techconsult
TECHNOLOGY MARKET ANALYSTS

DSGVO und Collaboration

Wie unsichere Lösungen zur Zusammenarbeit den Datenschutz in Unternehmen gefährden

Unterstützt durch Conceptboard

Inhalt

Vorwort

Die digitale Evolution der Geschäftswelt hat in den letzten Jahren große Sprünge gemacht. Immer mehr Unternehmen bieten flexible und moderne Arbeitsumgebungen an. Ein wichtiger Bestandteil von Remote-Work ist der Einsatz von Collaboration-Tools. Damit können Teams unabhängig von geographischen Grenzen, über Cloud-Dienste, Dateien und Informationen teilen oder gemeinsam an Dokumenten arbeiten.

Doch diese digitale Zusammenarbeit schafft auch neue Problemfelder. Denn nicht immer sind die eingesetzten Tools auch mit den Anforderungen an den Datenschutz im Rahmen der DSGVO vereinbar. Das kann schwerwiegende datenschutzrelevante Sicherheitsverstöße mit gravierenden Folgen nach sich ziehen. Denn heute, fünf Jahre nach Inkrafttreten der DSGVO, sollten alle Bereiche eines Unternehmens DSGVO-konform agieren.

Doch wie ist der Stand der DSGVO-Umsetzung in den Unternehmen? Welche Arten von Collaboration-Tools werden in den Unternehmen eingesetzt? Und welche Konsequenzen haben datenschutzrelevante Sicherheitsvorfälle für die Unternehmen?

Um diese Fragen zu beantworten, wurden im Dezember 2022 im Rahmen dieser Studie 204 entscheidende oder stark am Entscheidungsprozess beteiligte Personen zu ihrem Grad der DSGVO-Umsetzung, eingesetzten Collaboration-Tools und Sicherheitsvorfällen befragt.

Sonstiges
Aufgrund von Rundungsanpassungen summieren sich einige Summen möglicherweise nicht zu 100%.
Aus Gründen der besseren Lesbarkeit wird bei Personenbezeichnungen und personenbezogenen Hauptwörtern in dieser Studie die männliche Form verwendet. Entsprechende Begriffe gelten im Sinne der Gleichbehandlung grundsätzlich für alle Geschlechter. Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

DSGVO-Reifegrad: Unternehmen auf dem richtigen Weg

Seit dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) in der Europäischen Union wirksam. Mit dieser Verordnung sollen sämtliche Daten von jeder betroffenen Person, also vom Kunden über die Mitarbeitenden bis zu externen Geschäftspartnern, geschützt werden. Bei Nichteinhaltung sind empfindliche Strafen vorgesehen. Und für viele Unternehmen stellt die DSGVO auch heute noch eine größere Herausforderung dar. Beispielsweise ist nicht immer klar, was als personenbezogene Daten gilt und manche Formulierungen innerhalb der Richtlinie lassen bei der Definition einiges an Spielraum für individuelle Auslegungen.

