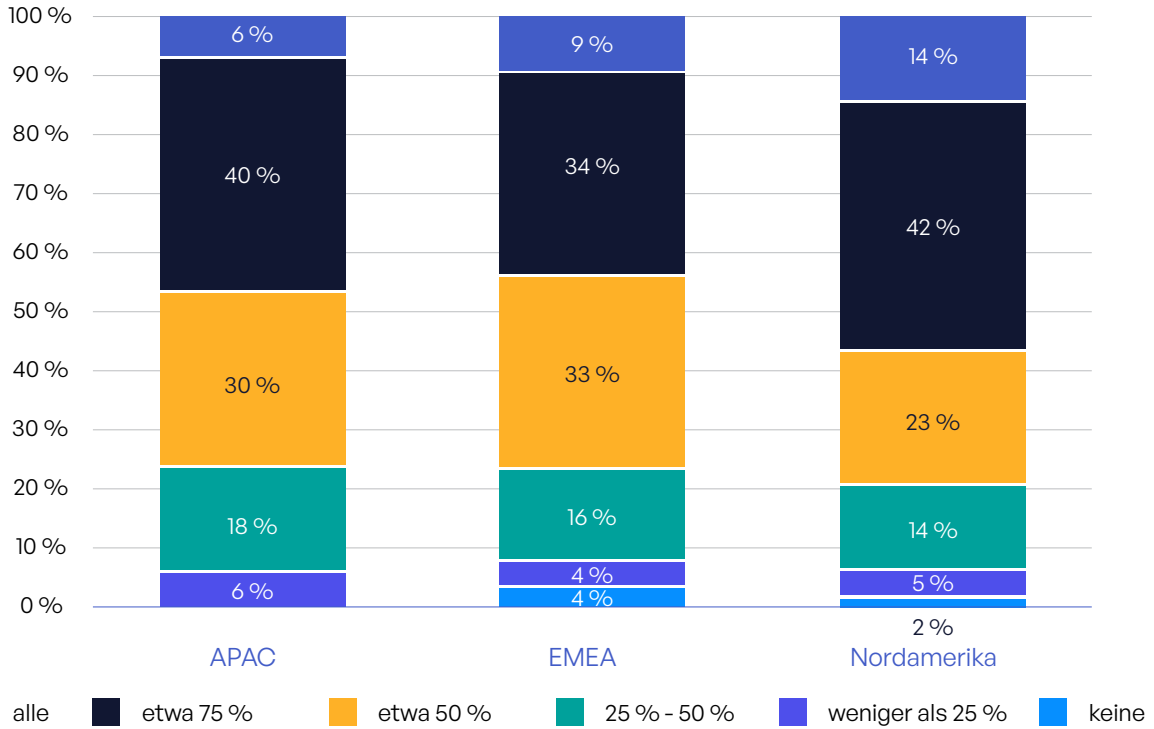


Abb. 52: Unstrukturierte Daten, die gekennzeichnet und klassifiziert sind, nach Regionen.

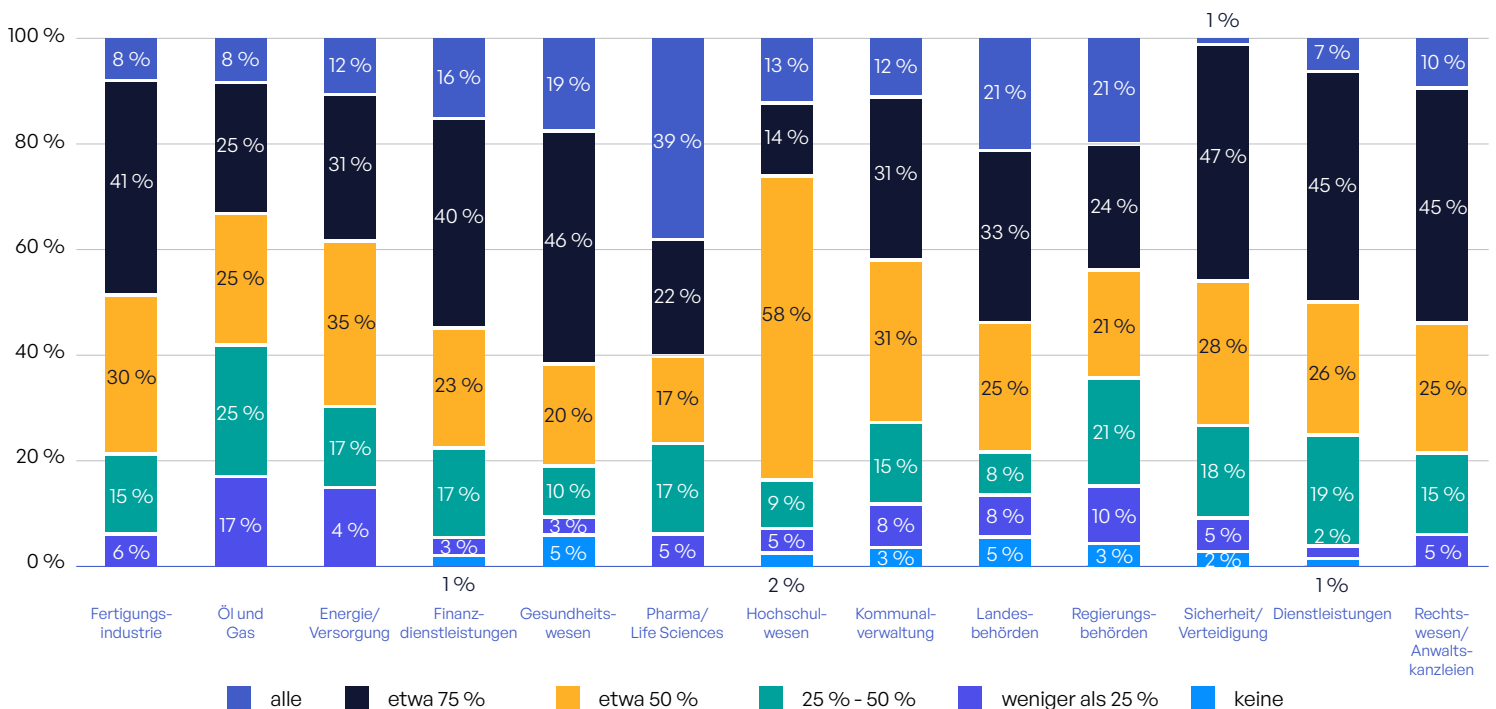


Abb. 53: Unstrukturierte Daten, die gekennzeichnet und klassifiziert sind, nach Branchen.

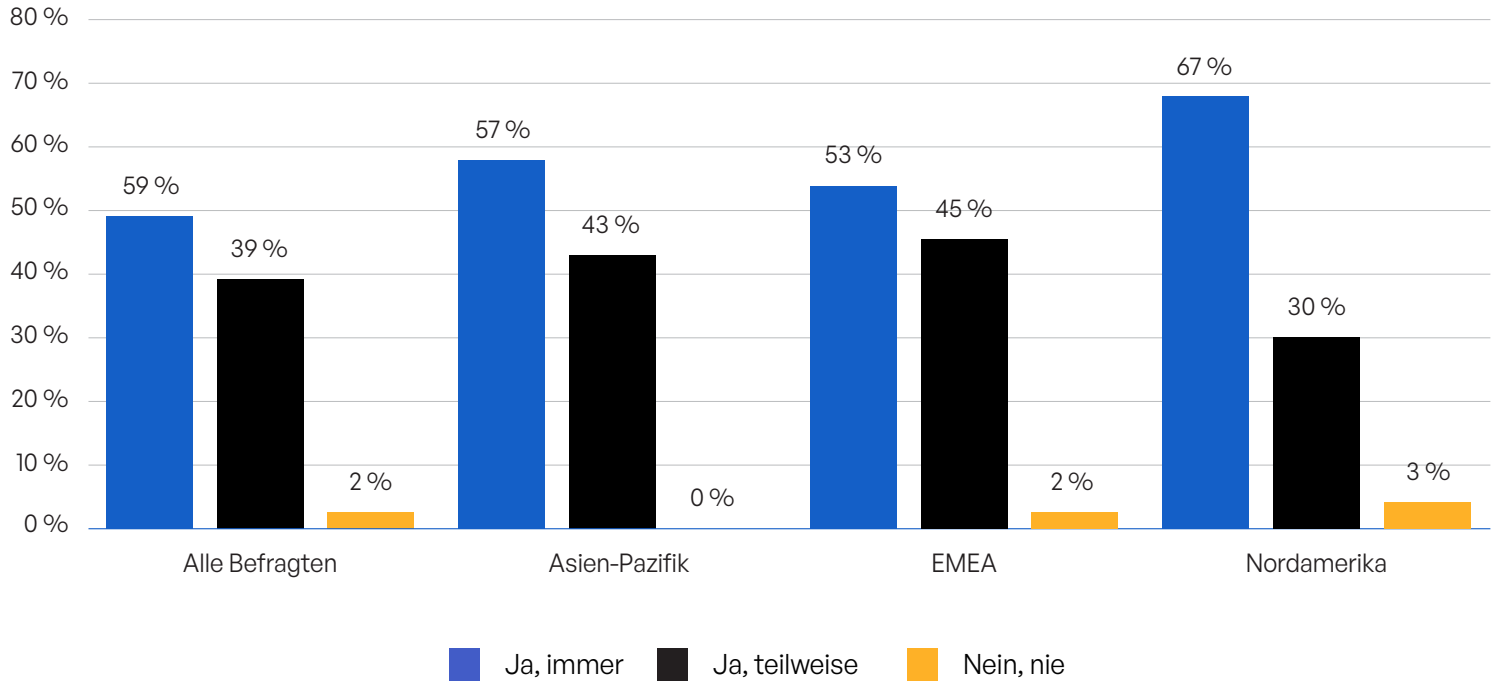


Figure 54: Erweiterte Sicherheit bei der Kommunikation sensibler Inhalte nach Regionen.

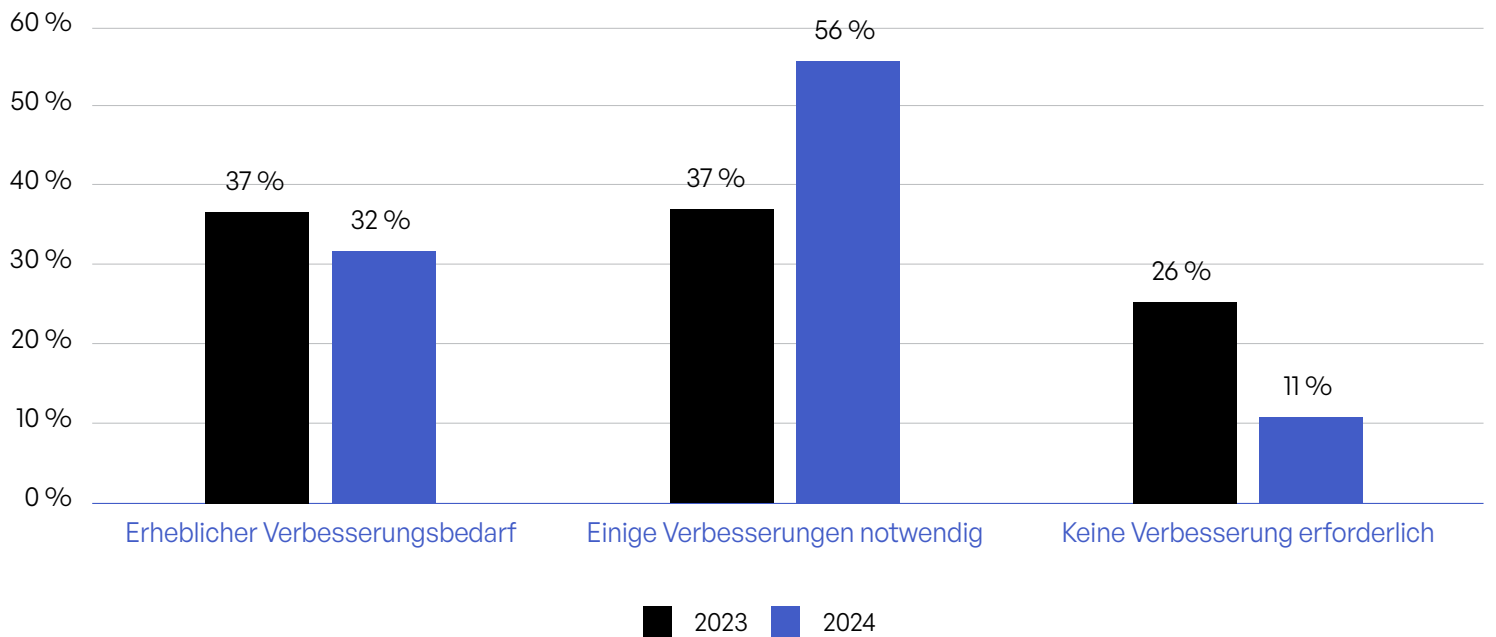


Abb. 55: Verbesserungsbedarf beim Risikomanagement der Kommunikation sensibler Inhalte.

