Pridatect

Studie zum Datenschutz im Gesundheitssektor 2020

Inhalt

01. Einleitung

Im Gesundheitssektor werden personenbezogene Gesundheitsdaten von Kunden oder Patienten verarbeitet, die besonders geschützt werden müssen, da eine unzureichende Sicherung dazu führen kann, dass die Privatsphäre von Menschen gefährdet wird.

Insbesondere seit Inkrafttreten der DSGVO 2018 sind Gesundheitsorganisation dazu verpflichtet, ihre **Kunden oder Patienten darüber zu informieren, wie ihre Daten verarbeitet werden,** welche Informationen gespeichert werden und für welche Zwecke die Organisation diese Daten verarbeiten muss. Die DSGVO verpflichtet Organisationen rechtlich dazu, den Schutz personenbezogener Daten zu gewährleisten und ein Protokoll zur Speicherung, Verarbeitung und Löschung personenbezogener Daten zu erstellen. Ein Nichteinhalten der DSGVO kann erhebliche wirtschaftliche Sanktionen und Reputationsschäden zur Folge haben.

Die DSGVO betrifft alle Fachkräfte und Zentren im Gesundheitssektor, sowie Unternehmen, die sich mit Daten zur Gesundheit von Menschen befassen. Sie umfasst auch Gesundheitsanwendungen, Forschungsarbeiten oder Dienste, die mit gesundheitsbezogenen Daten arbeiten. Darüber hinaus muss hinzugefügt werden, dass die DSGVO Daten, die sich auf die Gesundheit von Menschen beziehen, als besonders **sensible Daten** betrachtet werden, weshalb diese eine spezielle Handhabung und **zusätzlichen Schutz** erfordern.

Neben zahlreichen Fitness- und Ernährungs-Apps kommen spätestens seit 2020 auch vermehrt medizinische Anwendungen auf den Markt, denn mit dem Inkrafttreten des "Digitalen Versorgungs-Gesetz" (DVG) sollen zukünftig bestimmte digitale Gesundheitsanwendungen von Ärzten verschrieben werden können und für gesetzlich Versicherte zu einer Kassenleistung werden.

Auch bei den Gesundheitsdaten, die von Softwarelösungen, Wearables und Gesundheits-Apps verarbeitet werden, handelt es sich um personenbezogene Daten mit besonderer Sensibilität. Sie unterliegen dem Schutz der EU-Datenschutz-Grundverordnung und des Bundesdatenschutzgesetzes. Ihre Erhebung, Verarbeitung oder Nutzung ist nur unter erhöhten Anforderungen auf Basis einer Rechtsgrundlage oder einer Einwilligung der Betroffenen zulässig. Dabei muss die **Einwilligung** freiwillig, informiert, ausdrücklich und nachweislich abgegeben werden.

Zur Informiertheit gehört auch die **Transparenz.** Dies bedeutet, dass Betroffene umfassend die Zwecke kennen müssen, für die ihre Daten verwendet werden. Sie sind über die möglichen Risiken aufzuklären. Die Betroffenen haben jederzeit das Recht, über ihre gespeicherten Daten Auskunft zu erhalten. Die Anbieter von Gesundheits-Apps müssen durch geeignete technische und organisatorische Maßnahmen gewährleisten, dass keine Unbefugten Zugriff auf die Gesundheitsdaten haben.

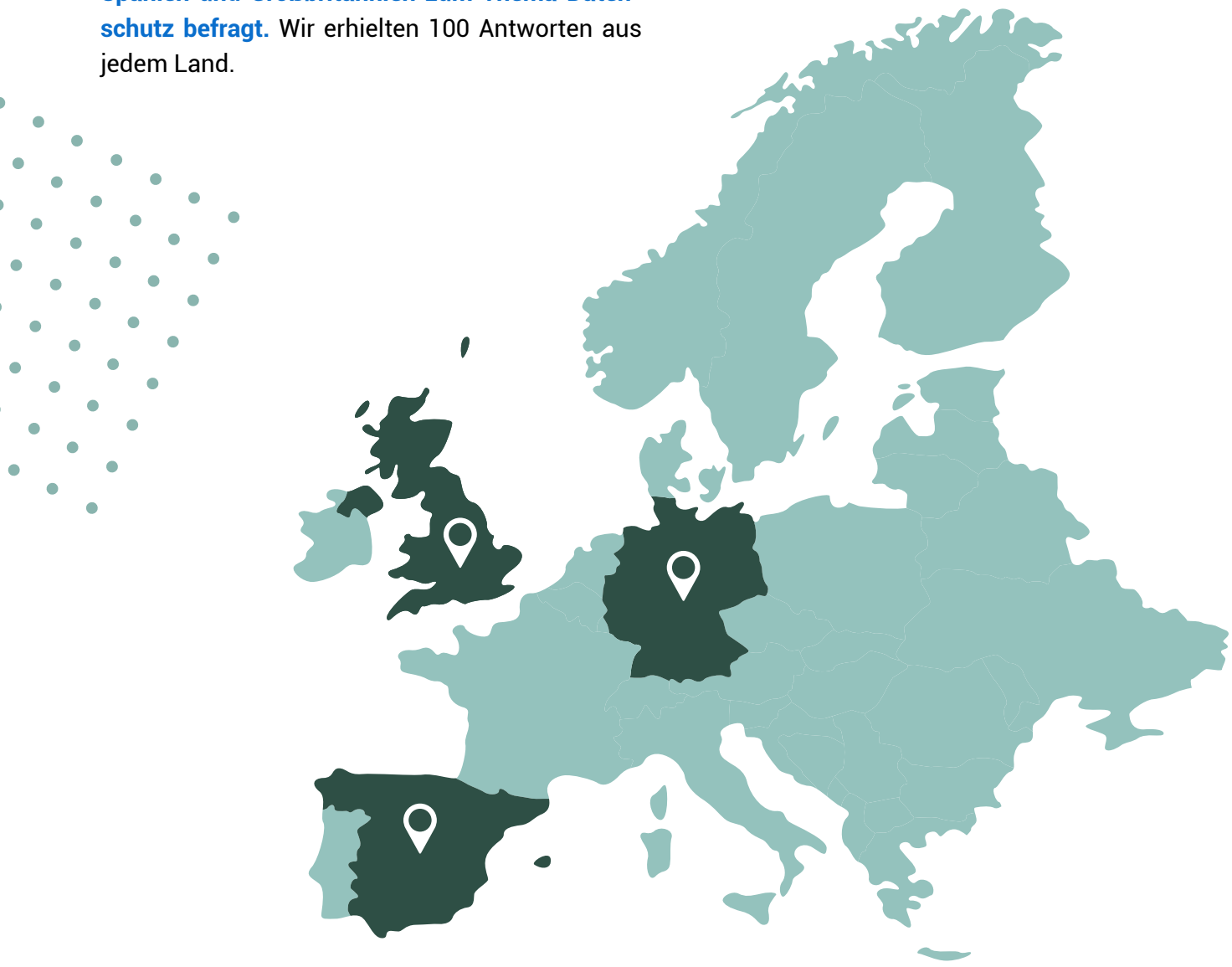
Die Einhaltung aller Anforderungen der DSGVO ist jedoch nicht immer eine leichte Aufgabe. Datenpannen im Gesundheitssektor können das Ansehen einer Organisation und das Vertrauen seitens Klienten und Partnern erheblich beeinträchtigen.

In dieser Studie analysieren wir, inwieweit sich Unternehmen des Gesundheitssektors der Bedeutung des Datenschutzes bewusst sind und ermitteln ihren Kenntnisstand über die damit verbundenen Verpflichtungen und Implementierung geeigneter Schutzmaßnahmen.

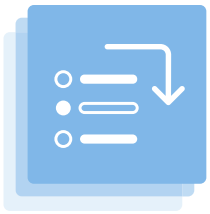
02. Methodik

Um ein Bild über die aktuelle DSGVO Konformität zu bekommen und um Organisationen und der wachsenden Forschung gute Praktiken zur Verfügung zu stellen, **haben wir im Mai 2020 die CEOs und Manager von 300 Organisationen des Gesundheits- und Pharmasektors in Deutschland, Spanien und Großbritannien zum Thema Datenschutz befragt.** Wir erhielten 100 Antworten aus jedem Land.

In dieser Studie analysieren wir **die in Deutschland erzielten Ergebnisse** und ziehen Vergleiche zu den Daten auf europäischer Ebene.



03. Studie zum Stand des Datenschutzes im deutschen Gesundheitssektor



A. Eigene Wahrnehmung der Datenschutz-Compliance

Wir untersuchen, wie viel Bedeutung Unternehmen und Zentren aus dem Gesundheitssektor dem Datenschutz beimessen.

B. Erhebung und Verarbeitung personenbezogener Daten

Wir analysieren, inwieweit sich Organisationen an die Vorschriften der DSGVO halten, wenn es um die Informationspflicht gegenüber Ernährungs-Apps kommen spätestens seit 2020 auch vermehrt medizinische Anwendungen auf den Markt, denn mit dem notwendigen Einwilligungs- und Vertraulichkeitsvereinbarungen einzuholen.

C. Sicherheitspolitik und -maßnahmen

Wir finden heraus, ob die empfohlenen Richtlinien und Protokolle befolgt werden, um den Schutz der persönlichen und gesundheitlichen Daten, mit denen die Unternehmen arbeiten, zu gewährleisten.

Frage 1

Auf einer Skala von 1 bis 5 - Wie wichtig ist Datenschutz für Ihre Organisation?

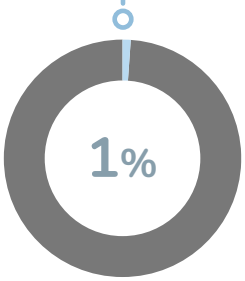
Mit der fortschreitenden Digitalisierung und Vernetzung im Gesundheitswesen sind Ärzte, Krankenhäuser, Pharmaunternehmen und viele andere Anbieter **zunehmend gefordert, sich mit Fragen des Datenschutzes und der Datensicherheit zu befassen.** Von der DSGVO werden Gesundheitsdaten in die Kategorie **besonders sensibler Daten** eingestuft, die aus diesem Grund eines besonderen Schutzes bedürfen.

Sind sich die Organisationen des Datenschutzes bewusst?

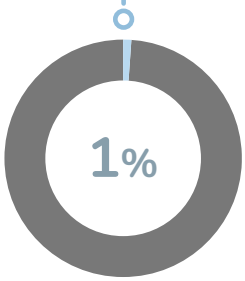
Die Ergebnisse unserer Befragung zeigen, dass zwar nur 2% der Organisationen dem Datenschutz eine geringe bis sehr geringe Wichtigkeit beimessen, jedoch auch nur 69% der Organisationen im Gesundheitssektor den Datenschutz für "sehr wichtig" halten.

Im europäischen Vergleich stellt sich heraus, dass Spanien mit einem Ergebnis von 77% und England mit 89% Datenschutz durchschnittlich als wichtiger erachten, als es die deutschen Organisationen tun.

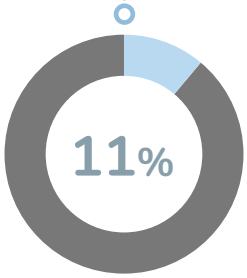
Überhaupt nicht wichtig



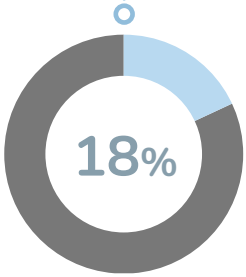
Wenig wichtig



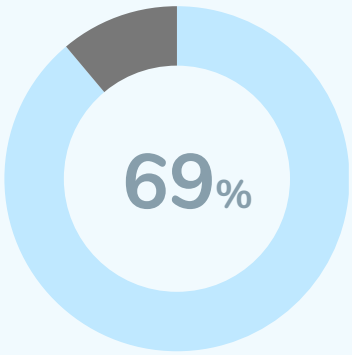
Wichtig



Relativ wichtig

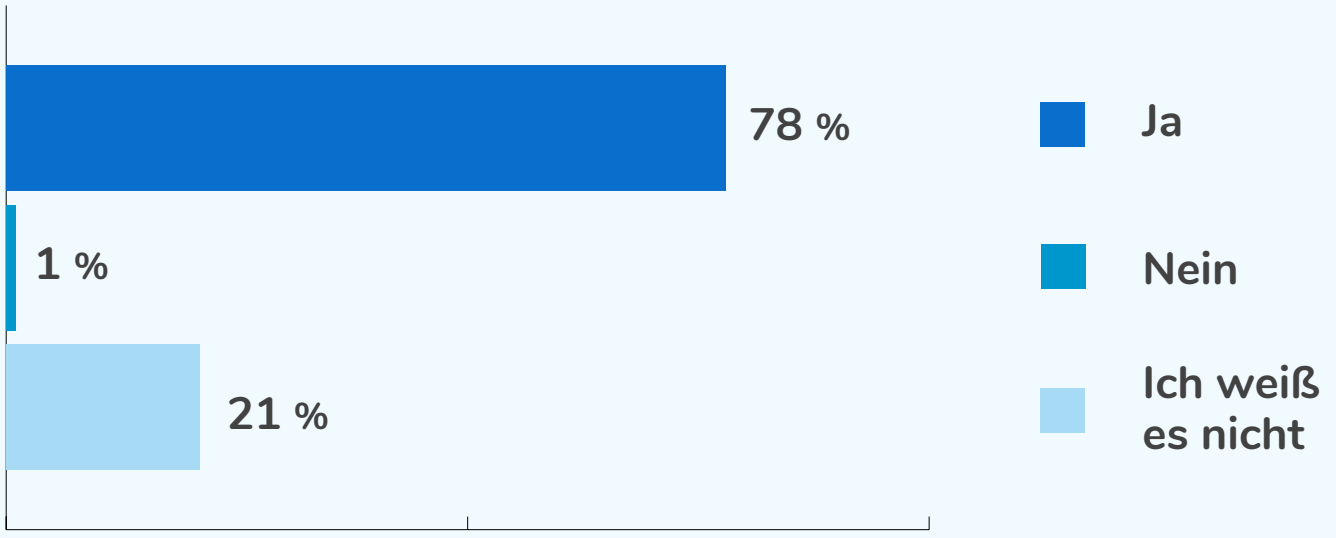


Sehr wichtig



Frage 2

Erfüllt Ihre Organisation die Kriterien, um DSGVO-konform zu sein?