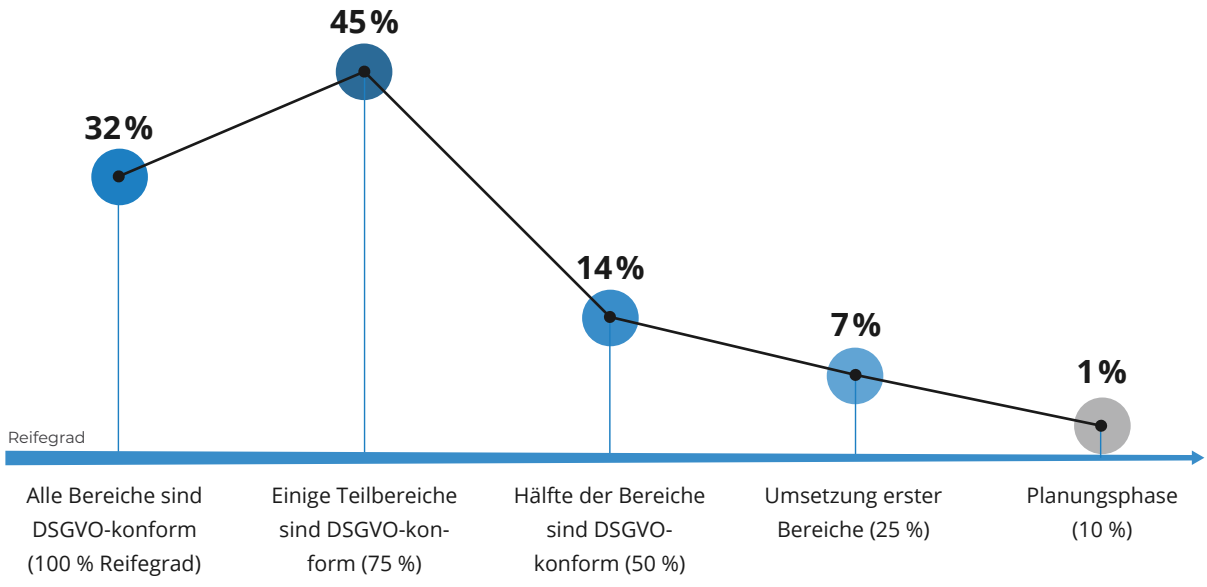
Doch wie sieht der Umsetzungsgrad nach fünf Jahren DSGVO aus? Die Umsetzung der DSGVO ist in vielen Unternehmen immer noch nicht vollständig. Positiv lässt sich allerdings feststellen, dass die überwiegende Mehrheit sich bereits auf einem guten Weg befindet. So gaben 32 Prozent der befragten Unternehmen an, bereits im gesamten Unternehmen DSGVO-konform zu sein.

Die überwiegende Mehrheit (45 Prozent) hingegen ist in den meisten Teilbereichen bereits DSGVO-konform und aktuell im Prozess, weitere Teilbereiche DSGVO-konform zu gestalten. Weitere 14 Prozent würden von sich behaupten, dass sie etwa zur Hälfte den Auflagen der DSGVO gerecht werden. Nur die allerwenigsten, knapp sieben Prozent, der Unternehmen sind noch am Anfang ihrer DSGVO-Umsetzung.

Dabei zeigt sich, dass insbesondere kleinere Unternehmen auf ihrem Weg zur DSGVO-Konformität gegenüber den größeren Unternehmen mit mehr als 100 Mitarbeitenden hinterherhinken. So sagen beispielsweise rund zehn Prozent der Unternehmen bis 999 Mitarbeitenden, dass sie erst am Anfang der DSGVO-Umsetzung stehen, während der Anteil bei den größeren bei gerade einmal vier Prozent liegt.

Reifegrad der DSGVO-Umsetzung

Basis: 204 Unternehmen



DSGVO – Enabler oder Bremse?

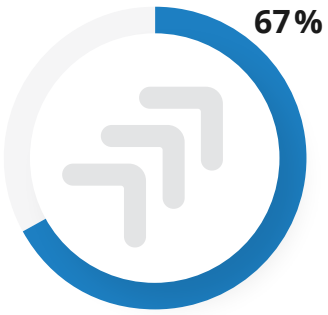
Die verpflichtende Umsetzung der DSGVO sollte für Unternehmen nicht nur als lästige Pflicht angesehen werden, sondern auch als Chance, die eigenen Digitalisierungsbestrebungen zu beschleunigen und zu verbessern. Wo früher jeder Staat seine eigenen Regelungen hatte, in Deutschland gab es sogar Abweichungen je nach Bundesland, so existiert mit der DSGVO ein einheitliches Regelwerk für alle in Europa agierenden Unternehmen. Und innerhalb der DSGVO werden auch die besonderen Anforderungen der Digitalisierung im Kontext von Datenschutz aufgegriffen und für Unternehmen übersichtlicher gestaltet.