		Alle Befragten	Fertigungs- industrie	Öl und Gas	Energie/ Versorgung	Finanzdienst- leistungen	Gesundheits- wesen	Pharma/ Life Sciences	Hochschul- wesen
Intern	Ja, immer	59 %	58 %	58 %	58 %	60 %	56 %	61 %	65 %
	Ja, teilweise	39 %	42 %	42 %	40 %	36 %	44 %	39 %	28 %
	Nein, nie	2 %	0 %	0 %	2 %	4 %	0 %	0 %	7 %
Extern	Ja, immer	59 %	62 %	58 %	44 %	70 %	56 %	78 %	72 %
	Ja, teilweise	38 %	38 %	42 %	52 %	27 %	44 %	22 %	21 %
	Nein, nie	3 %	0 %	0 %	4 %	3 %	0 %	0 %	7 %

		Kommunal- verwaltung	Landes- behörden	Regierungs- behörden	Sicherheit/ Verteidigung	Dienst- leistungen	Rechtswesen/ Anwaltskanzleien
Intern	Ja, immer	50 %	71 %	52 %	55 %	71 %	45 %
	Ja, teilweise	50 %	25 %	45 %	45 %	28 %	50 %
	Nein, nie	0 %	4 %	3 %	0 %	2 %	5 %
Extern	Ja, immer	50 %	67 %	48 %	51 %	60 %	50 %
	Ja, teilweise	38 %	29 %	45 %	48 %	40 %	45 %
	Nein, nie	12 %	4 %	7 %	1 %	0 %	5 %

Abb. 56: Erweiterte Sicherheit bei der Kommunikation sensibler Inhalte nach Branchen.

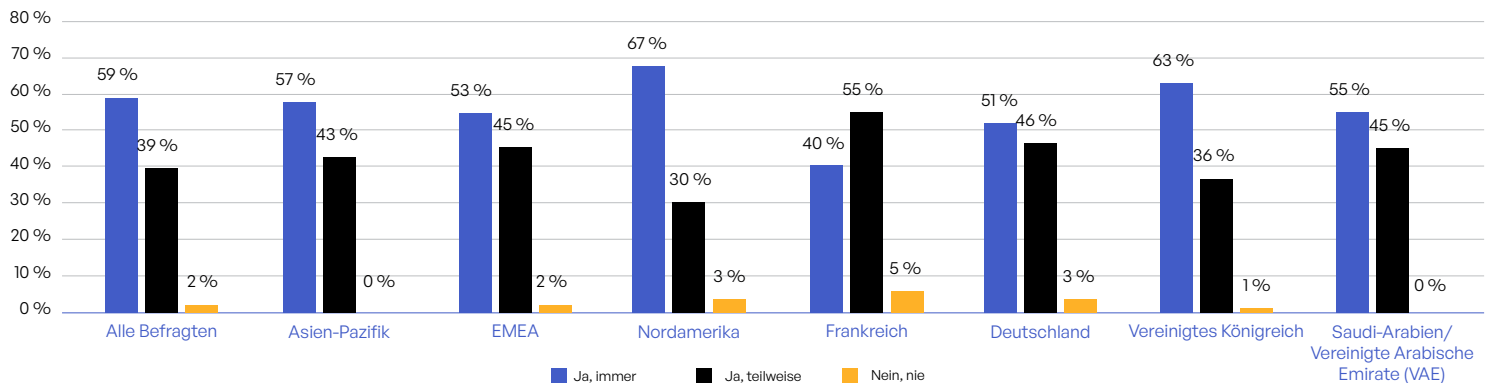


Abb. 57: Erweiterte Sicherheit für die Kommunikation sensibler Inhalte nach Regionen.

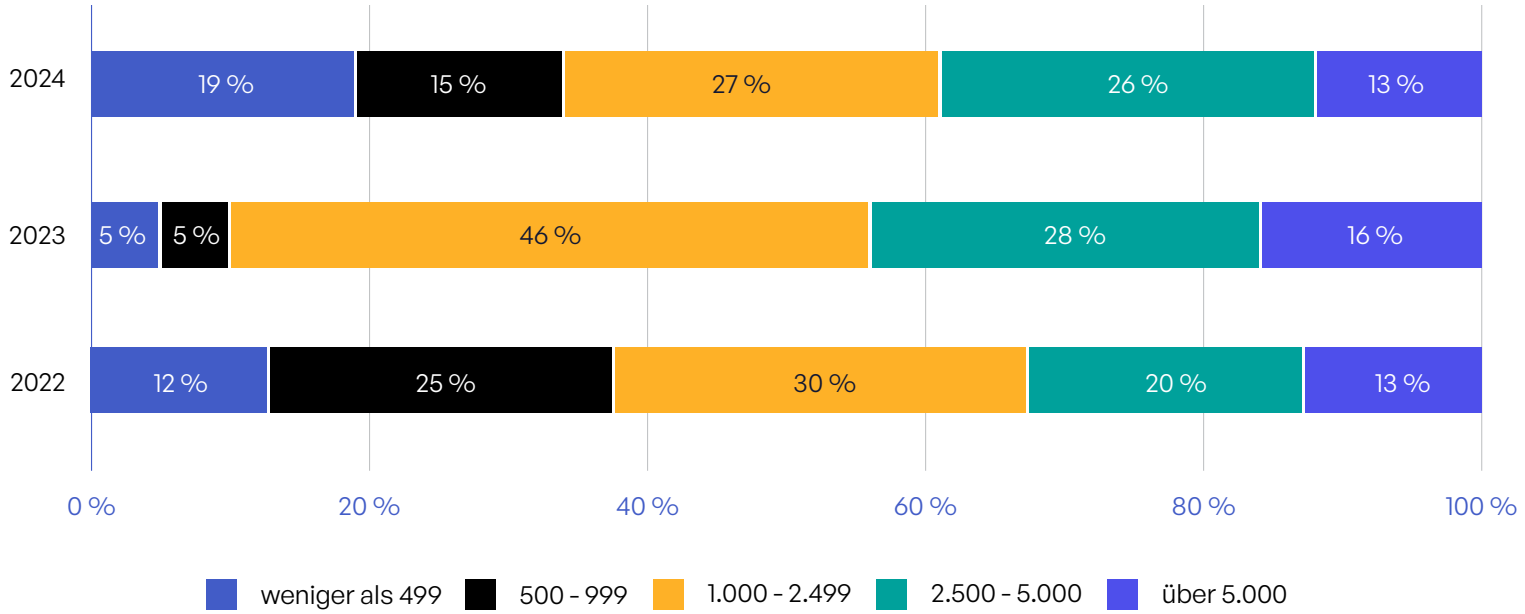


Abb. 58: Anzahl der externen Parteien, mit denen die Befragten vertrauliche Inhalte austauschen.

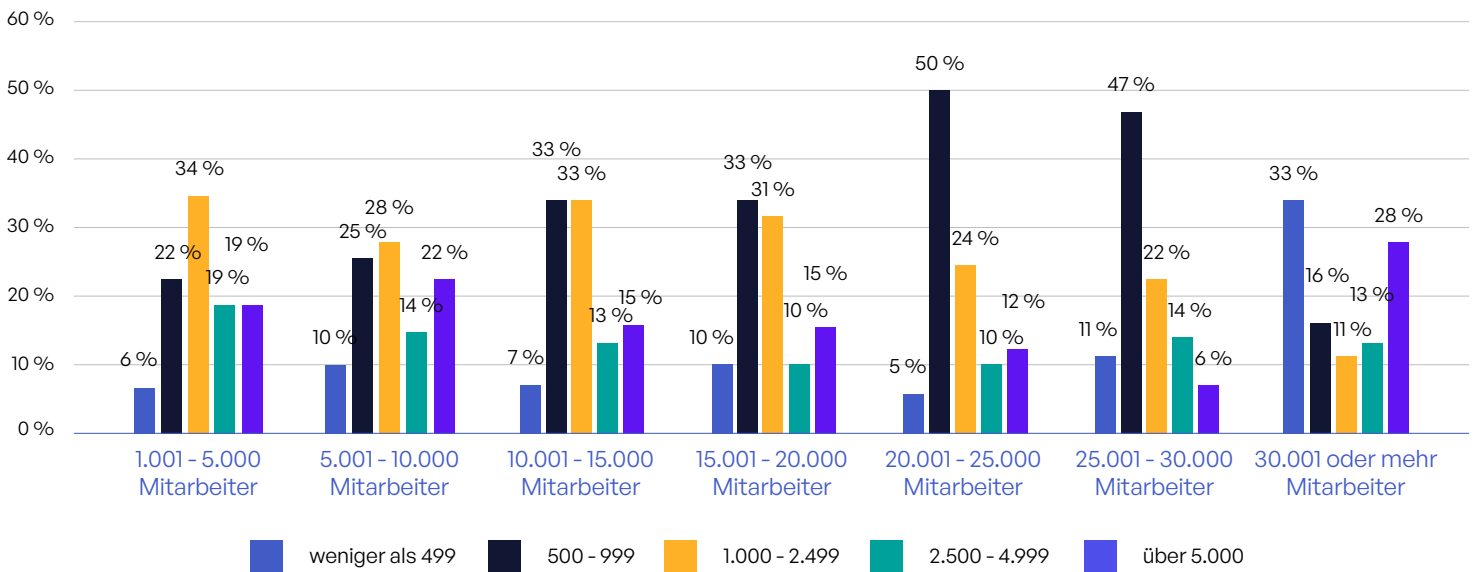


Abb. 59: Kommunikation sensibler Inhalte mit externen Parteien nach Unternehmensgröße.