Um die Einhaltung der Vorschriften zu gewährleisten, müssen eine Reihe von Vorkehrungen getroffen werden. Dazu gehört die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten, die Durchführung von Datenschutz-Folgenabschätzungen, die Durchführung von Risikoanalysen und Ermittlung möglicher Sicherheitslücken sowie ein Protokoll, wie diese gehandhabt werden. Zudem kann es - insbesondere im Gesundheitssektor - notwendig sein, einen Datenschutzbeauftragten zu benennen.

Wenn Sie eine Website haben oder Dienstleistungen über Apps anbieten, per E-Mail verschicken o.Ä., müssen Sie auch alle Anforderungen an die Datenschutzrichtlinien, Cookie Richtlinien und das Impressum erfüllen.

Die Anzahl der zu erfüllenden Vorschriften ist groß, sie sind jedoch sehr wichtig, um die **personenbezogenen Daten von Mitarbeitern, Kunden oder Patienten optimal zu schützen.**

Aus diesem Grund wollten wir wissen, ob Gesundheitsorganisationen der Meinung sind, dass sie alle Anforderungen zur Einhaltung der DSGVO erfüllen oder nicht.

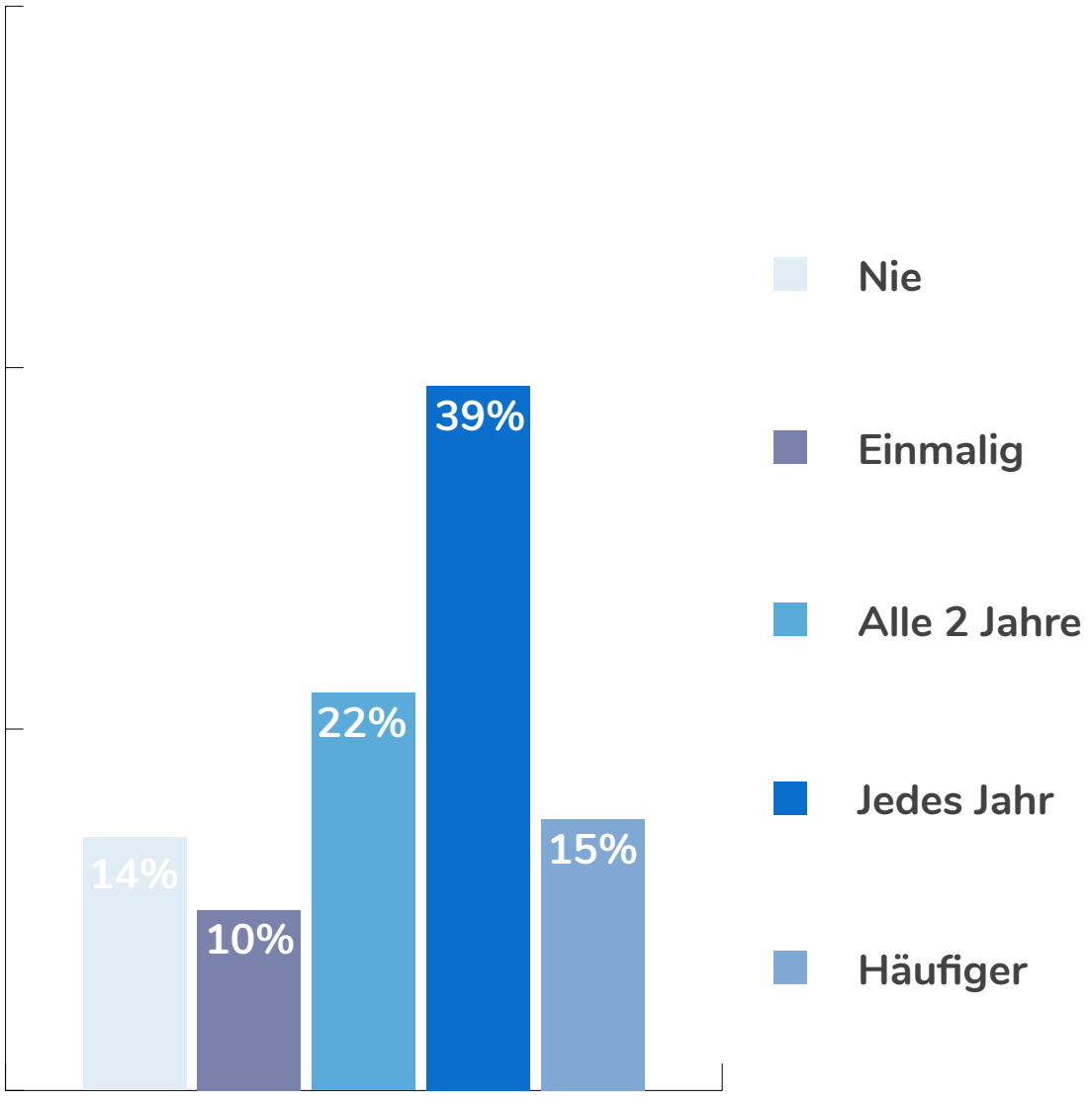
Nur 1% der Befragten gaben an, die DSGVO Vorschriften nicht zu erfüllen. **78% waren überzeugt, die verarbeiteten Daten vorschriftsgemäß zu schützen** und 21% der Befragten in Führungsebenen des Gesundheitssektors wussten nicht mit Sicherheit zu sagen, ob Ihre Organisation die Kriterien für die Einhaltung der DSGVO erfüllt.

Im europäischen Vergleich **zeigt sich, dass in deutschen Unternehmen überraschenderweise die die größte Unsicherheit darüber herrscht, ob** sie DSGVO konform sind und auch mit 78% Zustimmung schneidet Deutschland im Vergleich am schlechtesten ab.

Ein klares Nein geben aber nur 1% an, sodass Deutschland hier die niedrigste Prozentzahl und damit ein wünschenswertes Ergebnis hat.

Frage 3

Wie häufig führt Ihre Organisation Mitarbeiterschulungen zum Datenschutz durch?

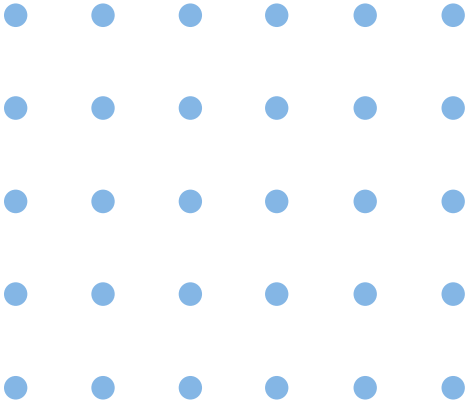


Auch wenn sich das Management der **Relevanz des betrieblichen Datenschutzes inzwischen immer mehr bewusst** wird, so sieht man doch in der Praxis, dass ein Faktor häufig vernachlässigt wird: Es sind **vor allem die Mitarbeiter, die im organisatorischen Alltag datenschutzkonform arbeiten müssen.**

Die DSGVO beinhaltet zwar keine direkte Schulungspflicht der Mitarbeiter, dennoch ist eine Einhaltung der DSGVO-Verpflichtungen ohne diese kaum realistisch möglich. Bei der Verarbeitung personenbezogener und im Gesundheitssektor besonders sensibler Gesundheitsdaten muss die Datenschutzverordnung durch jeden einzelnen Mitarbeiter, der personenbezogene Daten verarbeitet, beachtet und eingehalten werden. Um diese Vorgabe einhalten zu können, **ergibt sich automatisch eine Schulungspflicht.**

14% der befragten Organisationen führen überhaupt keine Datenschutzschulungen für ihre Mitarbeiter durch und nur 54% tun dies mindestens jährlich, während in Spanien und England mehr als 70% der Organisationen Schulungen jährlich oder öfter durchführen.

Datenschutz ist ein Thema, das lebt und sich fortwährend weiterentwickelt. Um zu gewährleisten, dass organisationsinterne Änderungen und externe Gesetzesänderungen berücksichtigt werden, empfehlen Datenschutzexperten regelmäßige Mitarbeiterschulungen. Die Häufigkeit richtet sich nach Faktoren wie der Art der Datenverarbeitungen des Unternehmens, sicher ist jedoch, dass eine einmalige Schulung oder Schulungen im 2-Jahres Takt nicht ausreichen.

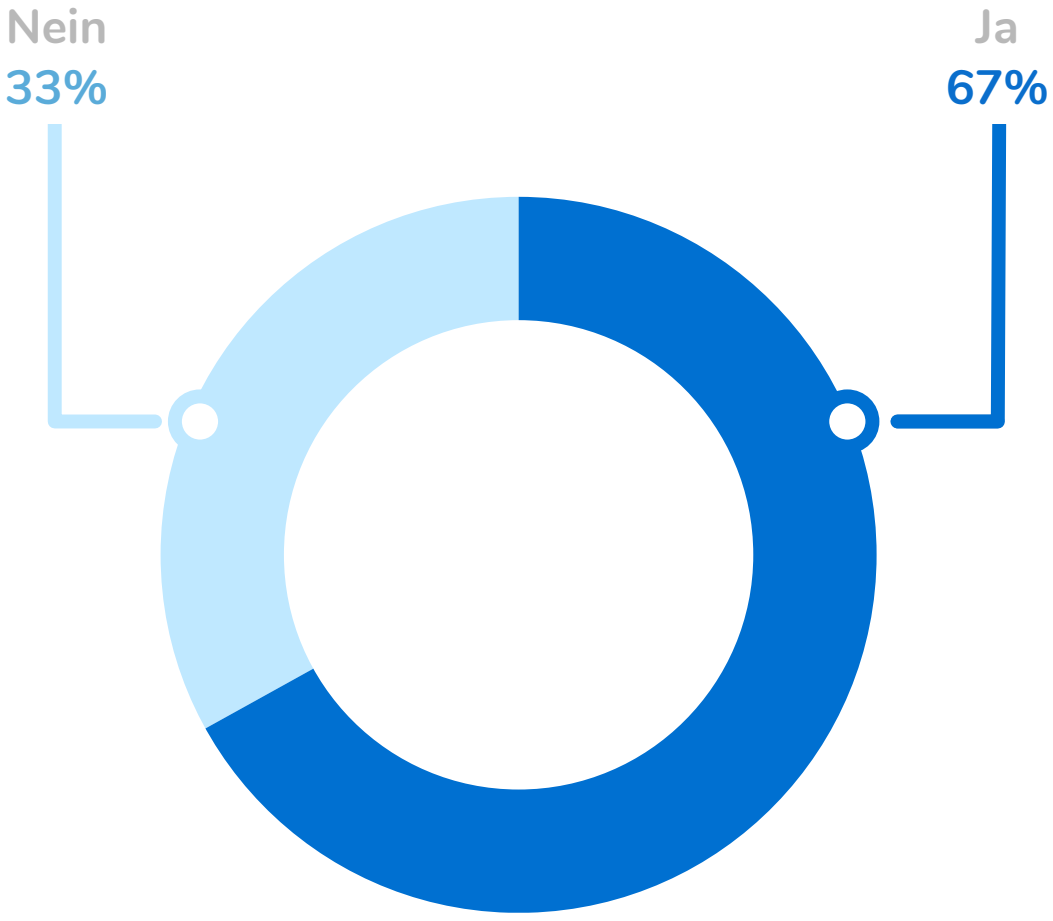


> *"Angesichts der Tatsache,* **dass nur 15% der Organisationen regelmäßige Mitarbeiterschulungen zum Datenschutz durchführen,** *ist es zweifellos notwendig, mehr in diese organisatorische Maßnahme zu investieren, da sie als eine der Wirksamsten zur Risikominderung gilt"*

Charles Maddy-Trevitt | Datenschutzexperte, Pridatect

Frage 4

Erkundigen sich Ihre Patienten/Kunden nach dem Datenschutz Ihrer Organisation?



Zwei Drittel der Patienten oder Kunden im Gesundheitswesen erkundigen sich bei Organisationen aktiv nach deren Datenschutz. Dies zeigt deutlich auf, welche Bedeutung dem Schutz sensibler Gesundheitsdaten vom Endnutzer beigemessen wird und wie ruf- und geschäftsschädigend eine Vernachlässigung des Datenschutzes sein kann.