Für gut zehn Prozent der Unternehmen erwies sich die DSGVO bislang als reiner Bremsklotz für die eigenen Digitalisierungsbestrebungen. Noch immer herrscht an vielen Punkten Rechtsunsicherheit bezüglich der genauen Ausprägungen der Verordnung, was die Einführung neuer digitaler Technologien erschwert. Keinen spürbaren Einfluss hatte die DSGVO bei rund jedem fünften Unternehmen.

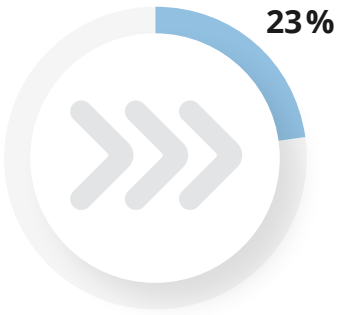
Für die Mehrheit der befragten Unternehmen ist die DSGVO tatsächlich ein Treiber beim Ausbau der Digitalisierung. Knapp zwei Drittel der Unternehmen gaben an, dass die DSGVO die Umsetzung wichtiger digitaler Prozesse beschleunigt hat. So können Unternehmen, die dem Datenschutz einen hohen Stellenwert zuweisen, sich im Wettbewerb gegenüber jenen, die den Datenschutz eher vernachlässigen, einen Vorteil verschaffen und ein besseres Vertrauensverhältnis gegenüber Kunden aufbauen. Des Weiteren sorgt DSGVO-konformität auch dafür, dass Unternehmen bedenkenlos für einen modernen und flexiblen Arbeitsplatz sorgen können. So werden beispielsweise Gefahrenpotenziale minimiert, die durch den erhöhten Einsatz von Cloud-Services zunehmen. Digitalisierung und Datenschutz sind daher keine Antagonisten, sondern ergänzen sich und bringen Unternehmen reale Vorteile.

DSGVO als Treiber der Digitalisierung

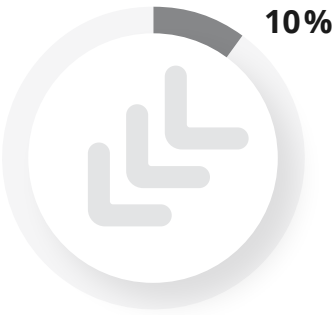
Basis: 204 Unternehmen



Die Datenschutzgrundverordnung hat in unserem Unternehmen wichtige digitale Prozesse **beschleunigt**.



Die Datenschutzgrundverordnung hatte **keinen Einfluss** auf unsere Digitalisierungsbestrebungen.



Die Datenschutzgrundverordnung hat uns in Sachen Digitalisierung **ausgebremst**.

Einsatz von sicheren Lösungen ist Mangelware

Mit Ausbruch der Pandemie und der daraus resultierenden Verlagerung der Arbeit ins Home-Office, stieg auch der Einsatz von Online-Collaboration-Tools stark an. Auch heute noch arbeiten viele Menschen von zu Hause aus. Um eine effektive Zusammenarbeit zu gewährleisten, ist der Einsatz von Collaboration-Tools essentiell. Doch diese Lösungen zur digitalen Zusammenarbeit bergen auch Risiken. Oftmals haben Unternehmen im Zuge des schnellen Implementierens von Collaboration-Lösungen irgendein Tool gewählt, ohne sich mit datenschutzrechtlichen und sicherheitstechnischen Aspekten auseinander zu setzen. Denn die Sicherheit und Datenschutzkonformität von sogenannten universellen Online-Collaboration-Lösungen kann nicht immer gewährleistet werden. Und wenn die Sicherheit der Lösungen nicht gewährleistet werden kann, so kann dies das gesamte Unternehmen gefährden.