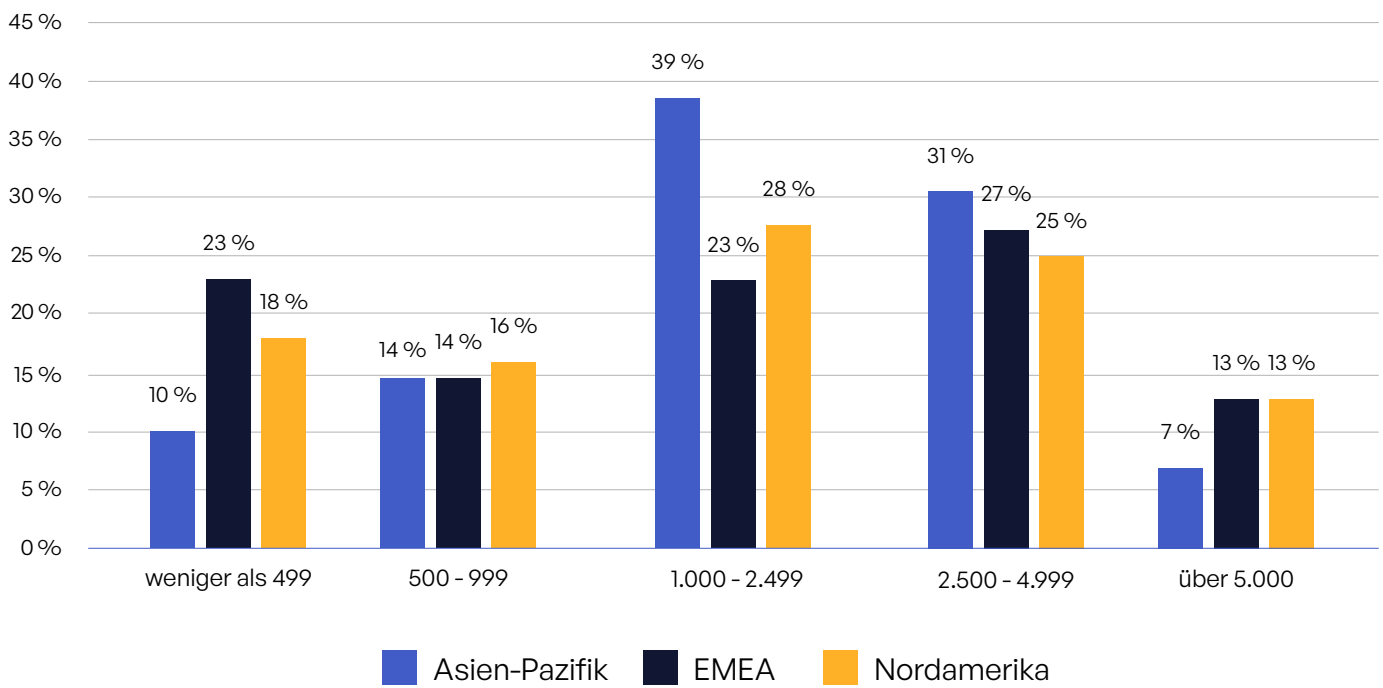


Abb. 60: Anzahl der externen Parteien, mit denen Unternehmen sensible Daten austauschen, nach Region.

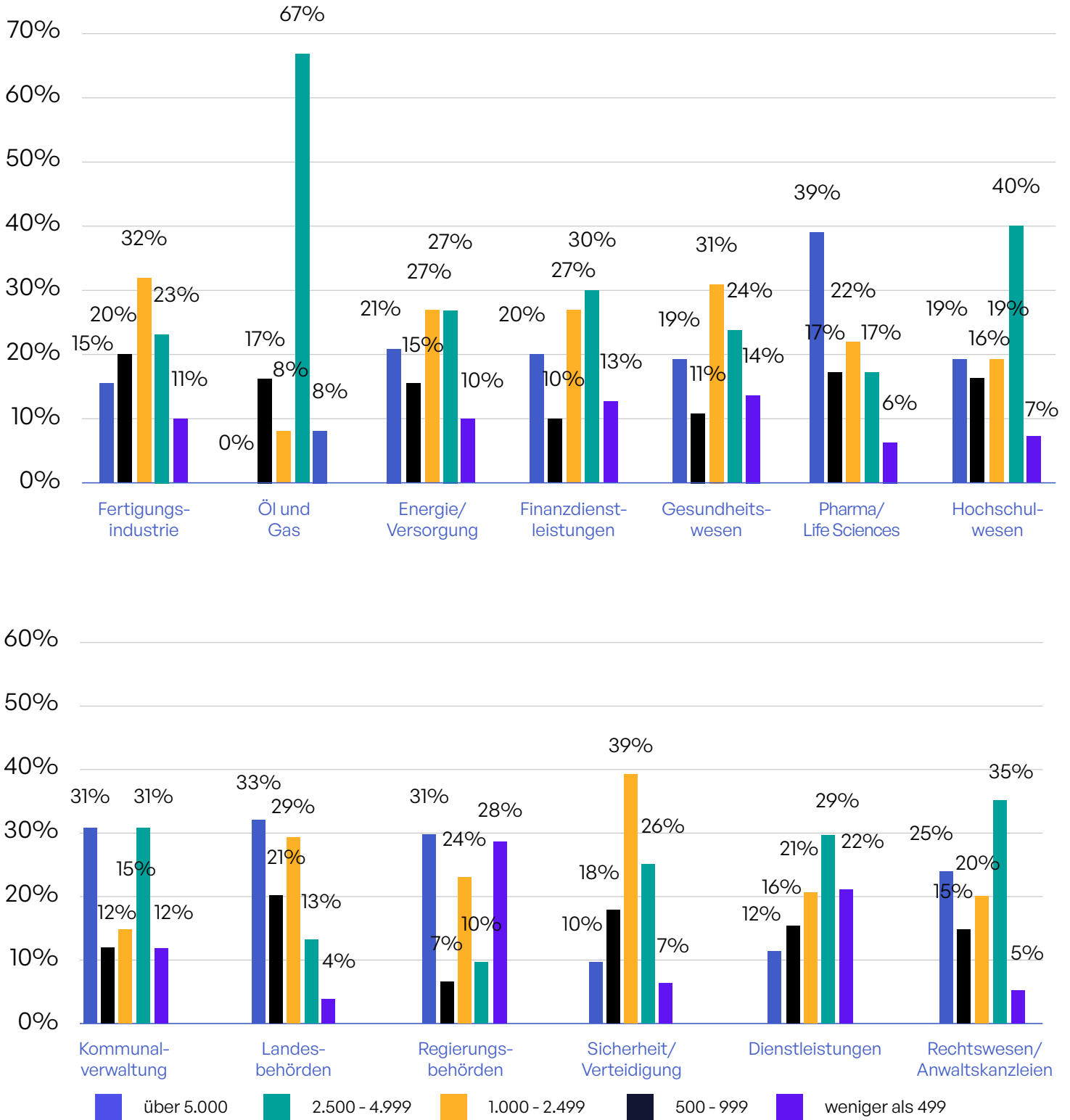


Abb. 61: Kommunikation sensibler Inhalte mit externen Parteien nach Branchen.

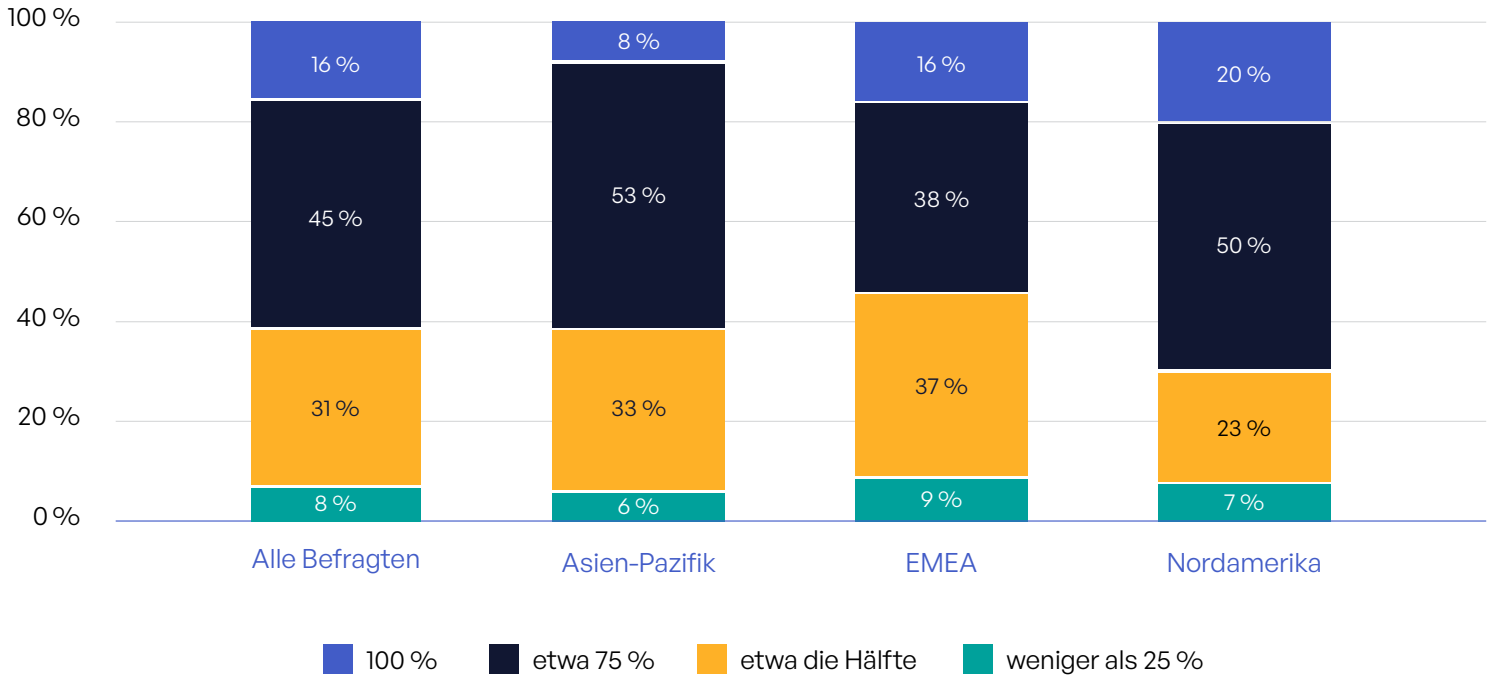


Abb. 62: Prozentualer Anteil der Kommunikation sensibler Inhalte, der nachverfolgt und kontrolliert wird, nach Regionen.