Die Tatsache, dass 67% der Befragten angeben, mit dieser Situation konfrontiert gewesen zu sein, zeigt deutlich, wie wichtig es ist, dass die Person, die direkt mit den erhobenen Daten arbeitet, dies auf die richtige Art und Weise tut und weiß, **dass die Vernachlässigung jeglicher datenschutzrechtlicher Details dem Ruf des Unternehmens und auch dem Unternehmen selbst schaden kann.**

Klare Informationen und Erklärungen zur Verfügung zu stellen, damit die Menschen wissen, was mit ihren Daten geschehen wird, sowie in der Lage zu sein, nachzuweisen, dass die notwendigen Maßnahmen ergriffen werden, damit diese Daten nicht gelöscht, verändert oder verbreitet werden, vermittelt Transparenz, die zum einen von der DSGVO verlangt wird und zum anderen dem Unternehmen hilft, mehr Vertrauen zu gewinnen.

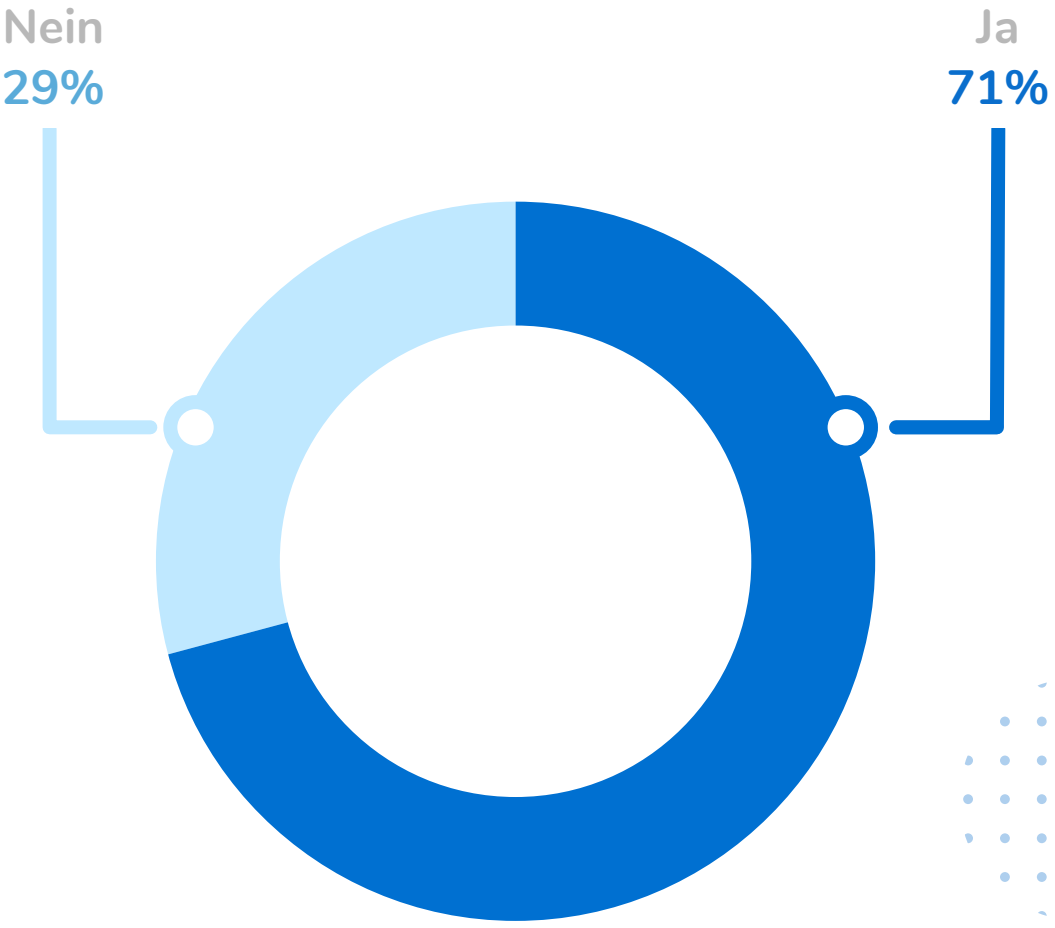
Deutschland spiegelt mit einem Ergebnis von 67% Ja und 33% Nein den Mittelwert wider, während das Interesse am Datenschutz der Patienten und Kunden in **Spanien** fast 10% höher, in **England** jedoch 10% niedriger ermittelt wurde.

> *"67% der Befragten gaben an, dass sich ihre Patienten/Kunden nach dem Datenschutz erkundigen, was zeigt, dass in der Bevölkerung das Bewusstsein über die Wichtigkeit des Datenschutzes zunimmt, was die Einhaltung des Datenschutzes nicht nur zu einer Verpflichtung, sondern auch zu einer Garantie für Qualität und Vertrauen für die Kunden macht".*

Lisa Hofmann | Chief of Legal Operations, Pridatect

Frage 5

Interessieren sich Ihre Patienten/Kunden für den Grund der Erfassung ihrer persönlichen Daten?



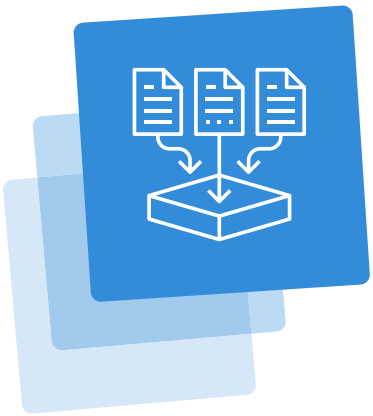
Ein wesentlicher Bestandteil der DSGVO ist das Recht des Einzelnen, über die Erhebung und Verwendung seiner persönlichen Daten informiert zu werden. Mit dieser Frage konnten wir erkennen, dass die überwiegende Mehrheit der Patienten wissen möchte, warum ihre Daten erhoben werden.

71% der befragten deutschen Unternehmen gaben an, von ihren Kunden/Patienten nach dem Grund der Erfassung ihrer Daten befragt zu werden, während 29% die Notwendigkeit der Datenverarbeitung nicht hinterfragen. Ähnliche Ergebnisse zeigten sich in den anderen befragten Ländern.

Die Patienten geben sich nicht damit zufrieden, ihre persönlichen Daten einfach herauszugeben, sondern wollen wissen, warum diese benötigt werden und was mit ihnen geschieht.

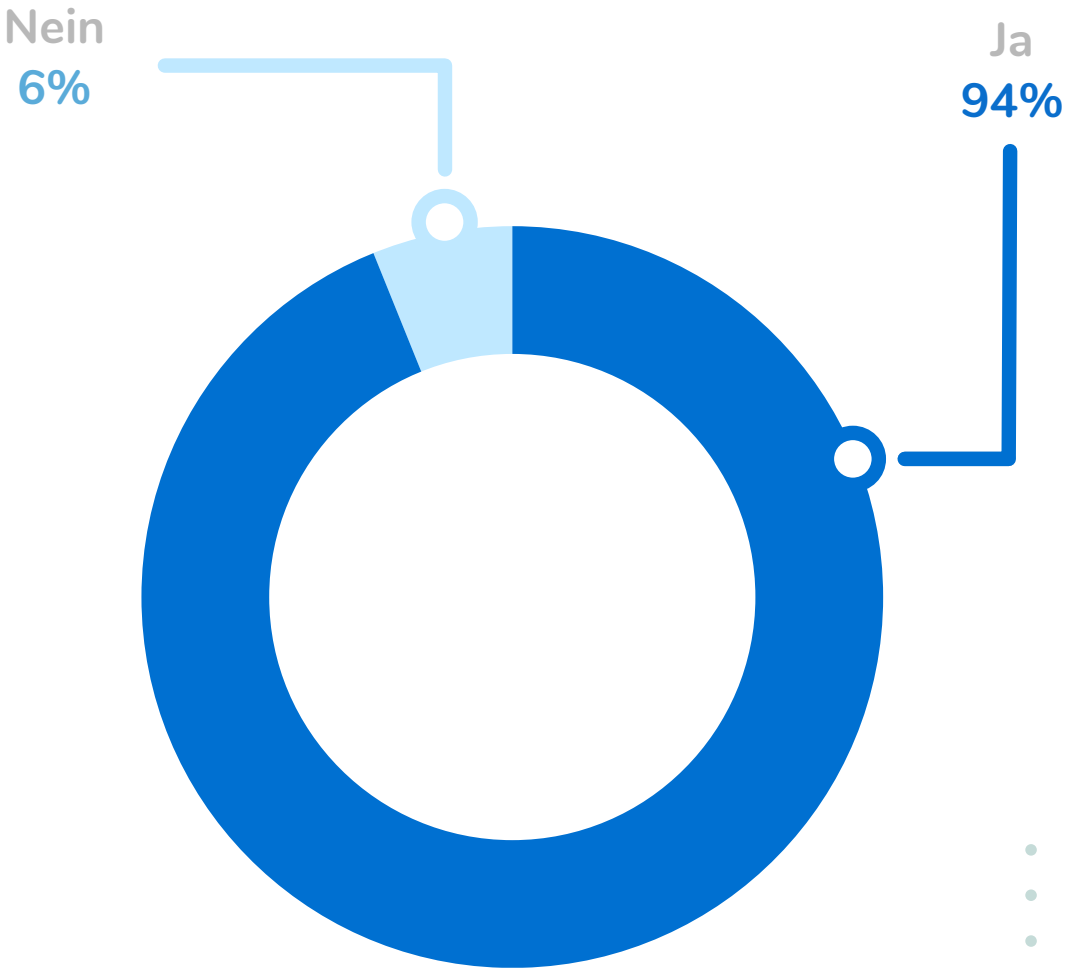
Deshalb muss es **Datenschutzrichtlinien und Einverständniserklärungen** geben, damit die Betroffenen klar erkennen können, für welchen bestimmten **Zweck oder aus welchem Grund ihre Daten erhoben und verarbeitet werden, wie lange diese gespeichert werden und an welche Empfänger diese Daten gehen.** Der Patient oder Kunde muss seine Einwilligung in freier, spezifischer, informierter und eindeutiger Weise aktiv geben können.

Andererseits ist auch die Notwendigkeit der Datenerhebung durch Gesundheitsorganisationen nachvollziehbar: Sie hilft ihnen, die bestmögliche Patientenversorgung zu gewährleisten. Doch trotz dieser Notwendigkeit sollte nicht vergessen werden, dass dies zum Zeitpunkt der Datenerhebung mitgeteilt und erklärt werden muss.



Frage 6

Informiert Ihre Organisation Patienten/ Kunden darüber, wie ihre persönlichen Daten behandelt werden?



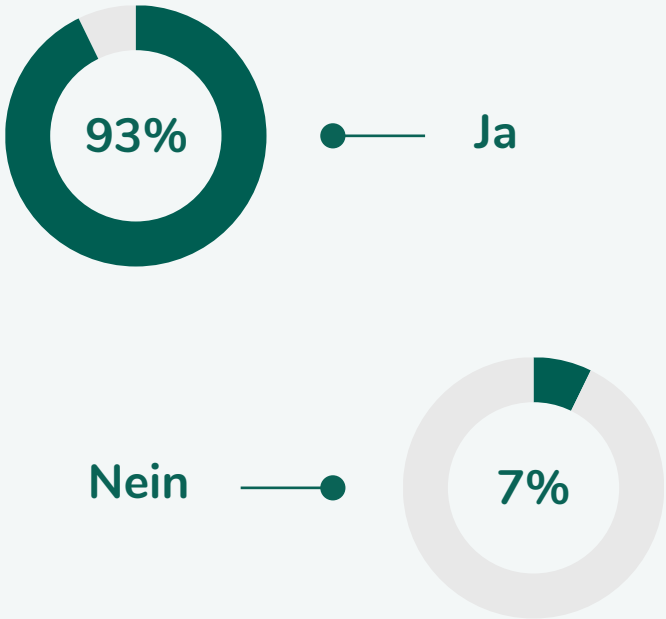
Wie in der vorherigen Frage erläutert, **wollen die meisten Patienten/Kunden wissen, wie und warum ihre Daten verarbeitet werden.** Daher haben wir gefragt, inwieweit die Organisationen diesem Interesse selbstständig entgegenkommen. 94% der befragten Organisationen informieren die Betroffenen eigenständig darüber, wie ihre persönlichen Daten behandelt werden. 6% der Organisationen geben an, Ihre Patienten/Kunden nicht darüber zu informieren, was mit den Daten geschieht. Deutschland spiegelt damit den Durchschnittswert wider.

Dass diese Grundvoraussetzung der DSGVO von 6% der befragten deutschen Organisationen nicht erfüllt wird, gibt Anlass zur Sorge. Die Betroffenen über die Verarbeitung ihrer Daten aufzuklären ist kein kompliziertes Verfahren und die Nichteinhaltung der Informationspflicht **kann zu Vertrauensverlust und hohen Sanktionen führen.** Noch problematischer wird es, wenn Patienten/Kunden nicht nur nicht informiert werden, sondern ihre Daten zudem auch für andere Zwecke als den offensichtlichen verwendet werden. Transparent im Bezug auf die Verarbeitung der erhobenen Daten zu sein wirkt sich auf jeden Fall positiv auf das Vertrauen der Patienten gegenüber dem Unternehmen aus.