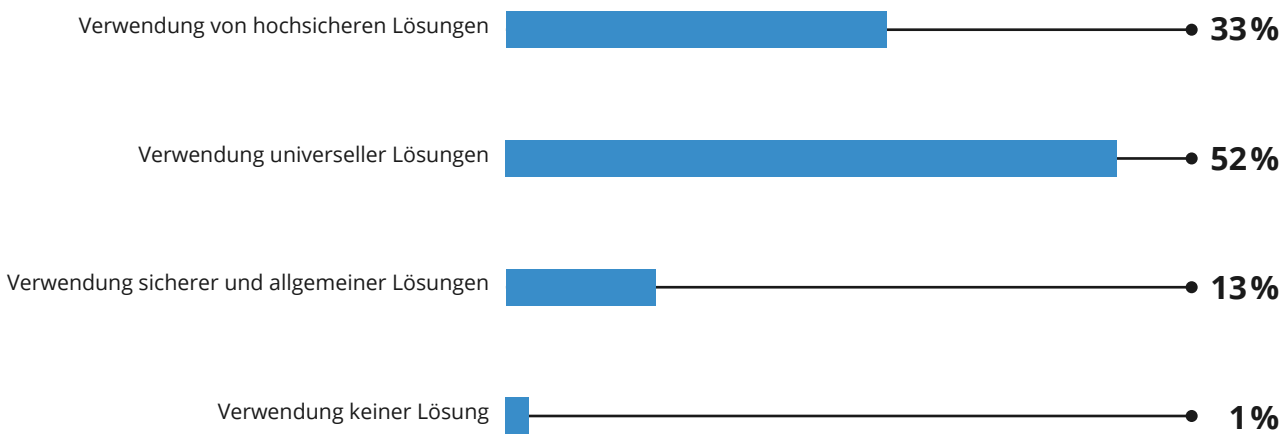
Die Mehrheit der befragten Unternehmen (53 Prozent) verwendet für die interne sowie externe Zusammenarbeit ausschließlich universelle Lösungen, wie beispielsweise Teams, Slack, Zoom und viele weitere erhältliche Tools.

Diese Collaboration-Tools ohne strenge Sicherheitsprotokolle machen die Unternehmen nicht nur anfällig für allerhand externe Bedrohungen. Datenschutzverletzungen können auch entstehen, wenn Mitarbeitende nicht ausreichend zum sicheren Umgang mit den Collaboration-Tools geschult werden. Denn der Mensch ist immer noch das schwächste Glied in der Sicherheitskette.

Nur ein Drittel der befragten Unternehmen setzt auf spezielle und hochsichere Lösungen für die digitale Zusammenarbeit. Solche Collaboration-Tools ergreifen von vornherein strenge Maßnahmen zum Schutz der Daten und stellen sicher, dass die Lösung gesetzeskonform ist. Im Gegensatz zu universellen Lösungen verfügen spezialisierte Anbieter über spezifische Schulungsprogramme, um menschliches Versagen beim Einsatz der Lösungen zu minimieren. Weitere 13 Prozent verwenden sowohl sichere Speziallösungen als auch allgemeine Lösungen.

Einsatzgrade von Collaboration-Lösungen

Basis: 204 Unternehmen



Datenschutzrelevante Vorfälle sind die Regel

Dass der Einsatz von sicheren Lösungen mehr als nur dringend ist, zeigen die datenschutzrelevanten Vorfälle der vergangenen 24 Monate. Nur 17 Prozent der befragten Unternehmen gaben an, in den letzten zwei Jahren nicht Opfer von datenschutzrelevanten Sicherheitsvorfällen gewesen zu sein. Betrachtet man die Konsequenzen dieser Vorfälle, so fällt schnell auf, dass vor allem unnötige Kosten entstehen.

Unnötige interne und externe Kosten

So geben mehr als ein Drittel der Unternehmen an, erhebliche zusätzliche interne Kosten zur Fehlerbehebung, beispielsweise im Rahmen von Überstunden in der IT, erlitten zu haben. Tritt ein datenschutzrelevanter Vorfall ein, so müssen die Lücken im System schnell ausfindig gemacht und geschlossen werden. Das kann bei einer Vielzahl von möglichen potenziellen Einfallstoren schnell zu einer langwierigen und kostspieligen Aufgabe werden.