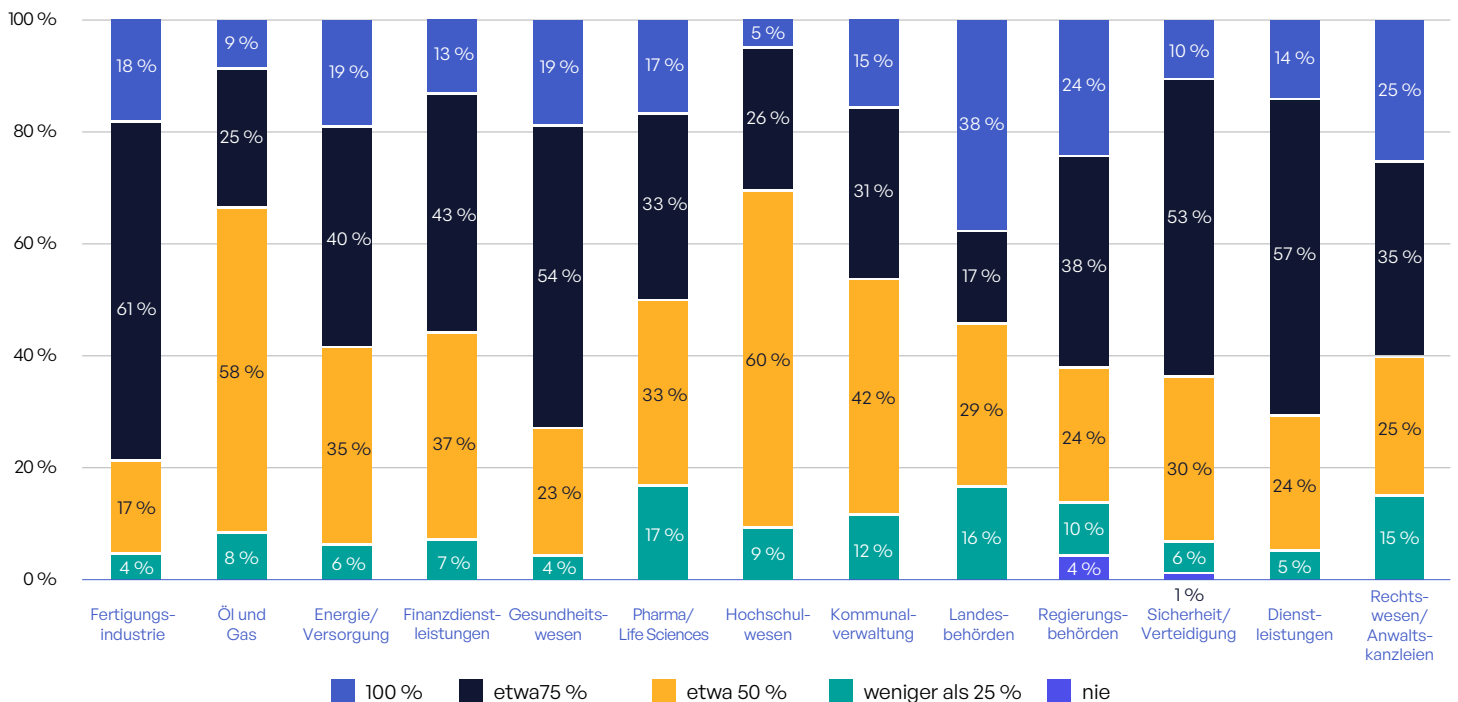


Abb. 63: Wie oft Unternehmen den Zugriff auf sensible Inhalte nachverfolgen und kontrollieren können nach Branchen.

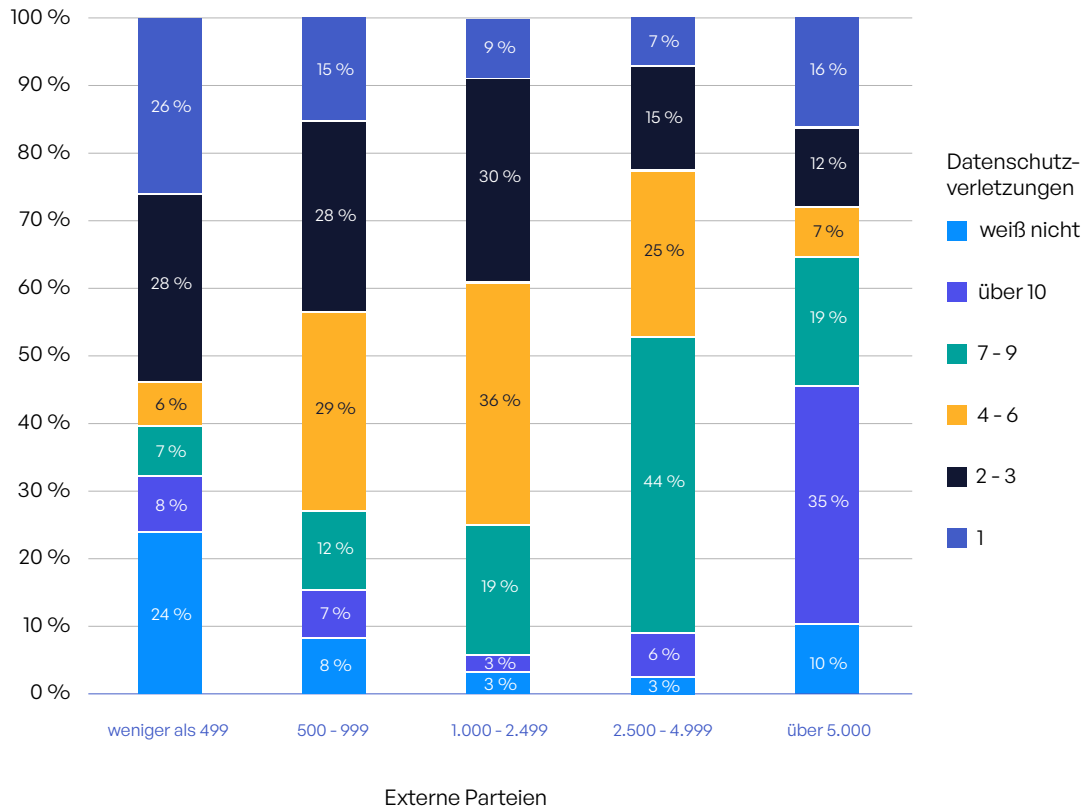


Abb. 64: Anzahl der externen Parteien und Anzahl der Datenschutzverstöße.

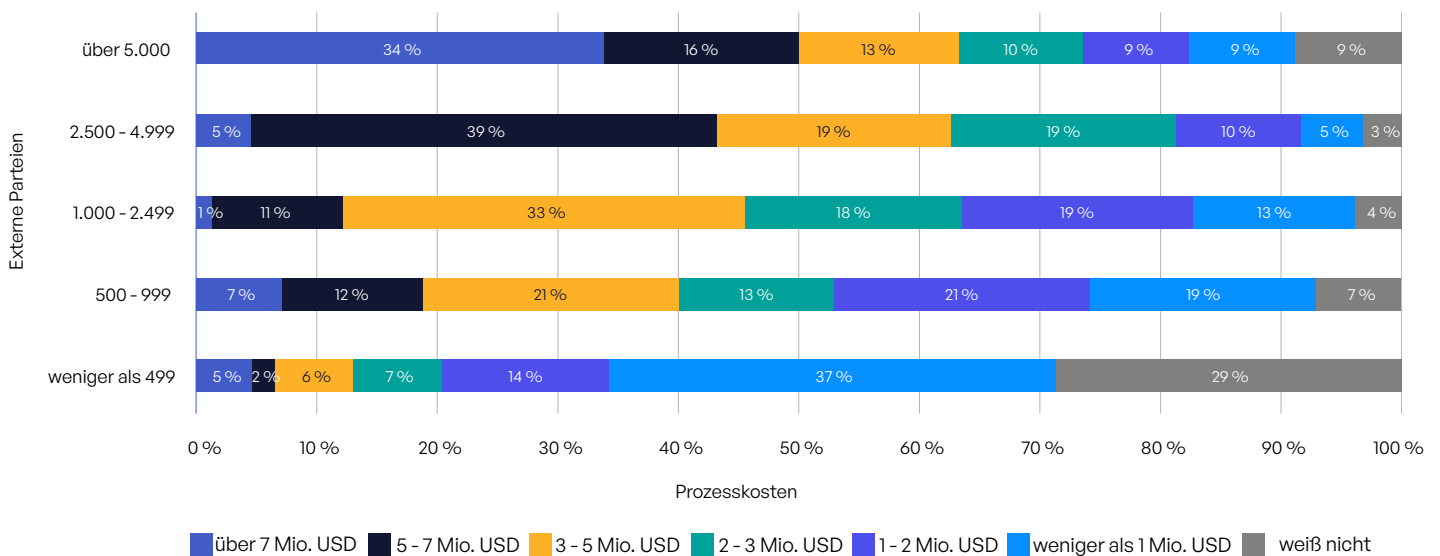


Abb. 65: Anzahl der externen Parteien und Prozesskosten.

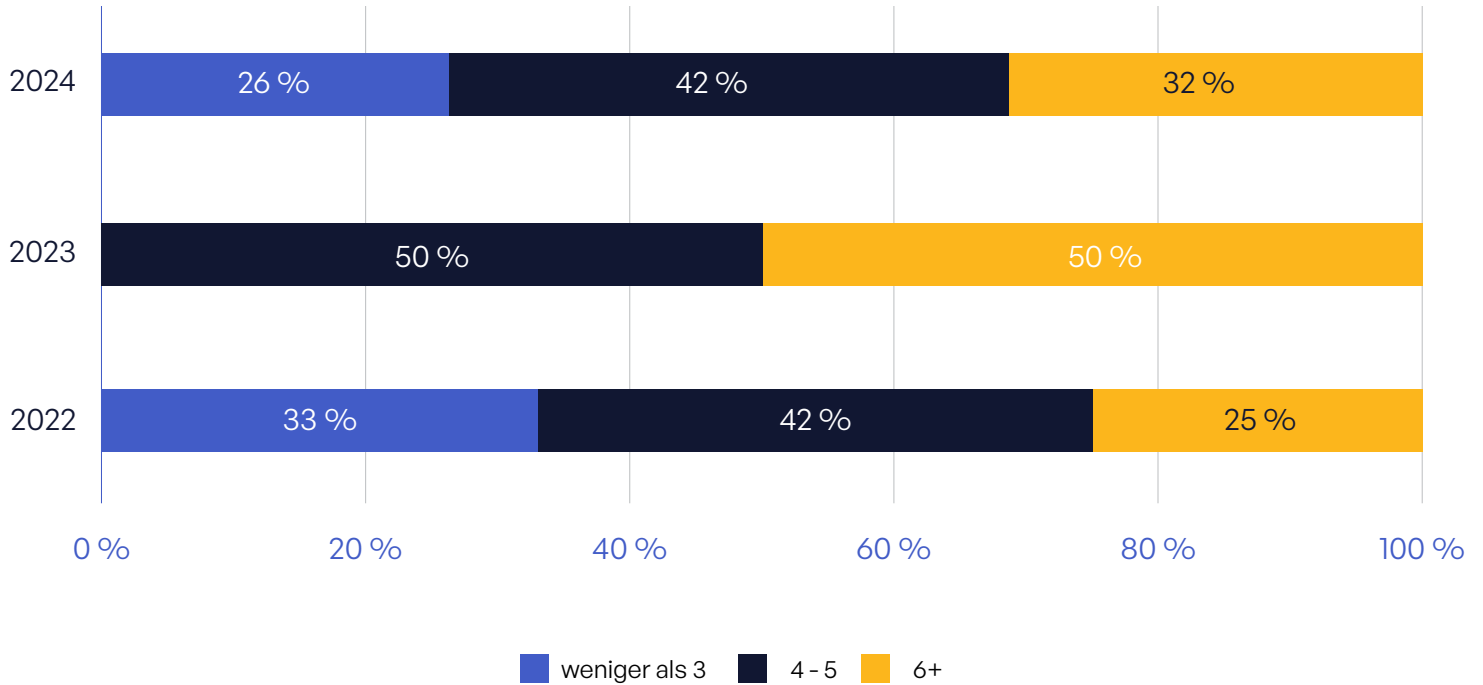


Abb. 66: Anzahl der für die Kommunikation sensibler Inhalte verwendeten Tools/Systeme.