"Organisationen werden sich zunehmend bewusst, wie sie mit den personenbezogenen Daten der Beteiligten, mit denen sie interagieren, umgehen müssen *(Patienten, Kunden, Lieferanten, Arbeitnehmer usw.). Daher kommen 94% der Organisationen der Informationspflicht bei der Verarbeitung von Daten nach."*

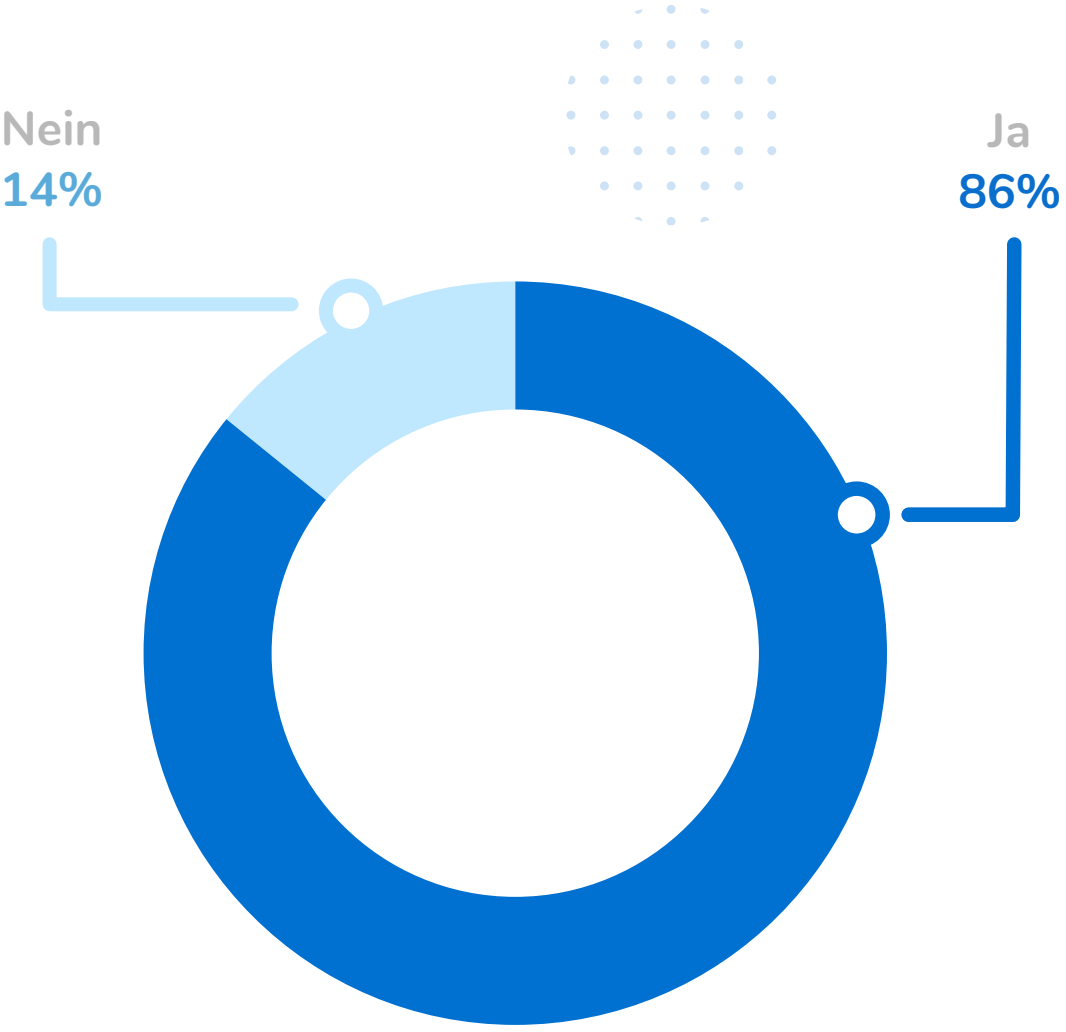
Charles Maddy-Trevitt |
Datenschutzexperte, Pridatect

Das gesamteuropäische Ergebnis zeigt, dass 93% der befragten Unternehmen seine Kunden informiert, während 7% gegen diese Vorschrift verstößt



Frage 7

Holen Sie die Zustimmung Ihrer Nutzer (von Kunden/Mitarbeitern/Lieferanten) zur Datenverarbeitung ein?



Welche Art von persönlichen Daten kann ein Unternehmen sammeln?

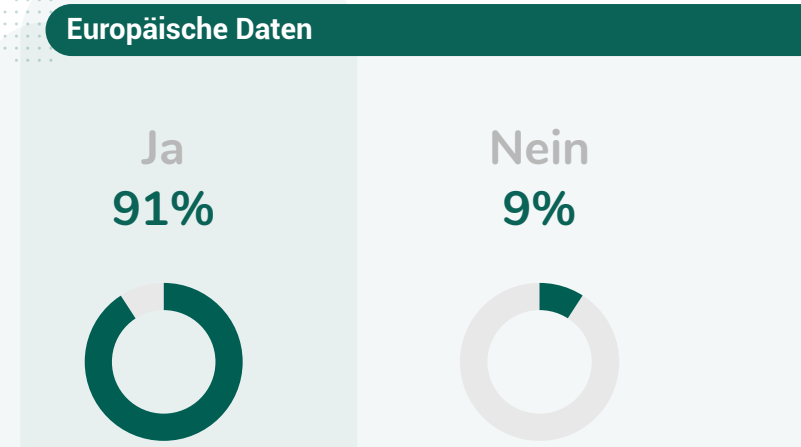
Vor- und Nachname, Alter, Adresse, Hinweise auf Bedürfnisse aufgrund von Dienstleistungen, die Kunden und Patienten in Anspruch nehmen und vieles mehr.

Insbesondere im Gesundheitsbereich stoßen wir auf besonders sensible Daten, wie beispielsweise Testergebnisse, Anamnese, akute Krankheiten, oder medikamentöse Behandlungen.

Es ist fast unvermeidlich, diese Art von sensiblen Daten zu erfassen und festzuhalten. Dafür bedarf es einer legalen Grundlage, die zumeist durch Einverständnis erteilt wird.

Fehlendes Einverständnis bei der Datenverarbeitung ist einer der gröbsten Verstöße gegen die DSGVO. Im Kontrast zur vorherigen Frage gaben nur 86% der deutschen Organisationen an, sich vor der Datenverarbeitung die Zustimmung der Betroffenen einzuholen. 14% gaben an, die Daten ohne explizites Einverständnis ihrer Patienten/Kunden zu verarbeiten. Die Aufklärung der Patienten und Kunden über die Verarbeitung ihrer Daten sollte bestenfalls mit einem Einverständnis seitens der Betroffenen einhergehen.

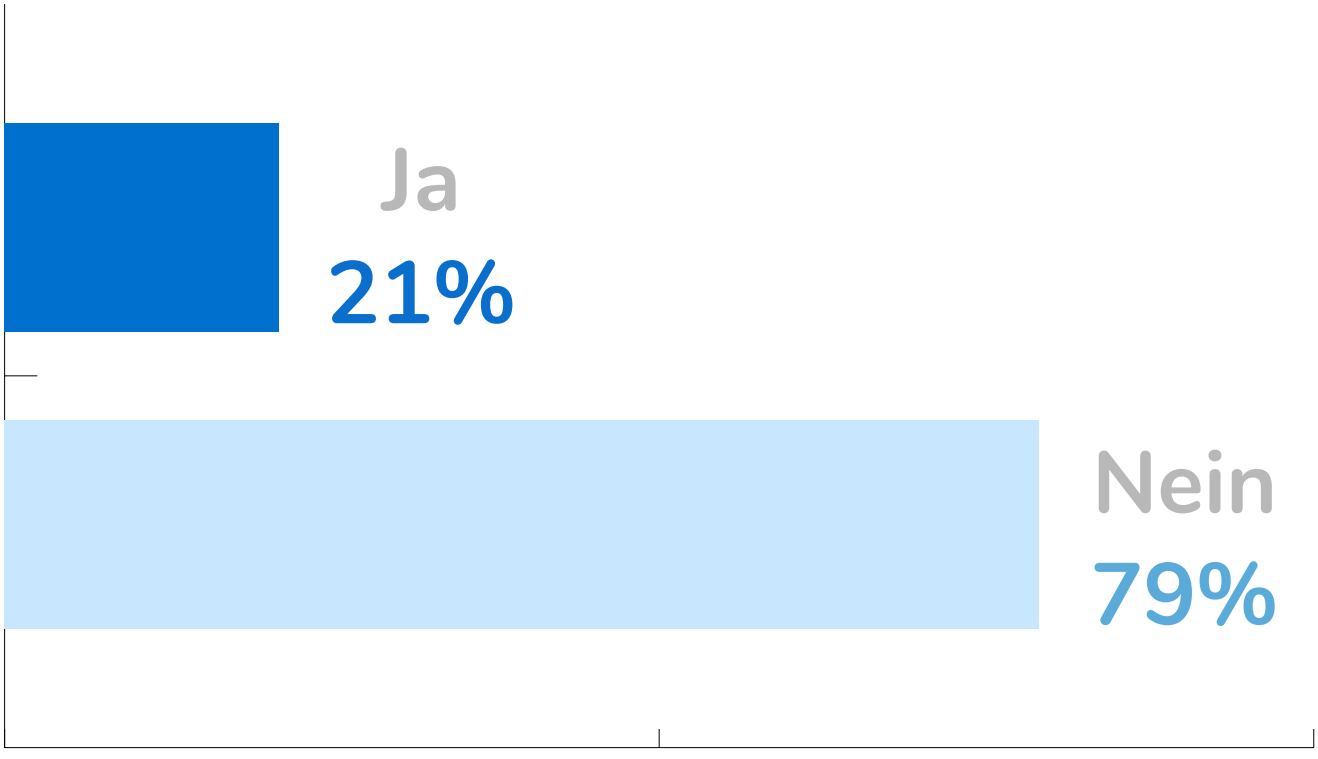
Die Daten auf europäischer Ebene sind ähnlich: 91% holen sich das Einverständnis ihrer Kunden ein, 9% tun dies nicht, womit einer der Grundsätze der DSGVO missachtet wird.



Nur wenige Umstände erlauben, Kunden/Patienten nicht über die Datenverarbeitung zu informieren, sodass es in jeder Situation ratsam ist, diese klar und deutlich zum Zeitpunkt der Datenerhebung zu kommunizieren: Zweck, Speicherdauer und Empfänger anzugeben und sich die entsprechende Zustimmung einzuholen, welche frei, spezifisch, fundiert und unmissverständlich sein muss.

Frage 8

Gibt Ihre Organisation personenbezogene Daten an Dritte weiter?



Nur 21% der befragten Organisationen gaben an, die personenbezogenen Daten an Dritte weiterzugeben. 79% behaupteten, die Daten nur selbst zu verarbeiten.

Im europäischen Vergleich steht Deutschland damit ganz hinten: Im Durchschnitt **gaben 32% aller befragten Unternehmen in Europa an, die Daten mit Dritten zu teilen.**

Trotz der Tatsache, dass mehr Unternehmen ihre Daten nur intern verarbeiten, ist die **unternehmensübergreifende Datenverarbeitung weiter verbreitet, als wir denken.**

Unter Umständen können sogar Vereinbarungen über die Übertragung von Daten getroffen werden, bei denen eine Organisation einer anderen technische Maßnahmen für die Verarbeitung von Daten zur Verfügung stellt. Dies würde unweigerlich eine spezifische und unzweideutige Zustimmung erfordern, die durch einen gesetzlichen Vertrag festgelegt wird.

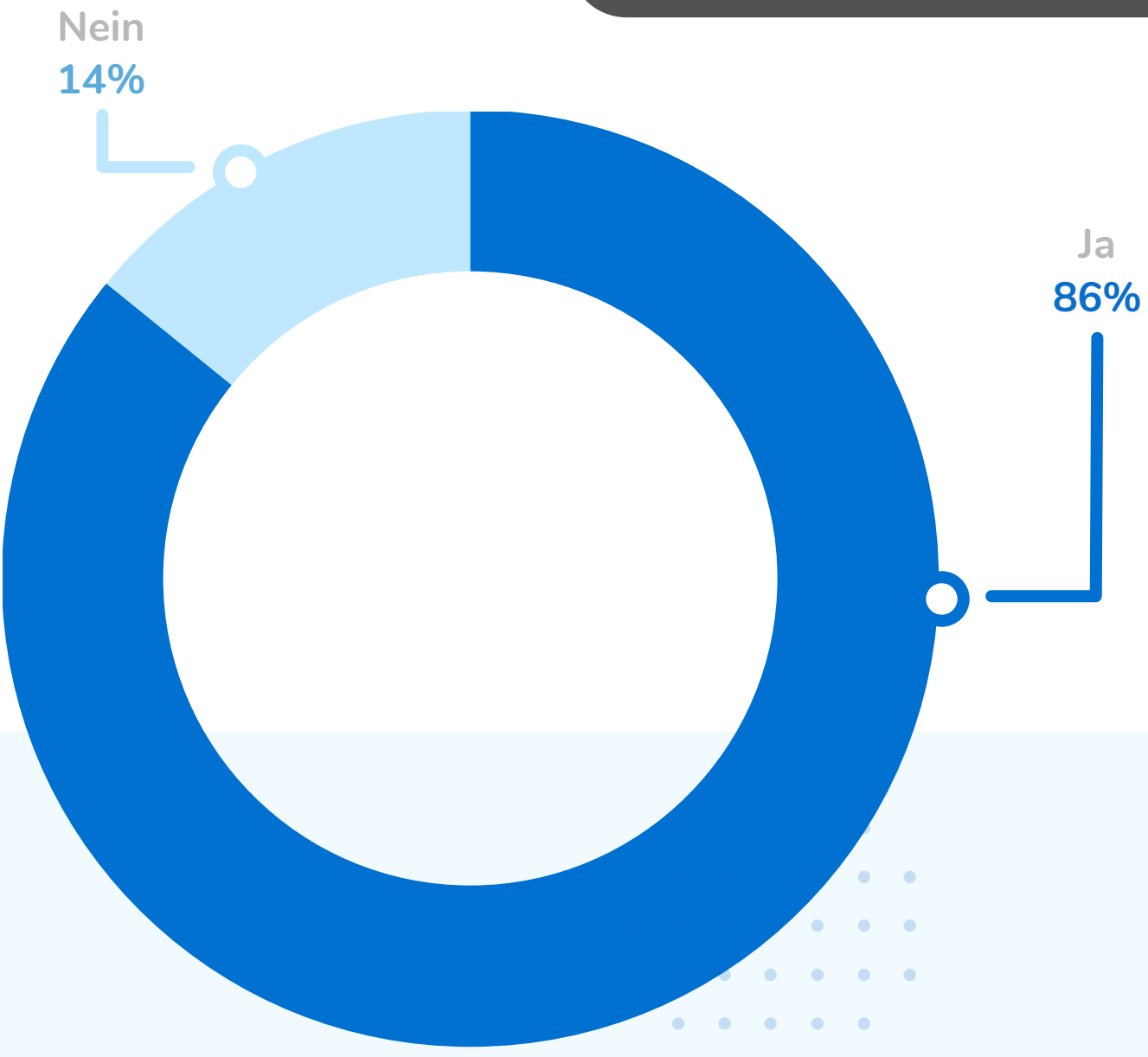
Auch wenn die Übermittlung von Daten an Dritte keine übliche Praxis ist, kann es doch gelegentlich vorkommen, **dass auf die Unterstützung einer dritten Partei zurückgegriffen werden muss:** Ein Gesundheitszentrum, das die Tests eines Patienten zur Analyse an ein Labor senden muss, oder eine Zahnklinik, die die Daten und Messungen eines Patienten für die Herstellung von zahnmedizinischen Materialien weiter leitet. Aber auch schon eine Softwareanwendung stellt einen weiteren Empfänger dar, der zumindest Einsicht in die gespeicherten Daten hat, sodass es notwendig ist, die Datenverarbeitung vertraglich festzulegen und einen Verantwortlichen zu benennen.