Bei weiteren 28 Prozent kamen auch noch zusätzliche Kosten für externe Dienstleister hinzu. Besonders dort, wo die IT-Expertise nicht dazu ausreicht, die Fehlerquelle zu identifizieren und zu beseitigen, müssen Spezialisten dafür Sorge tragen, dass die Lücken geschlossen werden.

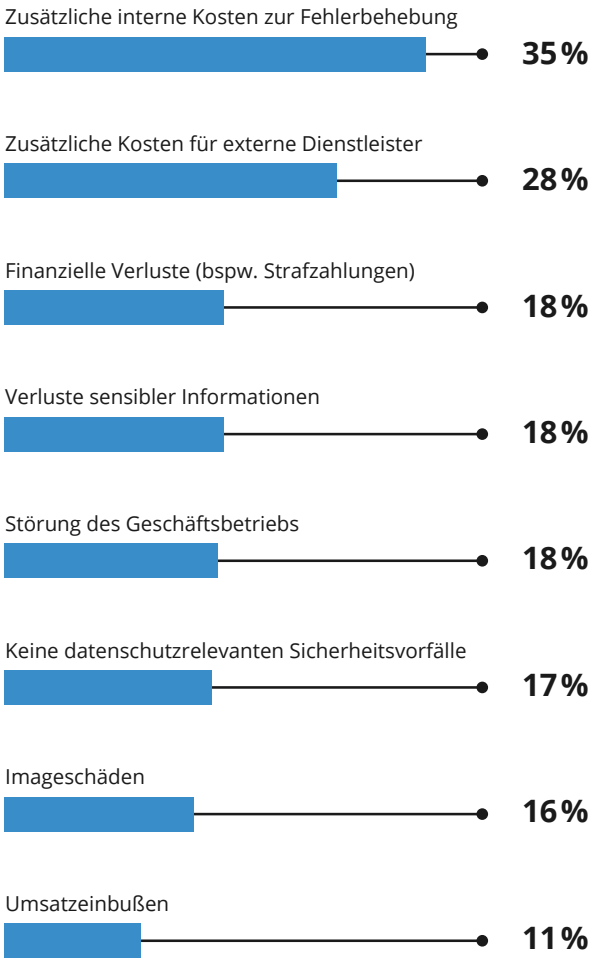
Für 18 Prozent kamen darüber hinaus noch direkte finanzielle Verluste in Form von Strafzahlungen hinzu. Im Rahmen von Verstößen gegen die DSGVO sind je nach Schwere des Vorfalls erhebliche Strafzahlungen an die entsprechenden Behörden zu zahlen.

Verlust sensibler Daten

Ein knappes Fünftel hat unterdessen auch noch unternehmenskritische oder sensible Informationen an die Angreifer verloren. Obwohl es sich hier um keinen direkten monetären Verlust handelt, wiegt der Verlust von sensiblen Informationen besonders schwer. Beispielsweise dann, wenn hochsensible Daten wie etwa Betriebsgeheimnisse bezüglich einer Rezeptur, einer Maschine usw. in die Hände von Wettbewerbern gelangen. So würde die eigene Marktposition stark geschwächt werden, was eine Minderung der zukünftigen Umsätze zur Folge hätte.

Konsequenzen von Datenschutzverletzungen

Basis: 204 Unternehmen | Mehrfachnennungen



Um diesen datenschutzrelevanten Vorfällen Herr zu werden, empfiehlt es sich, auf Lösungen zu setzen, die von vornherein so konzipiert sind, dass sie im Einklang mit den Anforderungen an die DSGVO sind. Nur so lässt sich gewährleisten, dass die sensiblen Informationen, die über die Collaboration-Software geteilt werden, nicht in die Hände Unbefugter gelangen.