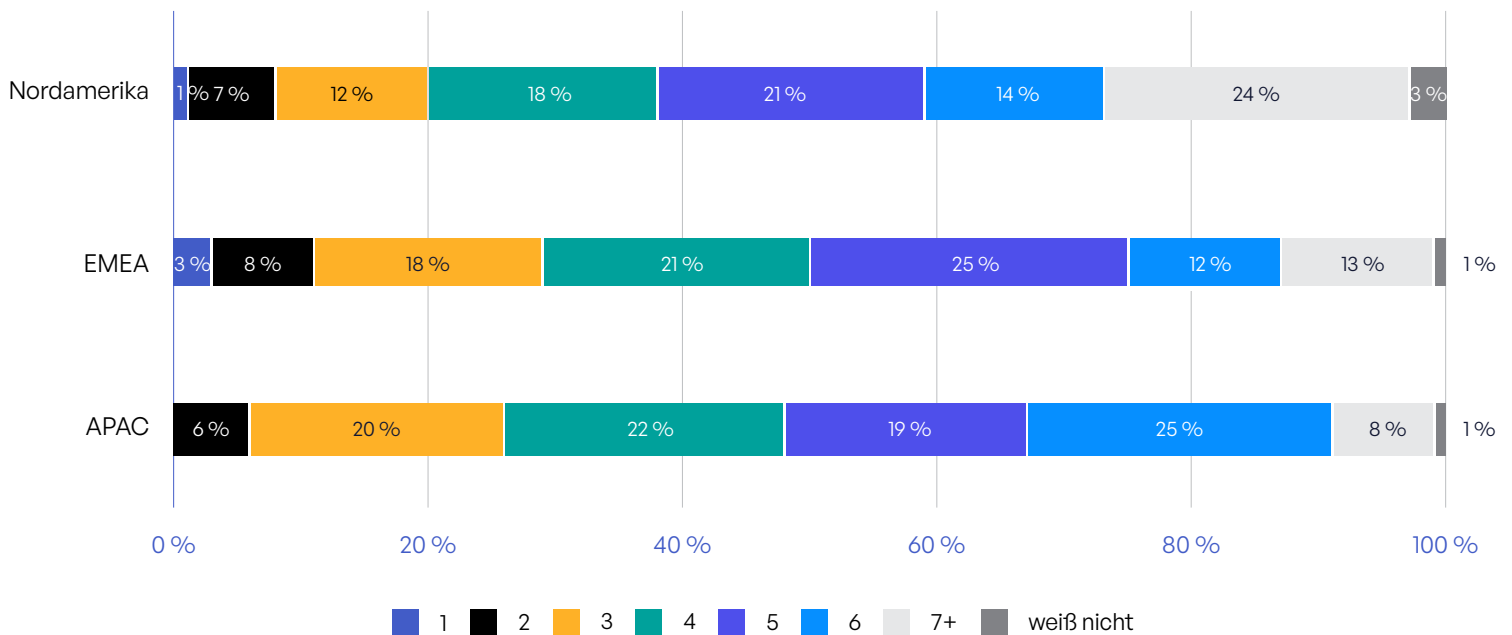


Abb. 67: Anzahl der verwendeten Kommunikationstools nach Regionen.

ERGEBNISSE DER UMFRAGE

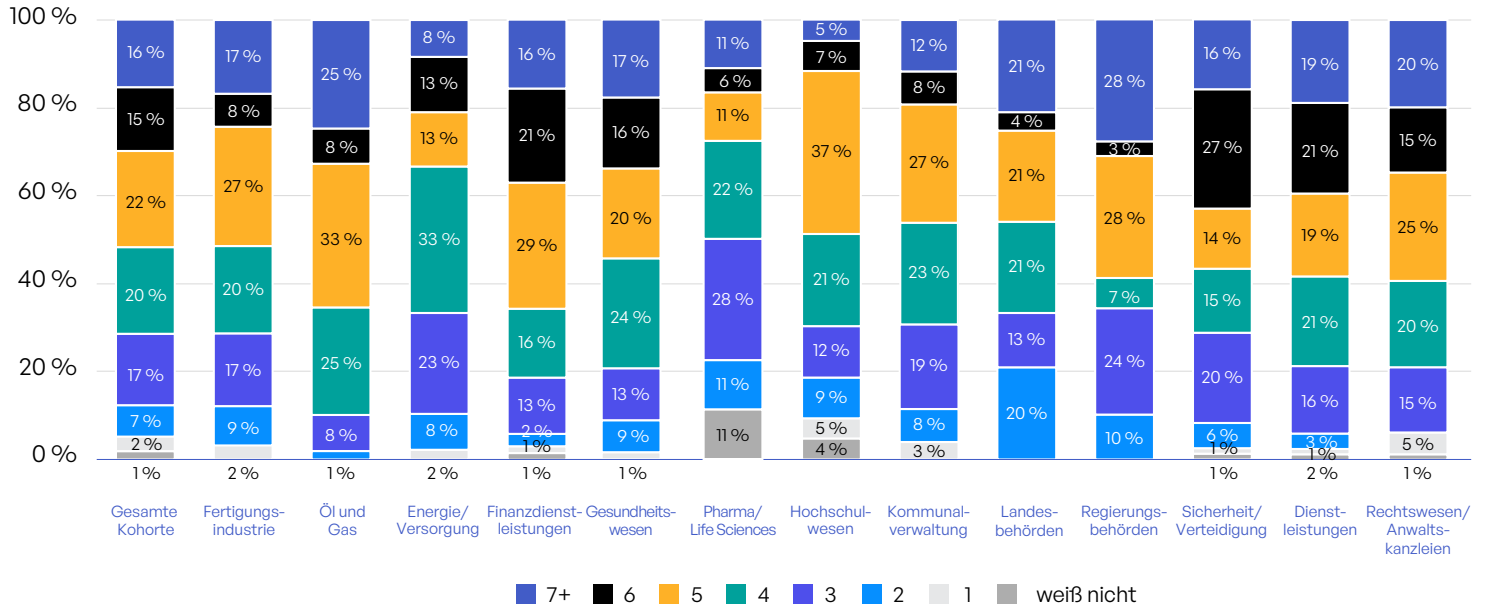


Abb. 68: Anzahl der verwendeten Kommunikationstools nach Branchen.

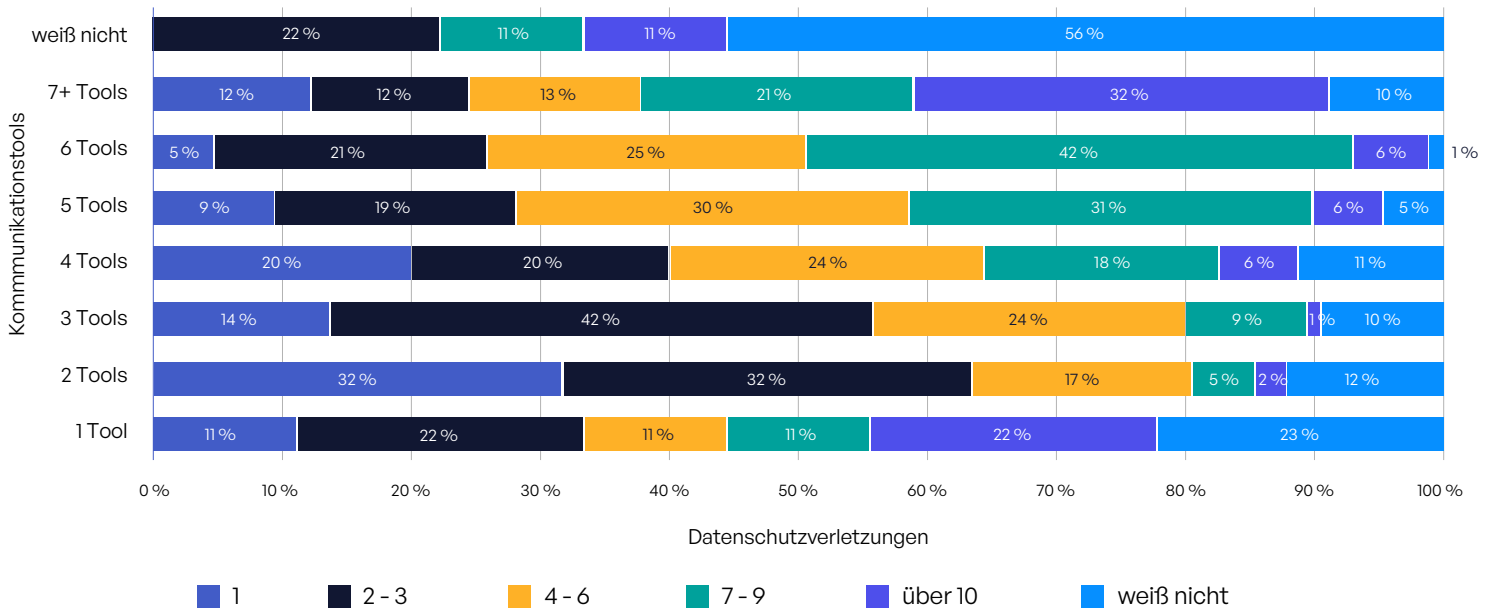


Abb. 69: Anzahl der Kommunikationstools und Anzahl der Datenschutzverletzungen.

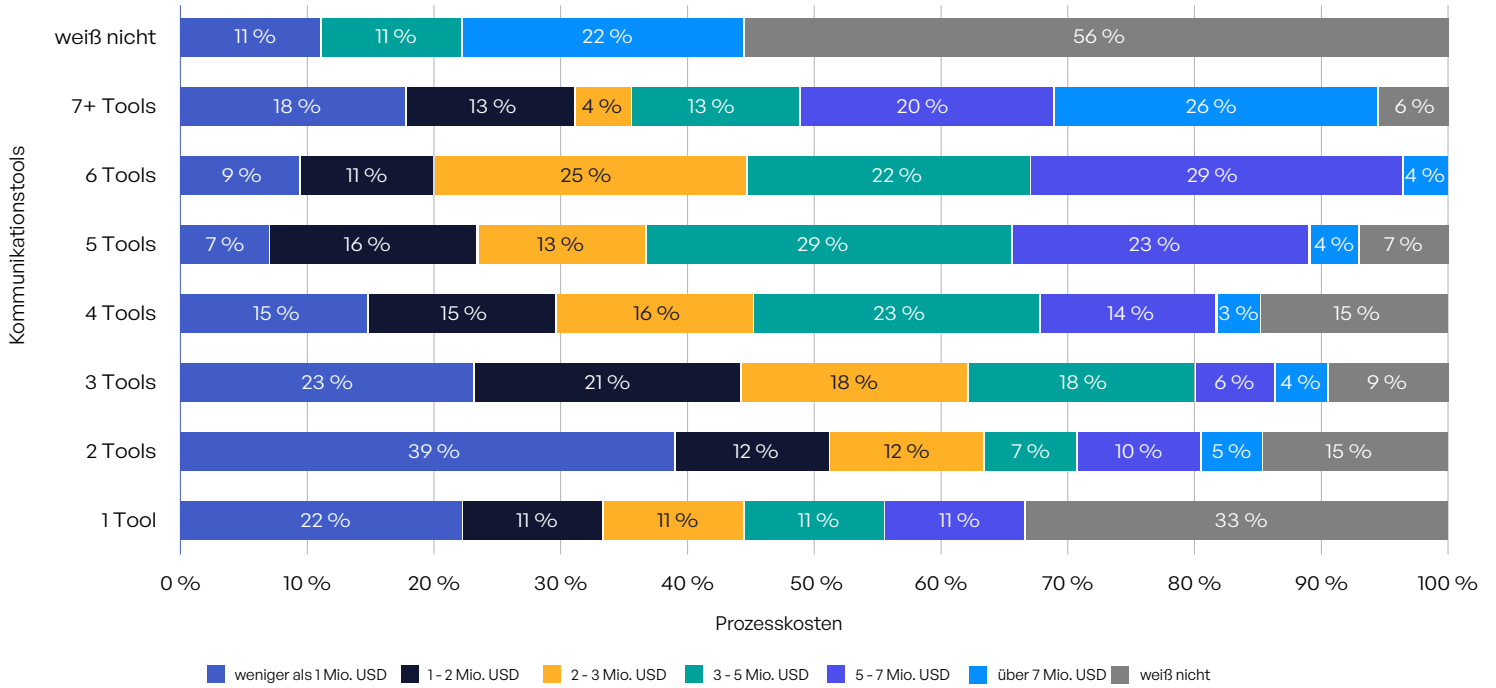


Abb. 70: Anzahl der Kommunikationstools und Prozesskosten im Zusammenhang mit Datenschutzverletzungen.