Frage 9

Haben Sie Drittempfänger vor Weitergabe der Daten Verschwiegenheitserklärungen unterzeichnen lassen?

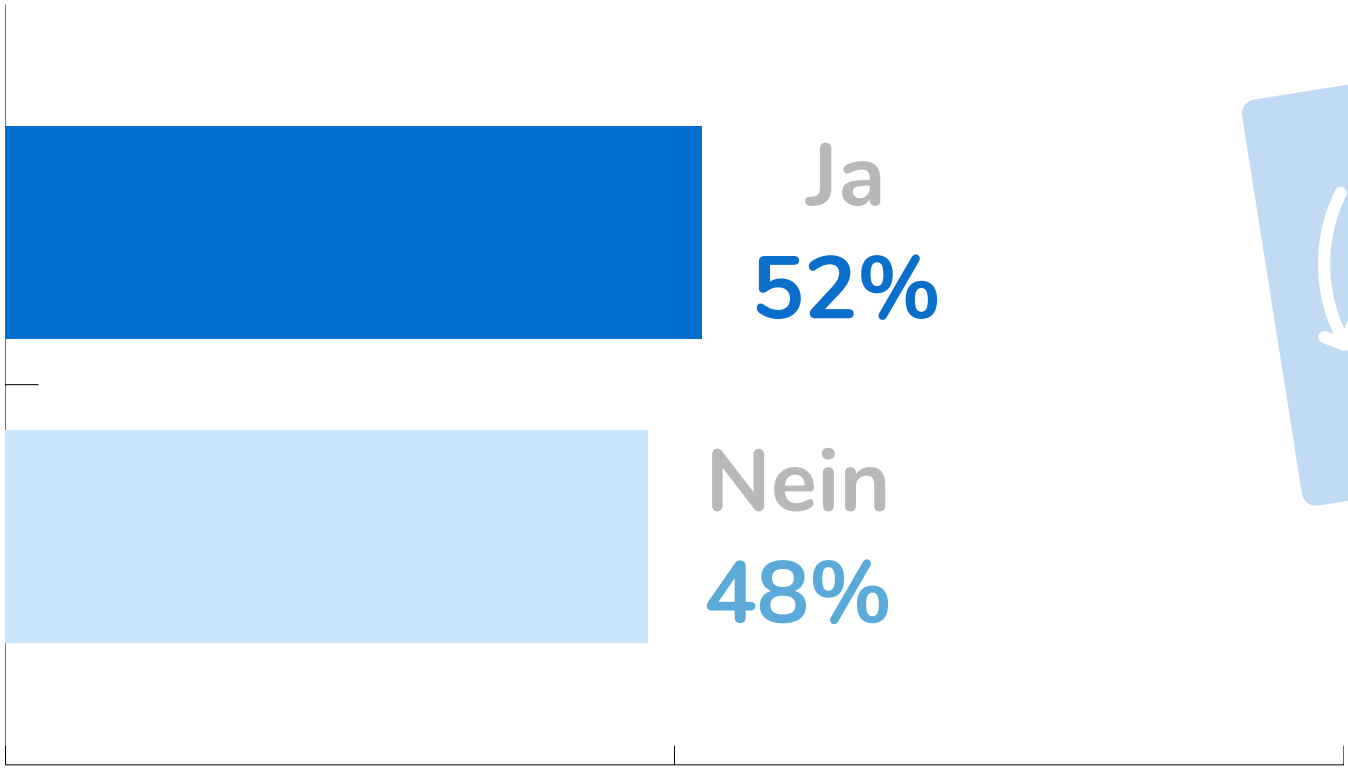
86% der Organisationen, die Daten an Dritte weitergeben, lassen vor der Weitergabe eine Vertraulichkeitsvereinbarung unterzeichnen und legen daher im Vorfeld die Verpflichtungen und Einschränkungen fest, während 14% diesen wichtigen Schritt überspringen, wodurch Dritte die Möglichkeit haben, frei mit den Daten umzugehen.

Es ist von entscheidender Bedeutung, **die Verpflichtung des Unternehmens**, an welches die Daten weitergegeben werden, **schriftlich und unter Berücksichtigung der rechtlichen Anforderungen festzulegen,** die Vertraulichkeit zu wahren **und diese Informationen nicht für andere als die im Vertrag festgelegten Zwecke zu verwenden.**



Frage 10

Hat Ihre Organisation in den letzten 12 Monaten eine neue Softwarelösung für die Verarbeitung von Gesundheitsdaten implementiert?

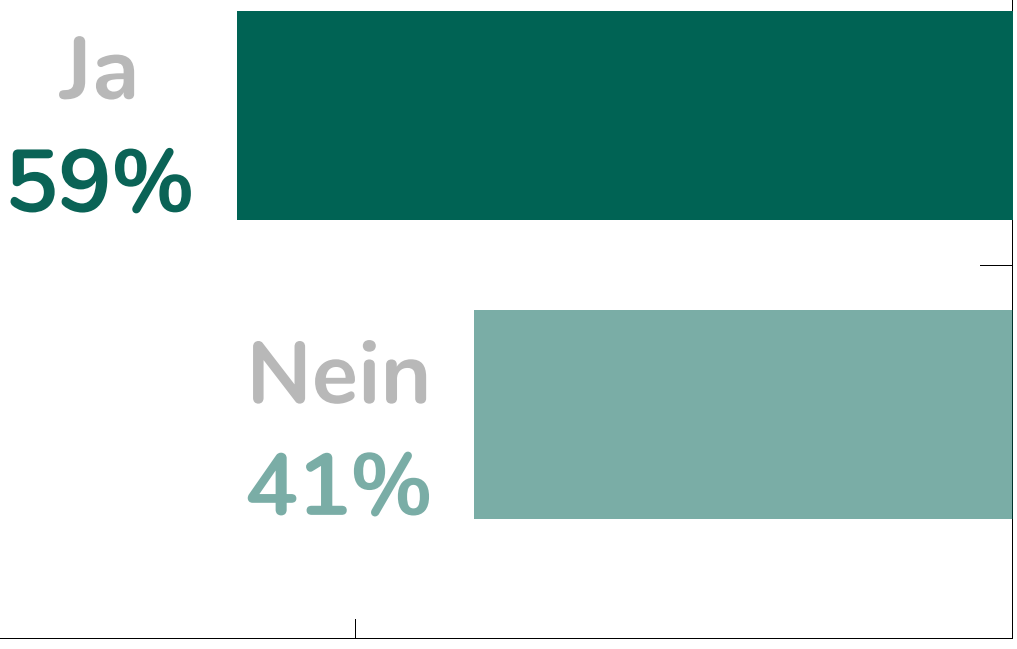


Etwa die Hälfte aller Befragten, 52% der Unternehmen im Gesundheitswesen, haben in den letzten 12 Monaten neue Softwarelösungen implementiert, die Gesundheitsdaten verarbeiten. 48% der Befragten nutzen weiterhin ihre bisherigen Softwares oder nutzen manuelle Prozesse zur Verarbeitung sensibler Gesundheitsdaten.

Da die Verarbeitung von Gesundheitsdaten unter die Kategorie besonders sensibler Daten nach DSGVO fällt, ist in diesem Fall immer die **Durchführung einer Datenschutz-Folgenabschätzung ratsam**. Es müssen die mit der Verarbeitung der Daten verbunden Risiken ermittelt und bewertet werden, sowie geeignete Technische und Organisatorische Maßnahmen implementiert werden, um diese zu mindern.

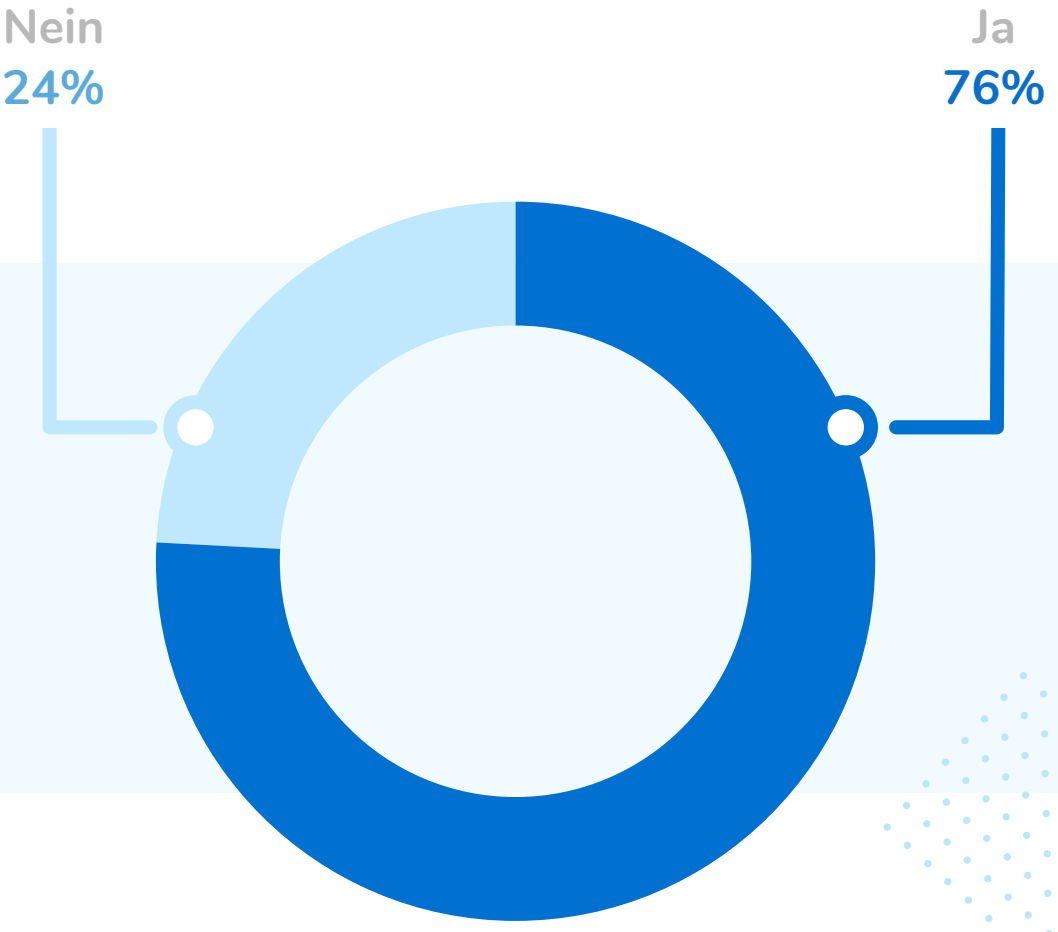
Im europäischen Durchschnitt zeigt sich, dass 59% aller Organisationen in den letzten 12 Monaten neue Softwarelösungen zur Verarbeitung sensibler Daten implementiert haben. Im europäischen Vergleich zeigt sich, dass deutsche Organisationen am wenigsten auf neue Technologie zurückgreifen.

Europäische Daten



Frage 11

Hat Ihre Organisation einen Datenschutz-beauftragten ernannt?



Die Abschnitte 37 und 39 der DSGVO regeln die Verpflichtung, in bestimmten Fällen oder für bestimmte Arten von Unternehmen einen Datenschutzbeauftragten zu benennen. Dazu gehören: Öffentliche Einrichtungen, Organisationen, die Daten in großem Umfang verarbeiten und Unternehmen, die als Gesundheitszentren kategorisiert sind und sensible Patientendaten verarbeiten. Somit ist die Ernennung eines DSB für viele Unternehmen des Gesundheitssektor obligatorisch.