Sicherheitsfunktionen im Fokus

Wenn sich Unternehmen dazu entscheiden, eine neue Lösung für die digitale Zusammenarbeit anzuschaffen, dann achten sie dabei auf ganz spezifische Eigenschaften, die die Lösung mit sich bringen muss. Das kann von erweiterten Funktionen über die Herkunft des Herstellers bis hin zum Vorhandensein von wichtigen Zertifizierungen reichen.

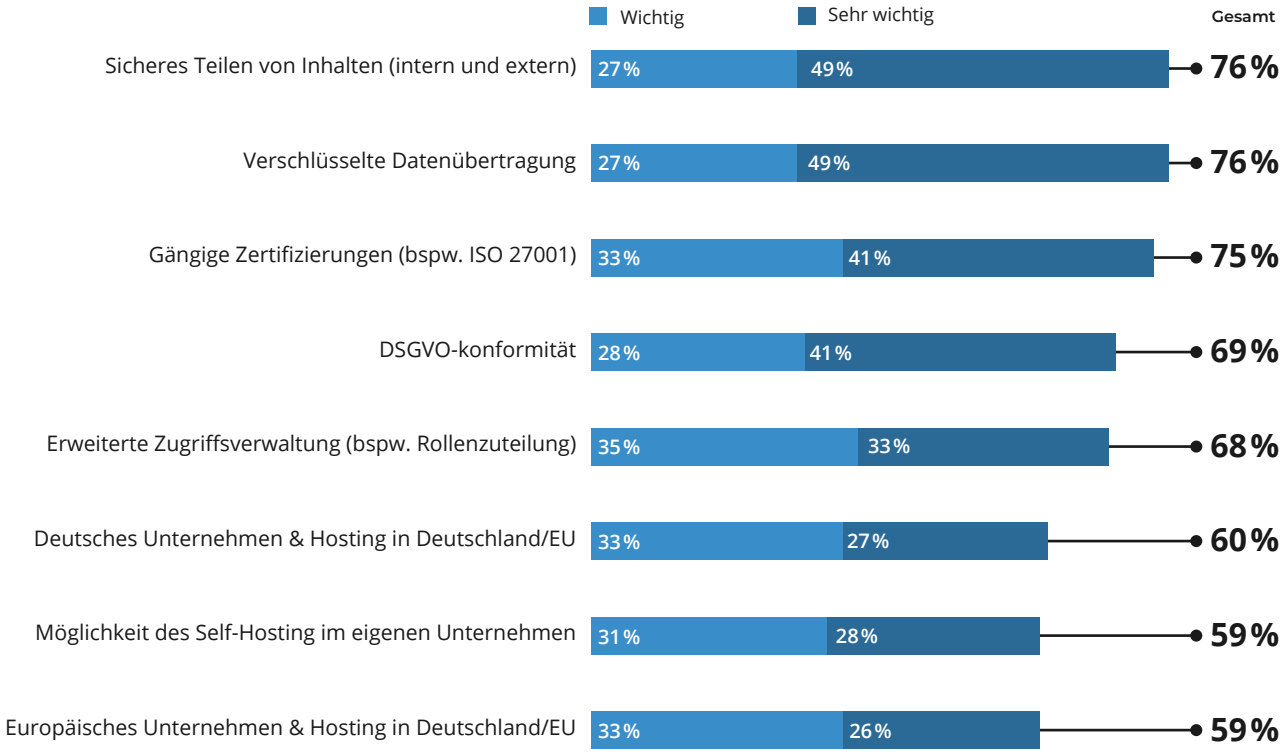
Auf die Frage, welche sicherheitsrelevanten Eigenschaften bei Lösungen für die digitale Zusammenarbeit besonders im Fokus stehen, antworten knapp drei Viertel der befragten Unternehmen, dass das sichere Teilen von Inhalten mit internen und externen Mitarbeitern die höchste Priorität hat. Um sensible Inhalte sicher zu teilen, muss gewährleistet sein, dass nur Personen mit entsprechenden Berechtigungen Zugriff haben. Eine gute Collaboration-Lösung sollte daher in der Lage sein, unterschiedliche Zugriffsebenen zuzuweisen und diese gegebenenfalls noch mit einem zusätzlichen Passwort abzusichern.