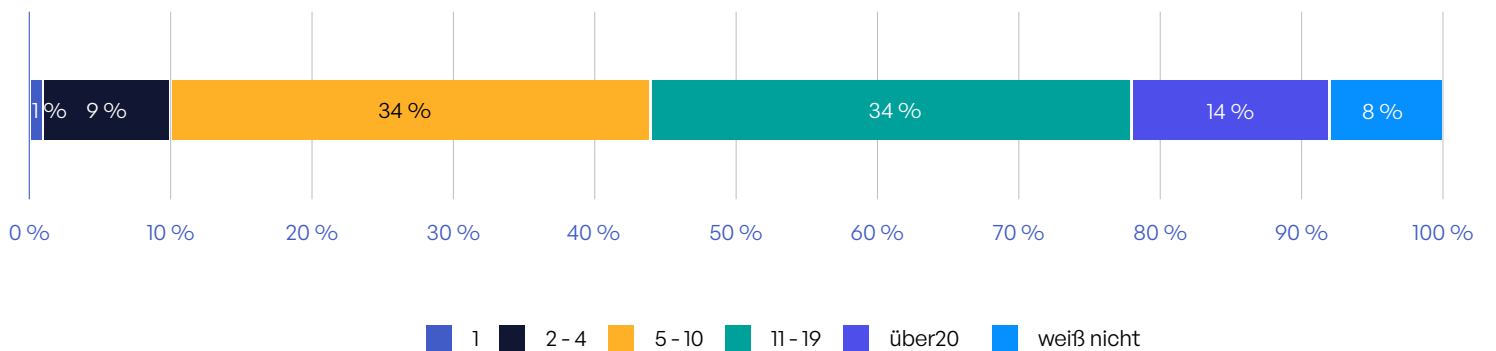


Abb. 71: Anzahl der Audit-Protokolle, die konsolidiert werden müssen.

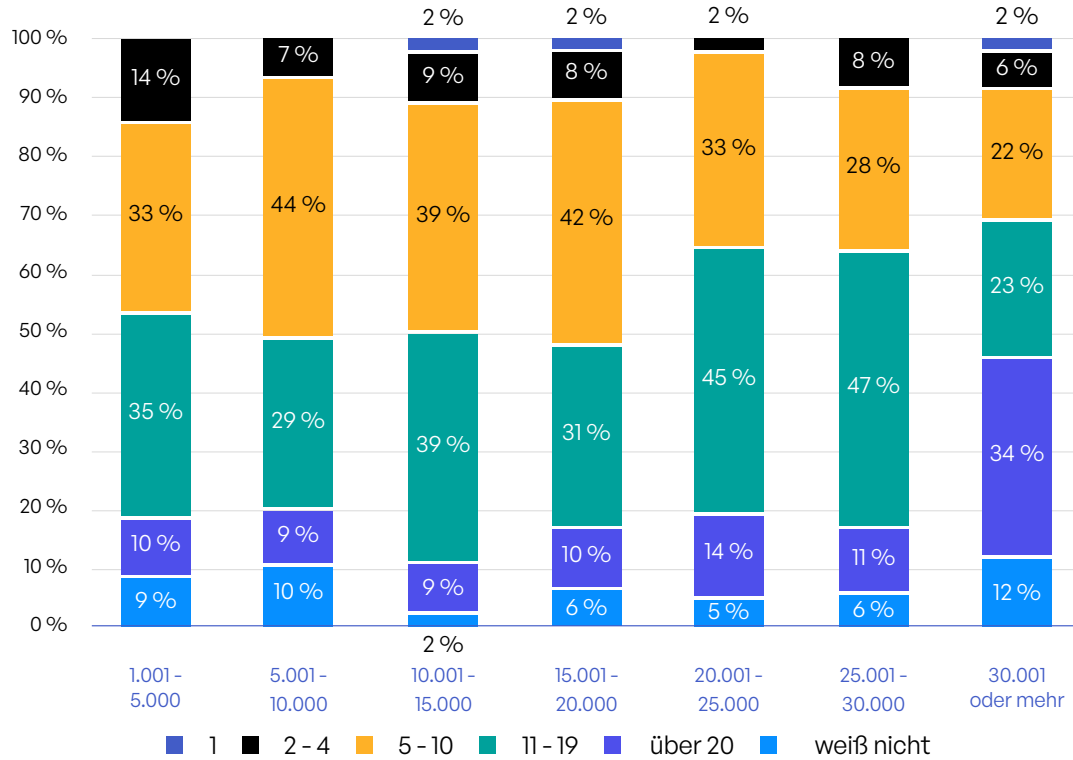


Abb. 72: Anzahl der Protokolle, die konsolidiert werden müssen, nach Unternehmensgröße.

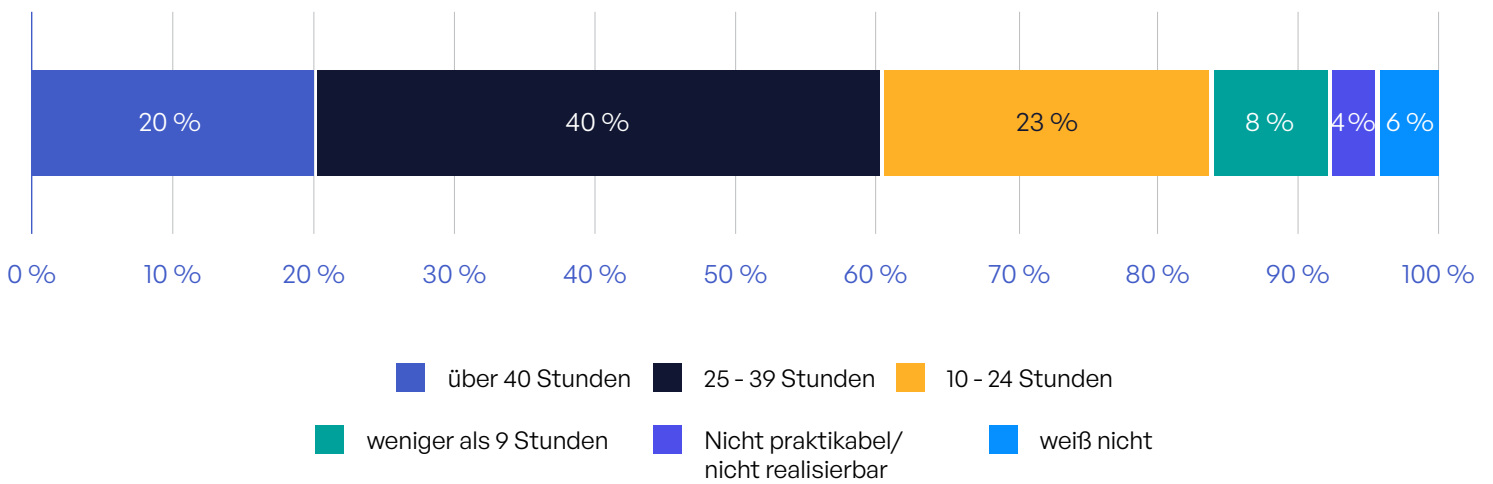


Abb. 73: Zeitaufwand für die Konsolidierung von Audit-Protokollen pro Monat.

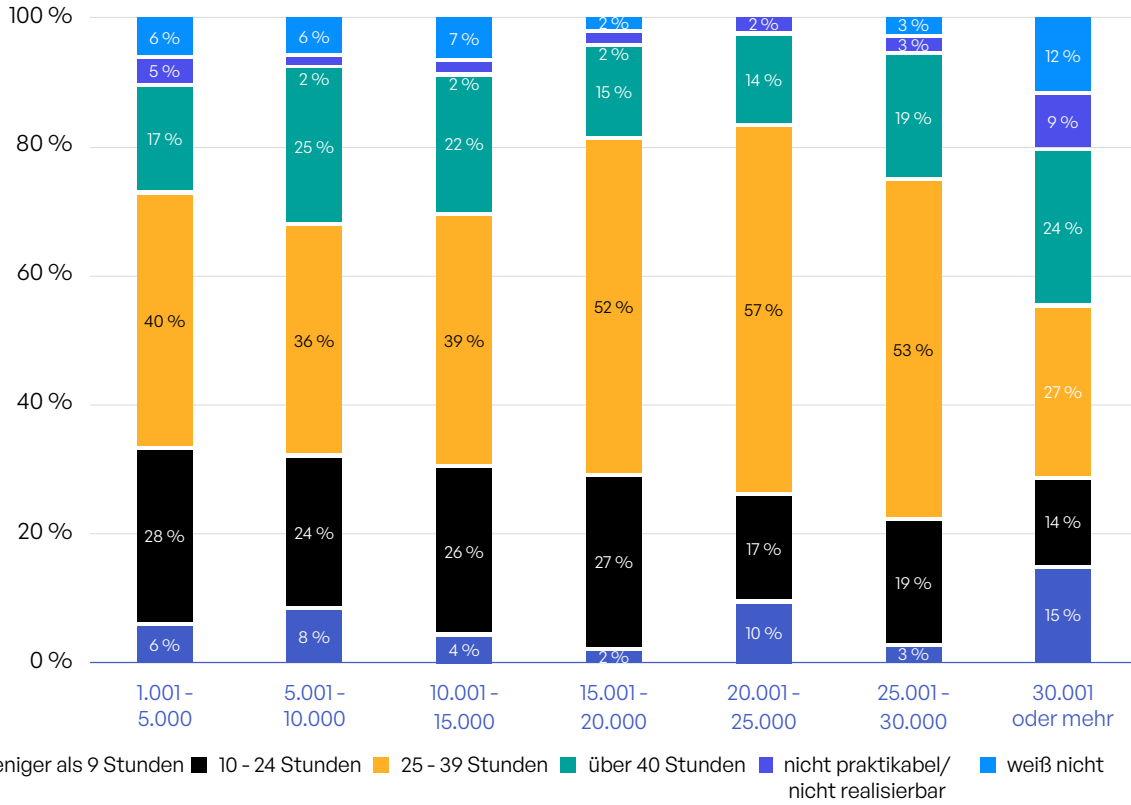


Abb. 74: Monatlich aufgewendete Zeit für die Konsolidierung von Protokollen für die Kommunikation sensibler Inhalte nach Unternehmensgröße.