Erst im vergangenen Jahr 2019 wurde die deutsche Einheit von **Facebook Inc. mit einer Geldstrafe von 51.000 Euro** (55.500 US-Dollar) belegt, weil man zwar dem Team der Hauptniederlassung in Dublin die Rolle des Datenschutzbeauftragten für alle europäischen Tochterunternehmen übertragen hatte, es aber **versäumt hatte, dies der Behörde in Hamburg mitzuteilen**. Diese Geldstrafe wurde als "Warnung" ausgesprochen, denn Verstöße gegen die DSGVO können nach Art. 83 zu Geldbußen in Höhe von 4% des Umsatzes des letzten Geschäftsjahres oder 20 Millionen Euro betragen.

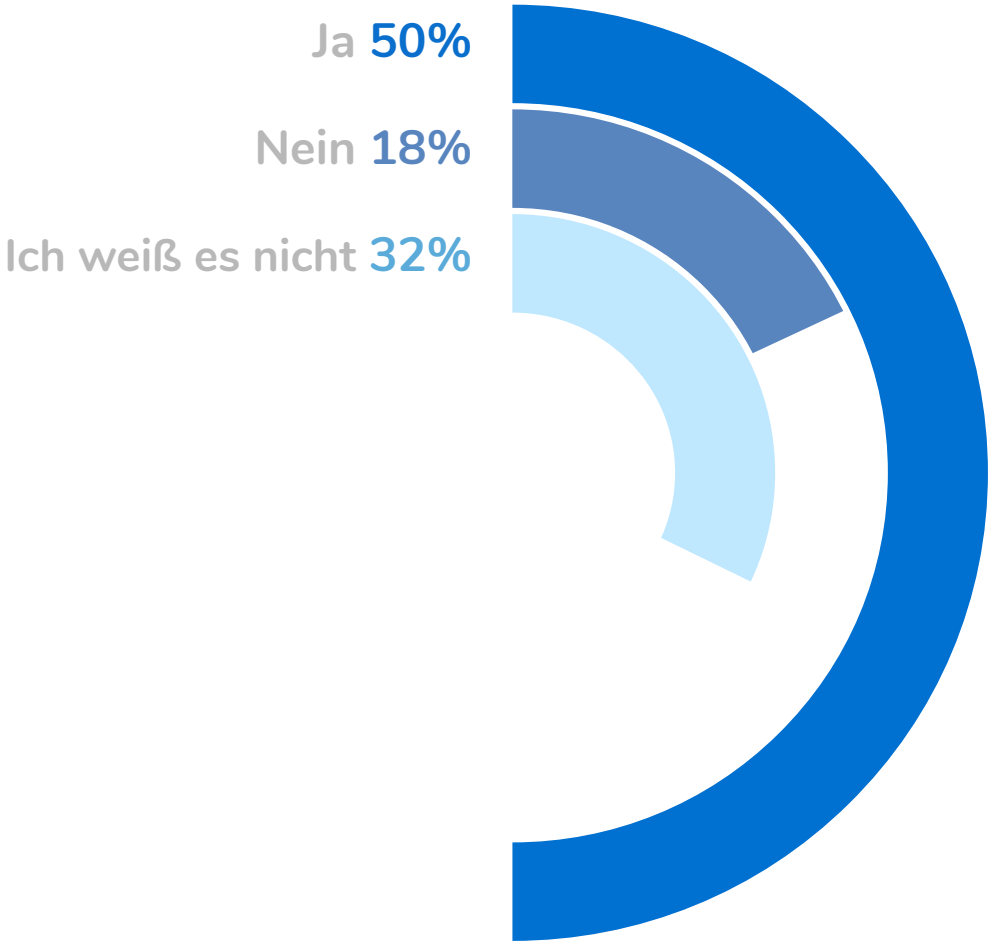
Einen Datenschutzbeauftragten zu benennen ist von entscheidender Bedeutung, um die Einhaltung der Vorschriften zu gewährleisten. Sobald sensible Daten verarbeitet werden, spielt es keine Rolle, wie groß das Unternehmen ist: Rechtfertigungen, dass das eigene Unternehmen "zu klein" sei und solche Maßnahmen für "übertrieben" gehalten werden, haben keinen Wert und schützen vor Strafe nicht.

Es darf ein Unternehmensmitglied sein, sollte aber in jedem Falle ein Datenschutzexperte sein. **Der DSB fungiert als Anlaufstelle, Verantwortlicher und Vermittler** für die zuständigen Behörden und als Berater des für die Datenverarbeitung Verantwortlichen - das Unternehmen - in Bezug auf Verpflichtungen und die Überwachung der Einhaltung der Vorschriften. **Ein DSB hilft dabei, sicherzustellen, dass die Prozesse des Unternehmens mit den neuesten Vorschriften und Richtlinien in Einklang stehen,** zeigt aber auch die Bereitschaft und die Bemühungen des Unternehmens, Compliance zu erreichen.

Es zeigt sich, dass 24% der Organisationen keinen Datenschutzbeauftragten ernannt haben und damit möglicherweise gegen die Gesetzgebung verstoßen. **24% der deutschen Organisationen laufen demnach Gefahr,** Sicherheitsproblemen ausgesetzt zu sein, das Vertrauen ihrer Kunden/Patienten zu riskieren und hohe Geldstrafen auferlegt zu bekommen.

Frage 12

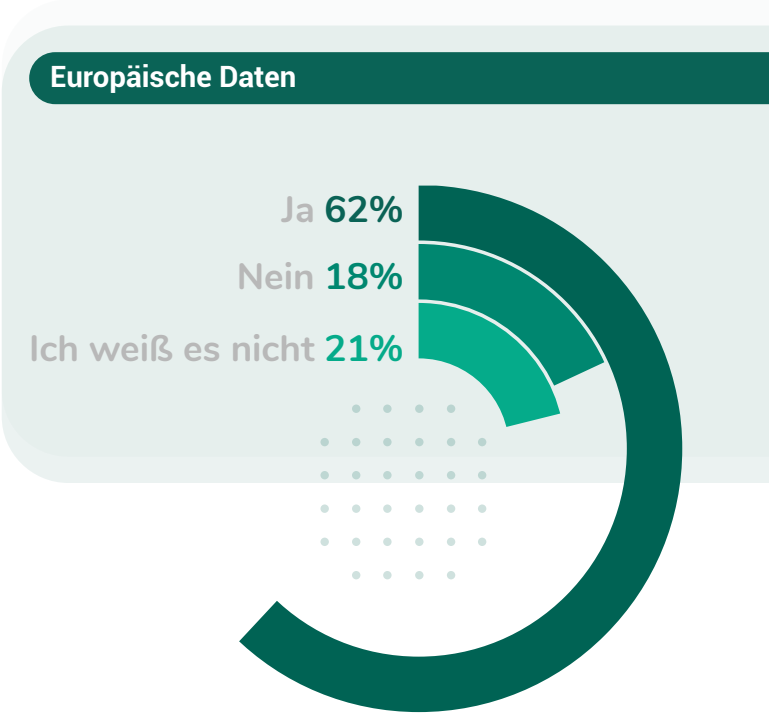
Hat Ihre Organisation eine Datenschutz-Folgenabschätzung durchgeführt, um die Risiken, denen die Daten, mit denen Sie arbeiten, ausgesetzt sind, zu identifizieren und zu bewerten?



Einer der wichtigsten Schritte, um den Datenschutz in einer Organisation zu gewährleisten, **ist die Durchführung von Datenschutz-Folgenabschätzungen.** Als Gesundheitsspezialist, Gesundheitszentrum oder Firma der Gesundheitsbranche verarbeitet man sensible Daten und muss sich dem Ausmaß aller möglicher Risiken und potentieller Schäden, die bei Sicherheitsproblemen im Datenschutz entstehen können, im Vorhinein bewusst sein.

In dieser Studie wollten wir wissen, **wie viele Unternehmen im Gesundheitssektor eine Datenschutz-Folgenabschätzung durchgeführt haben:** 50% der Befragten haben diese Frage bejaht, 18% haben keine Datenschutz-Folgenabschätzung durchgeführt und ganze 32% waren sich nicht sicher. Im Durchschnitt haben 62% der Organisationen in Europa eine DSFA durchgeführt, 21% wussten dies nicht mit Sicherheit zu bestätigen.

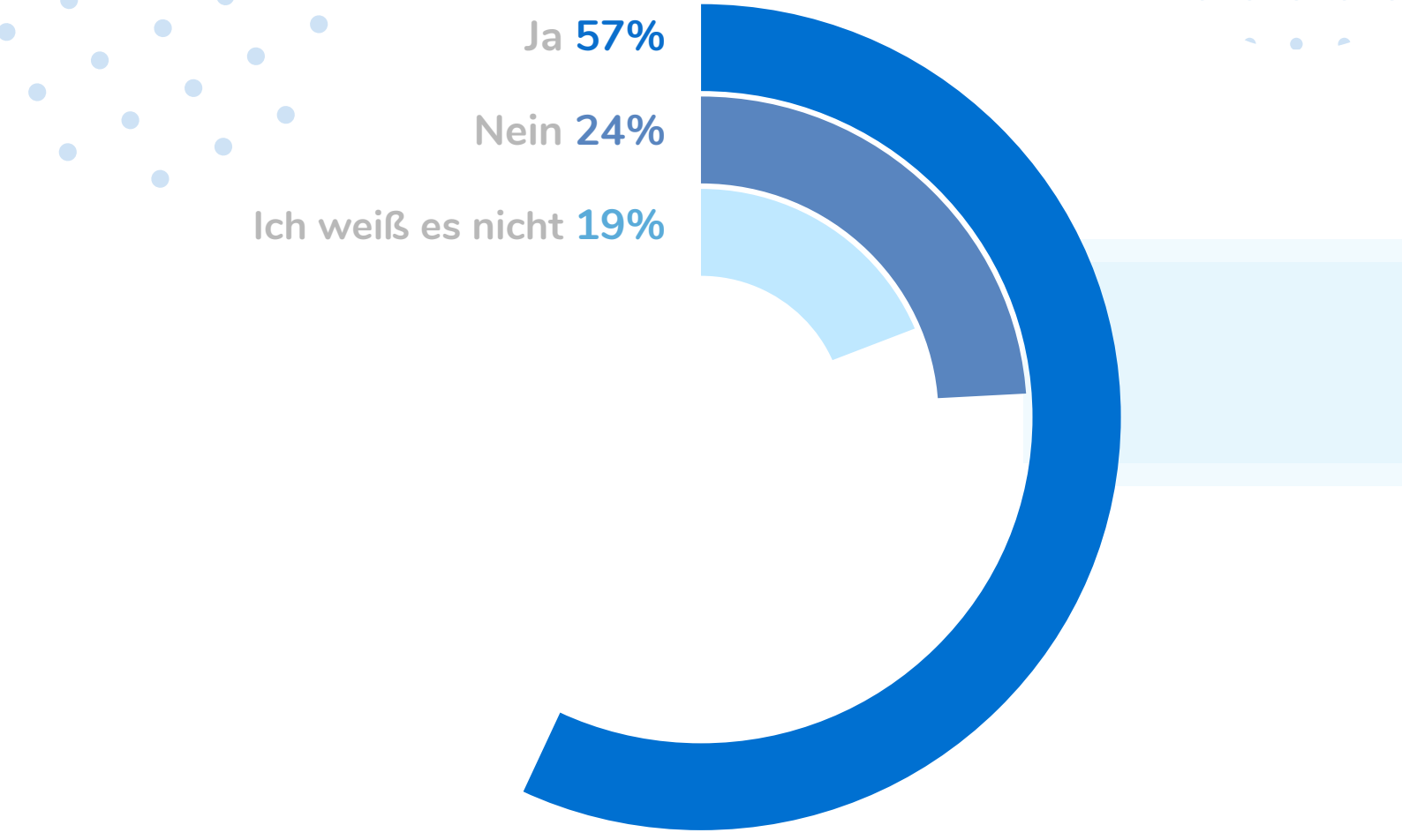
Kann diese Unsicherheit daher kommen, dass sie keinen DSB benannt haben, oder sogar daran, dass sie zwar einen DSB benannt haben, sich aber nicht im Klaren darüber sind, was dieser für ihr Unternehmen tut? Zeigt sich hier ein Mangel an Transparenz?



Nur die Hälfte aller befragten deutschen Unternehmen hat eine Datenschutz-Folgenabschätzung durchgeführt. Mit diesem Ergebnis steht Deutschland im europäischen Vergleich an letzter Stelle und auch was die Unwissenheit über den Datenschutz-Stand des eigenen Unternehmens betrifft, wussten gleich doppelt so viele Unternehmen nicht, ob sie jemals eine DSFA durchgeführt haben.

Frage 13

Führen Sie ein aktualisiertes Verzeichnis der Verarbeitungstätigkeiten?



Nach **Art. 30 DSGVO** muss jedes Unternehmen alle seine **Verarbeitungstätigkeiten dokumentieren**. Dies ist eine Grundvoraussetzung, die für jedes Unternehmen gilt, unabhängig von der Art oder Menge der verarbeiteten Daten, oder der Anzahl der Mitarbeiter. Ein bestimmtes Format ist dafür nicht vorgeschrieben, das Verzeichnis muss jedoch **fortlaufend** mit jeder Veränderung im Unternehmen **aktualisiert** werden.