Dahinter folgt mit ebenfalls rund drei Viertel der Unternehmen die verschlüsselte Datenübertragung, sowie das Vorhandensein von gängigen Zertifizierungen. Eine Verschlüsselung der Daten verhindert, dass nicht autorisierte Benutzer an die Informationen gelangen. So lässt sich auch im Fall eines erfolgreichen Hackerangriffs sicherstellen, dass die gestohlenen Informationen mangels Schlüssels für die Cyberkriminellen nutzlos sind. Zertifizierungen stellen darüber hinaus sicher, dass die Lösung den gängigen Sicherheitsstandards entspricht.

Ebenfalls sehr wichtig ist die DSGVO-Konformität der Lösung, die sichergestellt wird, wenn Rechenzentren der Betreiber ausschließlich in Deutschland oder der EU liegen. Für rund 60 Prozent der Unternehmen ist dies auch ein wichtiger Faktor bei der Auswahl der Collaboration-Software. Werden die Daten ausschließlich in sicheren europäischen Rechenzentren gespeichert, können Regierungen in Staaten außerhalb der EU nicht auf diese Daten zurückgreifen.

Wichtige sicherheitsrelevante Eigenschaften von Collaboration-Lösungen

Basis: 204 Unternehmen | Mehrfachnennungen



Fazit

Die DSGVO ist auch fünf Jahre nach dem Inkrafttreten noch immer nicht vollständig in den meisten Unternehmen umgesetzt. Dabei ist Datenschutz nicht nur ein lästiges Element, sondern kann als wichtiger Enabler für die eigene Digitalisierung angesehen werden. Insbesondere in der heutigen Zeit, mit modernen und flexiblen Arbeitsmodellen und dem rasanten Anstieg von digitalen Lösungen zur ortsunabhängigen Zusammenarbeit, muss der Schutz von sensiblen Daten und Informationen von höchster Bedeutung sein.

Der Einsatz von Collaboration-Lösungen stellt für Unternehmen einen wichtigen Grundpfeiler für einen modernen und zukunftssicheren Arbeitsplatz dar. Doch mit der Anschaffung von beliebigen Collaboration-Tools tun sich Unternehmen keinen Gefallen. Lösungen, die nicht von vornherein im Einklang mit dem Datenschutz konzipiert wurden, verfügen oftmals nicht über die nötigen Sicherheitsfunktionen, um einen datenschutzrechtlich sauberen Ablauf zu gewährleisten.

Viel eher ist es so, dass diese Lösungen sogar eine Gefahr für Unternehmen darstellen können. Der Verlust von sensiblen Daten über unsichere Tools führt nicht nur zu hohen internen sowie externen Kosten zur Schadensbeseitigung, sondern auch zu möglichen Verlusten der Kundenbasis und mit ziemlich großer Sicherheit auch zu Problemen mit Behörden.

Ratsam ist es, für die digitale Zusammenarbeit sichere Lösungen zu wählen, die den gängigen Sicherheitsstandards entsprechen. Nur so kann gewährleistet werden, dass sensible Informationen sicher sowohl intern als auch extern geteilt werden können. Dazu sollte nicht nur auf die Verfügbarkeit von Funktionen wie der Rollenverteilung geachtet werden, sondern auch darauf, dass die Lösungen über gängige IT-Security-Zertifizierungen verfügen, eine robuste Verschlüsselung anbieten und mit der DSGVO im Hinterkopf konzipiert wurden.