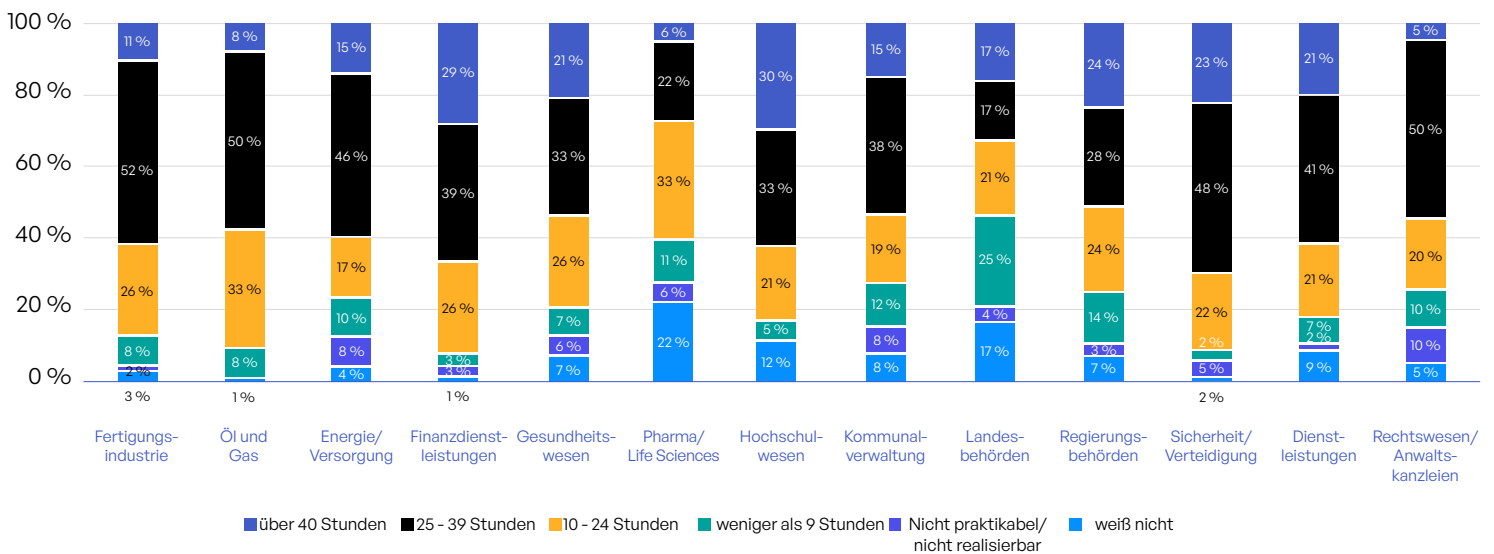


Abb. 75: Zeit, die Unternehmen jeden Monat damit verbringen, Audit-Protokolle manuell zu konsolidieren, nach Branchen.

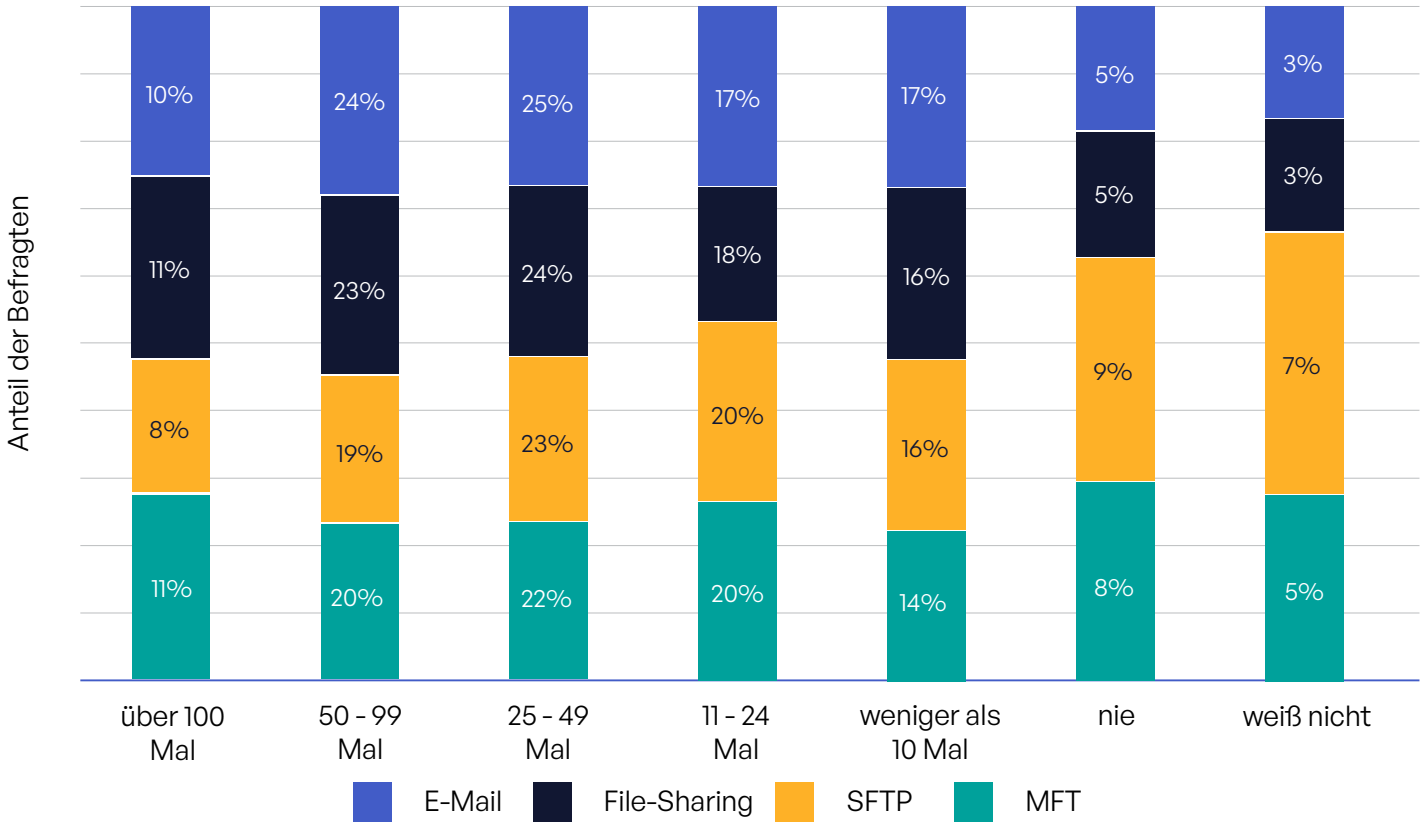


Abb. 76: Operative Auswirkungen und Sicherheits- und Compliance-Risiken in Bezug auf die Dateigröße großer Dateien.

	APAC				NORDAMERIKA				EMEA			
	E-Mail	File-Sharing	SFTP	MFT	E-Mail	File-Sharing	SFTP	MFT	E-Mail	File-Sharing	SFTP	MFT
keine	0 %	2 %	3 %	2 %	4 %	4 %	8 %	16 %	5 %	6 %	10 %	11 %
weniger als 10	9 %	14 %	9 %	9 %	14 %	13 %	14 %	10 %	21 %	17 %	18 %	17 %
10 bis 24	27 %	17 %	27 %	27 %	11 %	18 %	18 %	17 %	14 %	17 %	17 %	18 %
25 bis 49	32 %	24 %	24 %	25 %	20 %	23 %	22 %	21 %	24 %	24 %	21 %	20 %
50 bis 99	17 %	26 %	18 %	19 %	30 %	24 %	21 %	25 %	22 %	21 %	18 %	17 %
über 100	6 %	8 %	6 %	9 %	15 %	14 %	11 %	15 %	7 %	8 %	5 %	9 %
weiß nicht	3 %	3 %	7 %	3 %	1 %	1 %	3 %	3 %	2 %	3 %	8 %	5 %

Abb. 77: Monatlich erforderliche Workarounds aufgrund von Dateigrößenbeschränkungen nach Regionen.

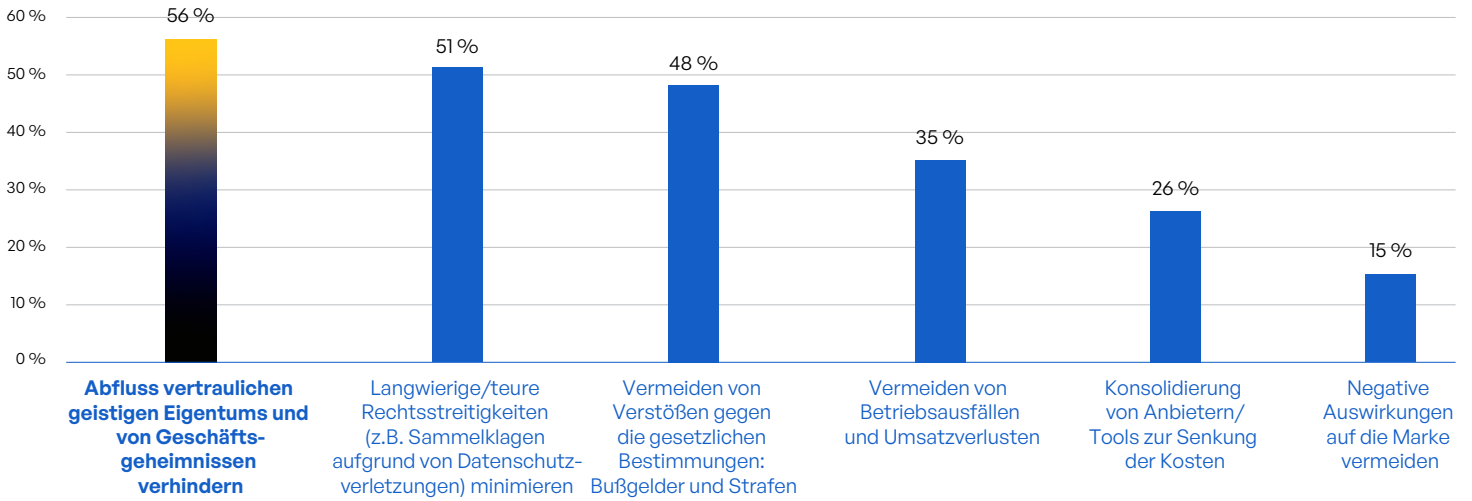


Abb. 78: Die wichtigsten Faktoren für die Vereinheitlichung und den Schutz der Kommunikation sensibler Inhalte.

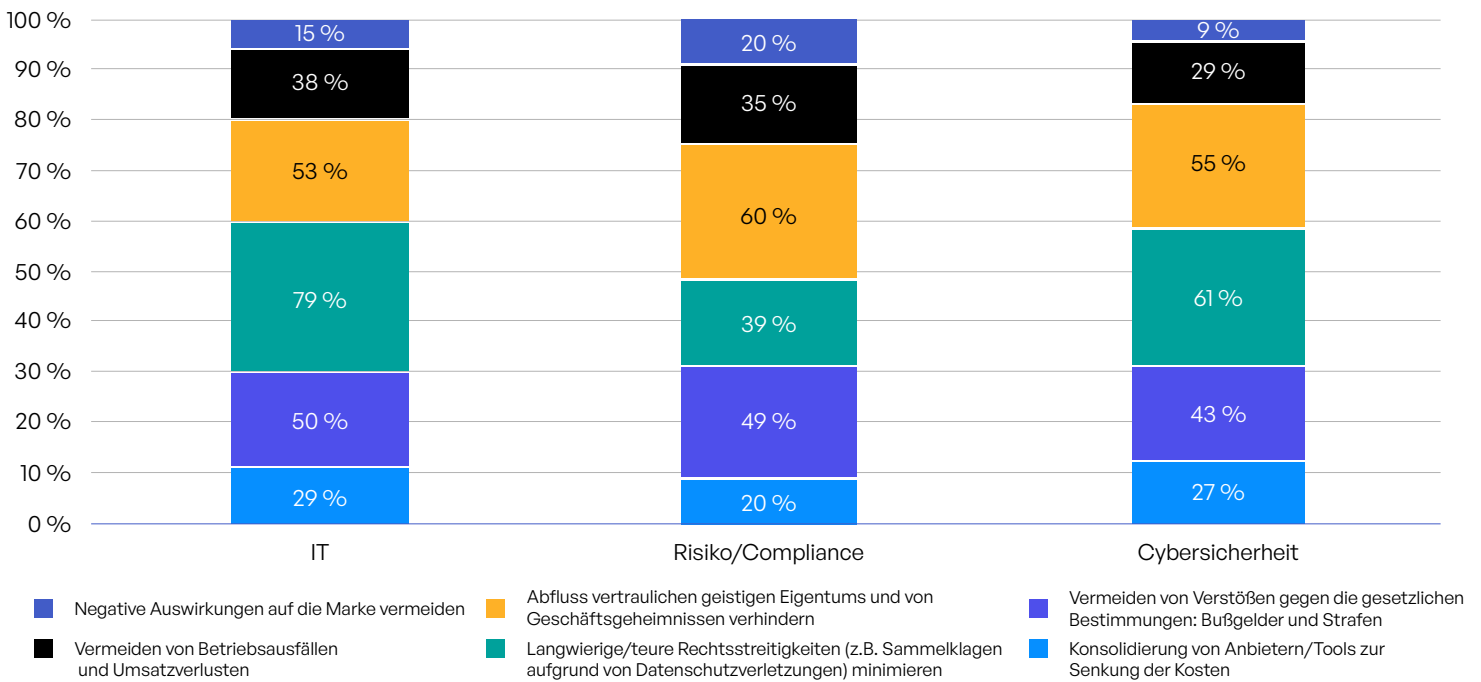


Abb. 79: Hauptrisikofaktoren bei der Kommunikation sensibler Inhalte nach Verantwortungsbereichen