Das Verzeichnis der Verarbeitungstätigkeiten muss folgende Informationen beinhalten:

- **Name und Kontaktdaten** aller an der Datenverarbeitung Beteiligten
- **Zweck** der Verarbeitung
- **Kategorien der verarbeiteten Daten, der betroffenen Personen und der Empfänger,** an welche die personenbezogenen Daten weitergegeben wurden oder weitergegeben werden sollen, einschließlich der Empfänger in Drittstaaten
- **Dauer der Datenspeicherung**
- Eine Übersicht der implementierten **Technischen und Organisatorischen Maßnahmen**

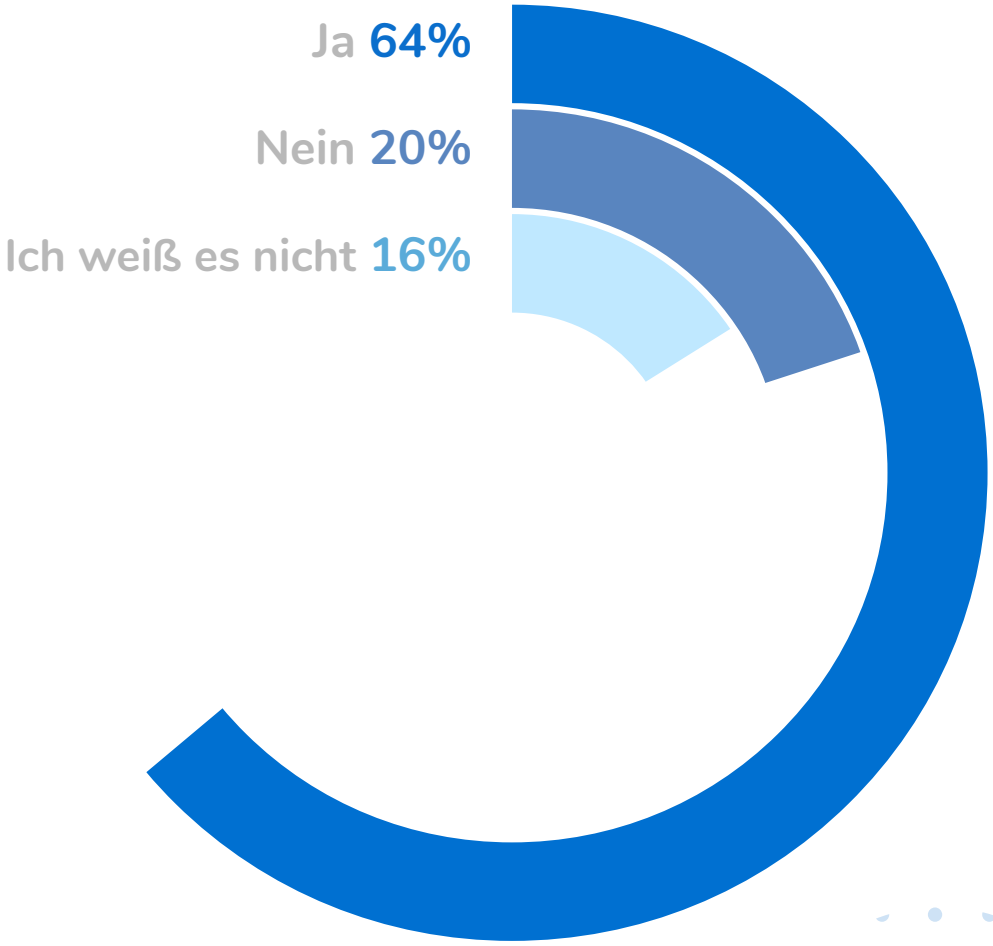
Die Nichteinhaltung dieser DSGVO Vorschrift kann zu Geldstrafen von bis zu **10 Millionen Euro** oder 4% der Gesamteinnahmen des Unternehmens führen.

57% der befragten deutschen Unternehmen bestätigten, ein aktualisiertes Verzeichnis der Verarbeitungstätigkeiten zu führen, **24%** gaben an, keines zu haben und ganze **19%** waren sich unsicher.

Bei der Erstellung des Verzeichnisses der Verarbeitungstätigkeiten müssen müssen Datenschutzberater und Unternehmen zusammenarbeiten. Dass 19% der befragten Unternehmen nicht wissen, ob sie ein solches Verzeichnis erstellt haben, lässt vermuten, dass sie letztentlich zu den 24% zu addieren sind, die mit “Nein” geantwortet haben, womit beinahe die Hälfte aller befragten deutschen Unternehmen gegen diese DSGVO Vorschrift verstoßen.

Frage 14

Haben Sie technischen und organisatorischen Maßnahmen in Ihrer Organisation definiert und implementiert, um die Risiken jeder Verarbeitungstätigkeit zu mindern und somit Sicherheitsmaßnahmen zu definieren?

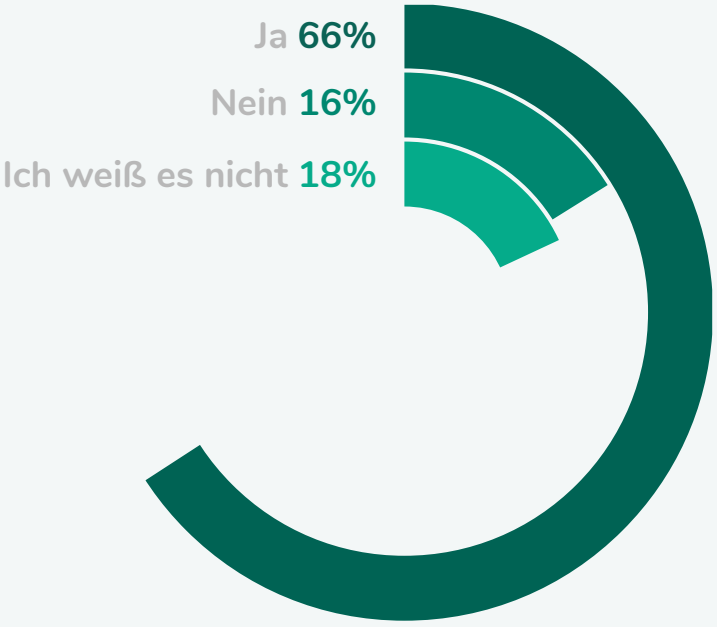


Die Implementierung von Technischen und Organisatorischen Maßnahmen hilft dabei, die Sicherheit der verarbeiteten Daten zu gewährleisten: Wo potentielle Risiken identifiziert werden, helfen TOMs, diese zu mindern und zu vermeiden.
64% der Befragten gaben an, TOMs in Ihrem Unternehmen implementiert zu haben, 20% der Befragten verneinten und die restlichen 16% wussten diese Frage nicht sicher zu beantworten.

Artikel 32 DSGVO schreibt vor, dass alle Unternehmen geeignete Technische und Organisatorische Maßnahmen implementieren müssen und diese auch nachweisen können muss, um nicht gegen die Vorschriften zu verstoßen und zu zeigen, dass alles Mögliche getan wurde, um die verarbeiteten Daten nicht zu gefährden.

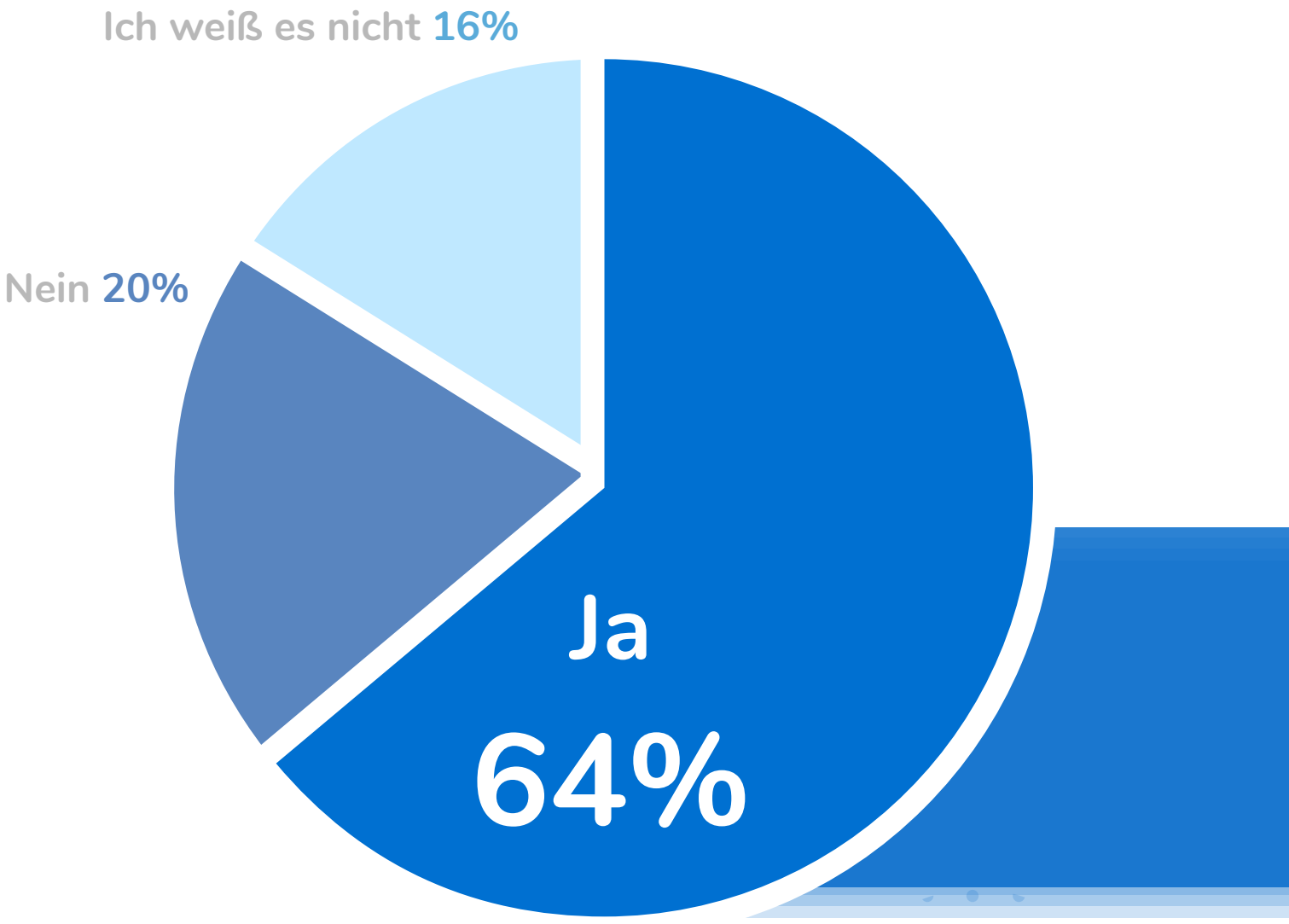
Sich dieser Verantwortung zu entziehen, kann Sanktionen zur Folge haben und nach dem, was wir in dieser Studie gesehen haben, gehen viele Zentren oder Unternehmen dieses Risiko immer noch ein.

Das Ergebnis auf europäischer Ebene zeigt uns, dass 66% aller befragten Organisationen technische und organisatorische Maßnahmen implementiert haben, 16% dies nicht getan haben und 18% es nicht genau wissen.



Frage 15

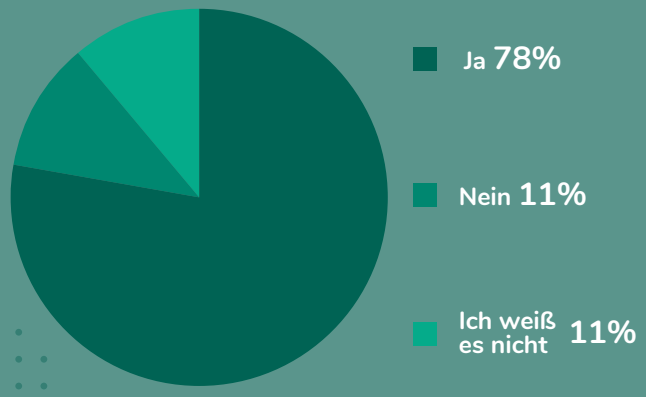
Verfügt Ihre Organisation über ein Aktionsprotokoll für den Fall einer Datenpanne (Diebstahl, Verlust, Datenänderung etc.) ?



Datenpannen können in jedem Unternehmen passieren. Von Verlust oder Änderung der Patientendaten bis hin zu Zugriff von Unbefugten. Wo Daten verarbeitet werden, entstehen Risiken und es gilt, sich diesen bewusst zu sein und sich entsprechend vorzubereiten, falls sie eintreten. Daher ist es wichtig, ein Protokoll oder einen Aktionsplan zu haben und zu wissen, wie bei einer Datenpanne zu handeln ist.

Artikel 33 DSGVO schreibt vor, dass Datenpannen innerhalb von 72 Stunden an die zuständige Behörde zu kommunizieren sind. Es ist daher fundamental, **Prozesse** zum Management von Datenpannen schon **im Vorhinein definiert zu haben, um so schnell wie möglich,** innerhalb der gesetzlich vorgegebenen Frist von 72 Stunden **zu handeln, um Schäden zu minimieren und Geldstrafen zu vermeiden.**

Im europäischen Durchschnitt zeigt sich, dass 78% der Unternehmen auf Datenpannen vorbereitet sind, während 22% es nicht genau wissen, oder direkt angeben, keine Prozesse festgelegt zu haben.