Zur Studie

Die Studie „DSGVO und Collaboration – Wie unsichere Lösungen zur Zusammenarbeit den Datenschutz gefährden“ wurde von der techconsult GmbH im Auftrag von conceptboard konzipiert und durchgeführt. 204 Unternehmen wurden zu ihrem Reifegrad der DSGVO-Umsetzung, datenschutzrelevanten Sicherheitsvorfällen und dem Einsatzgrad sicherer Lösungen zur digitalen Zusammenarbeit befragt. Ansprechpartner waren in erster Linie IT-Entscheidende.

Branche

Industrie:	25 %
Handel:	6 %
Dienstleistung:	47 %
Banken und Versicherungen:	10 %
Öffentliche Verwaltungen, Non-Profit, Gesundheits- und Sozialwesen:	13 %

Größenklassen

250 bis 499 Mitarbeitende:	21 %
500 bis 999 Mitarbeitende:	26 %
1.000 bis 1.999 Mitarbeitende:	25 %
2.000 oder mehr Mitarbeitende:	28 %

Weitere Informationen

Impressum

techconsult GmbH
Baunsbergstraße 37
34131 Kassel

E-Mail: **info@techconsult.de**
Tel.: +49-561-8109-0
Fax: +49-561-8109-101
Web: **www.techconsult.de**

Kontakt

Raphael Napieralski
Analyst
techconsult GmbH
Baunsbergstr. 37
D-34131 Kassel

E-Mail: **raphael.napieralski@techconsult.de**
Tel.: +49-561-8109-181

Über techconsult GmbH

Die techconsult GmbH, gegründet 1992, zählt zu den etablierten Analystenhäusern in Zentraleuropa. Der Schwerpunkt der Strategieberatung liegt in der Informations- und Kommunikationsindustrie (ITK). Durch jahrelange Standard- und Individual-Untersuchungen verfügt techconsult über einen im deutschsprachigen Raum einzigartigen Informationsbestand, sowohl hinsichtlich der Kontinuität als auch der Informationstiefe, und ist somit ein wichtiger Beratungspartner der CXOs sowie der IT-Industrie, wenn es um Produktinnovation, Marketingstrategie und Absatzentwicklung geht.

Über Conceptboard

Conceptboard ist die sicherste Lösung für digitale und ortsunabhängige Zusammenarbeit aus Deutschland. Die Software erleichtert virtuelle Kollaboration und ermöglicht es hybriden Teams auf der ganzen Welt, in Echtzeit zusammenzuarbeiten – mit einer großen Auswahl an Funktionen und vorgefertigten Templates für unzählige Anwendungsfälle. Das DSGVO-konforme und ISO 27001-zertifizierte Online-Whiteboard bietet maximale Sicherheit für Unternehmen oder Institutionen mit sensiblen Sicherheitsanforderungen. Dank modernster Sicherheitsmaßnahmen sowie der Zusammenarbeit mit erstklassigen Hosting Partnern in Deutschland erfüllt Conceptboard höchste Ansprüche und bietet maßgeschneiderte Hosting Lösungen: Cloudbasiert, hybrid, oder als On-Premises Data-Center-Edition. Die Stuttgarter bieten ihren Kunden dabei kompromisslose Datensouveränität und lückenlose Datenkontrolle.

2010 in Stuttgart von Daniel Bohn gegründet, ist Conceptboard heute bereits bei über 6.500 Kunden und 15 Millionen Usern im Einsatz, darunter SIEMENS und mehrere Unternehmen der Würth-Gruppe. Besonders staatliche Institutionen weltweit setzen auf Conceptboard und vertrauen auf höchste Datenschutzstandards und -zertifizierungen.

Mehr Informationen finden Sie unter: **https://conceptboard.com/de/**

Kontakt:

Conceptboard Cloud Service GmbH
Mansfelder Str. 56
06108 Halle (Saale)
Germany

Tel.: +49 (0) 711 508880240
E-Mail: **support@conceptboard.com**
Web: **www.conceptboard.com**

Conceptboard