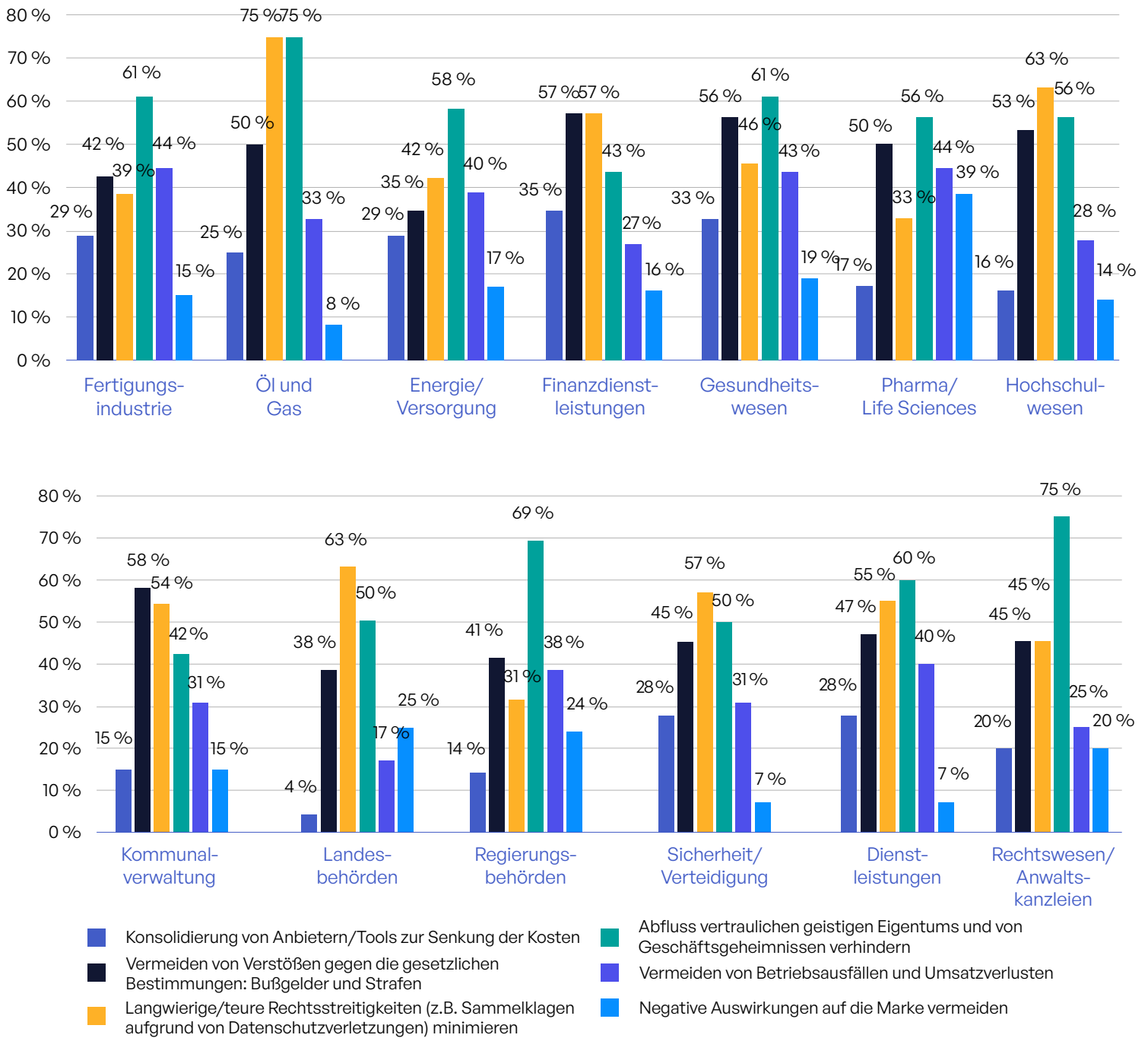


Abb. 80: Treiber für die Vereinheitlichung und den Schutz der Kommunikation sensibler Inhalte nach Branchen.

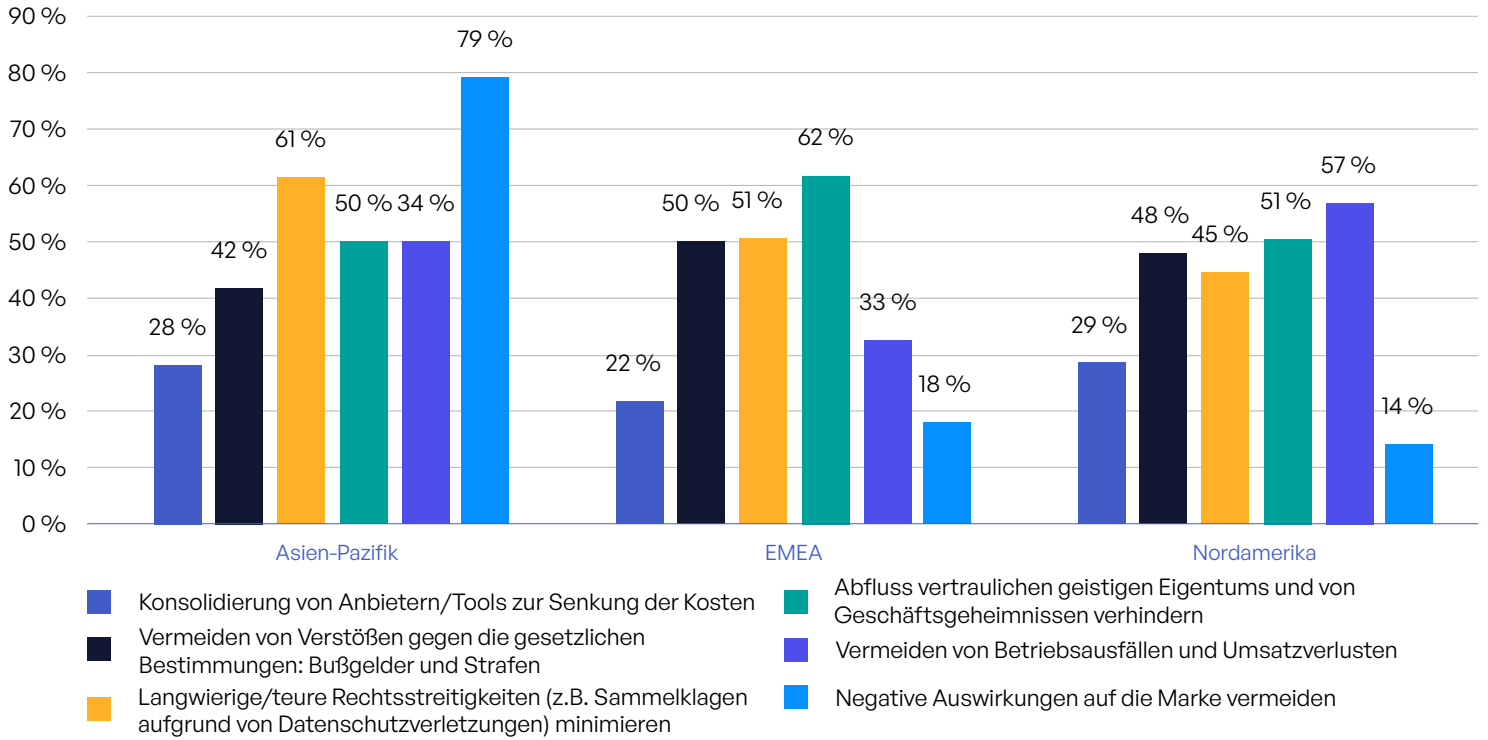


Abb. 81: Treiber für die Vereinheitlichung und den Schutz der Kommunikation sensibler Inhalte nach Regionen.

QUELLENANGABEN

1. "2024 Data Breach Investigations Report," Verizon, April 2024.
2. Matt Kapko, "Progress Software's MOVEit meltdown: uncovering the fallout," Cybersecurity Dive, 16. Januar 2024.
3. Bill Toulas, "Fortra shares findings on GoAnywhere MFT zero-day attacks," BleepingComputer, 1. April 2023.
4. "2024 Gartner Technology Adoption Roadmap for Larger Enterprises Survey," Februar 2024.
5. Eileen Yu, "Employees input sensitive data into generative AI tools despite the risks," ZDNet, 22. Februar 2024.
6. "2024 Global Threat Report," CrowdStrike, Februar 2024.
7. "Despite increased budgets, organizations struggle with compliance," Help Net Security, 24. Mai 2024.
8. "Data Protection and Privacy Legislation Worldwide," U.N. Trade & Development, abgerufen am 7. Juni 2024.
9. "U.S. State Privacy Legislation Tracker," IAPP, zuletzt aktualisiert am 28. Mai 2024.
10. Martin Armstrong, "EU Data Protection Fines Hit Record High in 2023," Statistica, 8. Januar 2024.
11. "Health Information Privacy: Enforcement Highlights," U.S. Health and Human Services, abgerufen am 30. April 2024.
12. "2024 Data Breach Investigations Report," Verizon, April 2024.
13. "2023 Data Breach Report," ID Theft Center, Januar 2024.
14. "Cost of a Data Breach Report 2023," IBM Security, Juli 2023.
15. ebd.
16. "2024 Global Threat Report," CrowdStrike, Februar 2024.
17. "2024 Data Breach Investigations Report," Verizon, Mai 2024.
18. "Privacy in Practice 2024," ISACA, Januar 2024.
19. "Fortinet Global Zero Trust Report Finds Majority of Organizations Are Actively Implementing Zero Trust But Many Still Face Integration Challenges," Fortinet Presse-Information, 20. Juni 2023.



Kiteworks

Copyright © 2024 Kiteworks. Kiteworks hat es sich zur Aufgabe gemacht, Unternehmen in die Lage zu versetzen, die Risiken beim Senden, Teilen, Empfangen und Speichern sensibler Inhalte effektiv zu managen. Die Kiteworks-Plattform stellt Kunden ein Private Content Network zur Verfügung, das Content Governance, Compliance und Schutz bietet. Die Plattform vereinheitlicht, verfolgt, kontrolliert und schützt sensible Inhalte, die innerhalb des Unternehmens und über die Unternehmensgrenzen hinaus ausgetauscht werden. Dadurch wird das Risikomanagement erheblich verbessert und die Einhaltung gesetzlicher Vorgaben für die gesamte Kommunikation mit sensiblen Inhalten sichergestellt.