Nur 64% aller Unternehmen gaben an, Aktionspläne oder Prozesse vorbereitet zu haben, nach denen sie sich im Falle einer Datenpanne richten können, um das Ausmaß der Folgen so minimal wie möglich zu halten. 20% der Befragten haben sich nicht mit dem Management von Datenpannen beschäftigt und 16% der Befragten wissen nicht sicher darauf zu antworten, was darauf schließen lässt, dass es keine Aktionspläne für Sicherheitspannen gibt.

04. Beispiel Psious: Implementierung von Datenschutzstandards im Gesundheitssektor

Psious ist eine Virtual-Reality-Lösung zur Behandlung zahlreicher verschiedener Krankheiten wie Angststörungen, Phobien, Esstörungen, ADHS uvm. Sie hilft Therapeuten und Therapeuten und psychiatrischen Fachkräften, ihre Patienten besser zu verstehen und zu behandeln. Mit Hilfe einer VR-Brille kann der Patient in verschiedene Situationen oder Umgebungen versetzt werden. Der behandelnde Experte hat jederzeit Einsicht darauf, was der Patient sieht, fühlt und wie das Angstlevel ausschlägt.

Solche Hilfsmittel speichern eine **große Menge an Daten über den Patienten, von denen viele sensibler Natur sind,** sodass es unverzichtbar ist, die Sicherheit dieser Daten zu gewährleisten um das Vertrauen der Patienten zu wahren

Psious ist sich bewusst, dass die von ihnen verarbeiteten Daten von äußerst sensibler Natur sind. Jedes Unternehmen sollte sich an die DSGVO Vorschriften halten, aber diese Verpflichtung wird umso wichtiger, je sensibler die erhobenen Daten sind. Ein Verlust oder eine **Verlust oder eine Modifikation dieser kann die Arbeit der behandelnden Fachleute behindern, die Privatsphäre des Patienten gefährden und und dem Ruf des Unternehmens schaden,** zusätzlich drohen in solchen Fällen erhebliche Bußgelder.

Viele der Nutzer von Psious sind Psychologen, die die Sitzungen ihrer Patienten abspeichern. Daher ist es für sie von wesentlicher Bedeutung, die Sicherheit dieser Daten zu garantieren; sowohl um Bußgelder zu vermeiden, als auch um ihre Patienten zu schützen und ihre Verantwortung, die Privatsphäre dieser zu wahren, ernst zu nehmen.

Eine weitere Herausforderung für Psious war es, die Einhaltung der verschiedenen internationalen Vorschriften zum Datenschutz sicher zu stellen. Datenschutzkonform zu arbeiten wird umso komplizierter, in je mehr Ländern man arbeitet, da jedes Land seine eigenen unterschiedlichen Spezifikationen und Standards hat. Psious hat eine große Zahl von Kunden in Ländern wie den Vereinigten Staaten, wo nicht die **DSGVO,** sondern die **HIPAA** Vorschriften eingehalten werden müssen. Für die dort ansässigen Kunden ist es eine Grundvoraussetzung, dass Psious ihre Daten nach den dort geltenden Regelungen schützt.

> "In unserer Branche verarbeiten wir äußerst sensible Kundendaten. Unsere Datenbank beinhaltet Daten von mehr als 1.500 Kunden in Europa und Amerika. Pridatect hat uns dabei geholfen lokale Standards einzuhalten, wie z.B. die HIPPA, der amerikanische Datenschutzstandard im Gesundheitswesen."

Xavier Palomer | Gründer und CEO von Psious

Mit dem Anliegen, ihr Unternehmen an die **HIPAA Compliance** anzupassen, um datenschutzkonform in den USA arbeiten zu können, wandte sich Psious an Pridatect.

Mithilfe der Datenschutzexperten und seines Datenschutzbeauftragten von Pridatect hat Psious es geschafft, alle notwendigen DSGVO und auch HIPAA Anforderungen umzusetzen und kann sein Tool nun in Europa und in den Vereinigten Staaten anbieten.

Gegenwärtig unterstützt Pridatect die Firma Psious auch bei der Einhaltung der **ISO 27001,** einer Norm, welche die Vertraulichkeit und Integrität der Daten und Informationen, mit denen wir arbeiten, sowie der Systeme, die diese Daten verarbeiten, garantiert.

05. Zusammenfassung & Ergebnisse

“Angesichts der globalen Gesundheitssituation war zu erwarten, dass wir eine Zunahme von Unternehmen und technologischen Lösungen erleben würden, die sich direkt mit sensiblen Gesundheitsdaten befassen”, sagt David Casellas, CEO von Pridatect. **Die Frage ist nur, wie man mit diesen sensiblen Daten umgehen wird.** Jede dieser Organisationen muss sich zu 100% der Datensicherheit verpflichtet fühlen. Das Gesundheitssystem ist, wie gerade gezeigt wurde, der Dreh- und Angelpunkt unserer Gesellschaft. Auch in der Gesundheitsbranche macht die Digitalisierung einen großen Sprung nach vorn, macht sie aber auch verwundbarer.

“Ich denke, dass im Gesundheitssektor ein Bewusstsein über die Wichtigkeit der Einhaltung der DSGVO besteht. Was aber fehlt ist das Wissen über die gesetzlichen Anforderungen, die erfüllt werden müssen. Während nur 1% der Organisationen zugeben, die Vorschriften der DSGVO nicht einzuhalten, geben 24% der Unternehmen an, keinen DSB benannt zu haben, was in jeder Organisation, die Daten in großem Umfang verarbeitet, gemäss Artikel 30 der DSGVO obligatorisch ist.”

David Casellas | CEO von Pridatect

Die Gesundheitsbranche muss umfangreiche Sicherheitsmaßnahmen ergreifen, um Datenschutzprobleme zu vermeiden. Wir sehen zum Beispiel, dass nur 1% der Organisationen angeben, die DSGVO nicht einzuhalten, aber 6% der Organisationen die Patienten und Kunden nicht umfassend über die Verarbeitung ihrer persönlichen Daten informiert, was gemäß Art. 13 DSGVO eine zwingende Voraussetzung für die Verarbeitung ist.

Lisa Hofmann | Chief of Legal Operations, Pridatect

Außerdem haben 52% der Unternehmen angegeben, dass sie in den letzten 12 Monaten eine neue Softwarelösung für die Verarbeitung von Gesundheitsdaten implementiert haben, aber nicht alle von ihnen haben eine Datenschutz-Folgenabschätzung durchgeführt, was bei der Implementierung durchaus notwendig wäre. Nur 57% gaben an, dass sie ein aktualisiertes Verzeichnis der Verarbeitungstätigkeiten führen. Diese Verpflichtung betrifft aber so gut wie Jeden, der personenbezogene Daten verarbeitet. Eine Aufsichtsbehörde wird Sie bei einer Prüfung des Unternehmens immer zuerst nach dem Verarbeitungsverzeichnis fragen. Es sollte also das Rückgrat des datenschutzrechtlichen Grundgerüsts eines jeden Unternehmens sein.

Auf Basis der in dieser Studie gewonnenen Ergebnisse können wir zusammenfassen, dass es zwar ein Bewusstsein über die Wichtigkeit der DSGVO gibt, jedoch noch einige Themen offen sind:

- Es ist wichtig, die Mitarbeiter öfter zu schulen.
- Einige Unternehmen wussten auf Fragen nur mit "ich weiss nicht" zu antworten. Es empfiehlt sich daher, auf die Unterstützung eines Experten zurückzugreifen um die offenen Punkte im Bezug auf die DSGVO Konformität zu überarbeiten und eine bessere Gesamtübersicht zu bekommen.

Die Notwendigkeit, über die Datenverarbeitung zu informieren ist offensichtlich:

- In 71% der in Deutschland befragten Organisationen erkundigen sich Patienten oder Kunden nach dem Zweck der Datenerhebung und in vielen Fällen besteht die Notwendigkeit, Daten mit Dritten zu teilen.
- Damit ein Patient seine Einwilligung in freier, spezifischer, informierter und eindeutiger Weise geben kann, sollte die Organisation den Patienten bei der Einholung der Einverständnis genau über den Zweck der Datenerhebung informieren. 6% der in Deutschland befragten Organisationen gaben an, dass sie ihre Patienten/Kunden nicht darüber informieren und somit gegen die DSGVO verstoßen. Es ist unerlässlich, eine Zustimmung für jede Datentransaktion einzuholen und einen Vertrag abzuschließen, wenn diese Daten an Dritte weitergegeben werden sollen.

Viele Unternehmen aus dem Gesundheitssektor der Organisationen im Gesundheitsbereich machen Fortschritte bei der Anpassung an die DSGVO, indem sie verschiedene Maßnahmen ergreifen, aber das ist nicht immer der Fall.

- 76% der befragten Unternehmen aus dem Gesundheitswesen haben bereits einen Datenschutzbeauftragten ernannt. Man sollte beachten, dass Unternehmen dieser Branche ständig mit sensiblen Gesundheitsdaten arbeiten und jederzeit Veränderungen eintreten können, die den Schutz der Daten gefährden.
- Es ist daher unerlässlich, Datenschutz-Folgenabschätzungen durchzuführen (was nur 50% der befragten Organisationen in Deutschland bereits getan haben) und technische und organisatorische Maßnahmen zu implementieren, sowie Protokolle und Aktionspläne für mögliche Sicherheitsprobleme bereit zu stellen, wie von 64% der befragten Unternehmen umgesetzt

Alle Unternehmen und Gesundheitszentren, die sich nicht an diese Vorschriften halten und die oben genannten Maßnahmen ergreifen, oder sich nicht sicher sind, ob sie das Richtige tun (laut dieser Studie rund 21% der Organisationen im Gesundheitssektor), gefährden die Gesundheitsdaten ihrer Kunden und riskieren Sanktionen aufgrund von Nichteinhaltung der DSGVO.

Die Pridatect-Plattform macht es einfach Risiken zu identifizieren und Daten zu schützen

RISIKEN RECHTZEITIG ERKENNEN

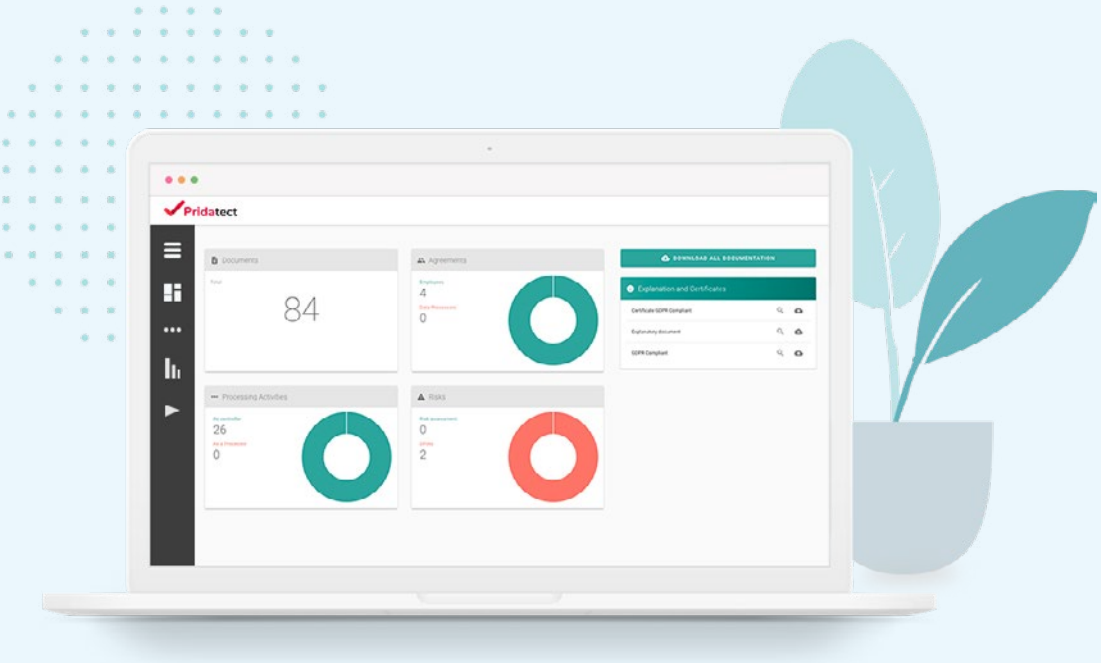
Erkennen und identifizieren Sie Risiken bei der Verarbeitung personenbezogener Daten (Kunden, Mitarbeiter, Anbieter ...). Mit der Pridatect-Plattform können wir Bedrohungen und Schwachstellen in Ihren Prozessen identifizieren und analysieren.

MASSNAHMEN DEFINIEREN UND EMPFEHLEN

Nachdem wir die Risiken in Ihrem Unternehmen identifiziert haben, können wir erforderliche Maßnahmen definieren, um diese zu reduzieren. Pridatect hilft schlägt notwendige Datenschutz- Maßnahmen für Ihr Unternehmen vor.

ÜBERWACHUNG UND UMSETZUNG DES DATENSCHUTZES

Datenschutz ist eine ständige Aufgabe innerhalb eines Unternehmens. Pridatect hilft nicht nur bei der ersten Implementierung, sondern auch bei der laufenden Überwachung und dem Aufgabenmanagement.



Kontaktieren Sie uns für eine kostenlose Online Demo oder für die sieben tägige Testversion unserer Datenschutzsoftware.