proofpoint.

BERICHT

DIE GROSSE DISKREPANZ

WAHRNEHMUNG UND WIRKLICHKEIT – ZUM STAND DER IMPLEMENTIERUNG DER DSGVO IN GROSSBRITANNIEN, FRANKREICH UND DEUTSCHLAND

proofpoint.com/de

Am 25. Mai 2018 wird die neue Datenschutzgrundverordnung (DSGVO) in Kraft treten. Die neue Verordnung soll die Datensicherheit für alle Bürger der Europäischen Union (EU) stärken und vereinheitlichen. Zudem regelt sie die Bedingungen für den Export personenbezogener Daten außerhalb der EU. Da die DSGVO in sechs Monaten in Kraft tritt, hat Proofpoint eine Umfrage zur Beantwortung der folgenden drei wichtigen Fragen in Auftrag geben:

- Wie bereiten sich Unternehmen auf die Einhaltung der DSGVO vor?
- Wie weit sind die Implementierungspläne fortgeschritten?
- Wie zuversichtlich sind sie, ihre Ziele bis Mai 2018 zu erreichen?

Im Rahmen der von Censuswide im Zeitraum vom 22. bis 29. September 2017 durchgeführten Umfrage wurden 1.500 IT-Entscheidungsträger von Unternehmen befragt, die mindestens 200 Mitarbeiter und ihren Sitz in Großbritannien, Frankreich oder Deutschland haben. Dabei wurden die Daten von mindestens 500 Teilnehmern pro Land aus verschiedenen Branchen erfasst.

In diesem Bericht werden die Ergebnisse dieser Umfrage vorgestellt. Wir zeigen auf, wie sich Unternehmen in Großbritannien, Frankreich und Deutschland auf die anstehende Verordnung vorbereiten. Außerdem analysieren wir, welche Unterschiede zwischen den Branchen bestehen, um die größten Risiken in Bezug auf die Nichteinhaltung aufzudecken.

DIE DSGVO IM ÜBERBLICK

Die DSGVO ersetzt die 22 Jahre alte EU-Datenschutzrichtlinie. Hauptziel der neuen Verordnung ist es, den EU-Bürgern die Kontrolle über ihre personenbezogenen Daten zu geben. Sie reguliert, wie Daten erfasst, verarbeitet, gespeichert, gelöscht und verwendet werden dürfen.

Unabhängig vom Standort müssen alle Unternehmen, die in Europa geschäftlich tätig sind und personenbezogene Daten von EU-Bürgern verarbeiten, diese neuen Regelungen einhalten.

Für Unternehmen ist es daher äußerst wichtig, einen Plan zur Einhaltung der neuen Vorschriften zu entwickeln. Die Nichteinhaltung der Vorschriften kann zu bisher beispiellosen Geldstrafen in Höhe von bis zu 4 Prozent des weltweiten Jahresumsatzes des Unternehmens bzw. bis zu 20 Millionen Euro führen – je nachdem, welcher der Beträge höher ist. Dieser Betrag ist also deutlich größer als die Geldstrafen, die von den Datenschutzbehörden in den einzelnen EU-Ländern bisher erhoben werden.

Der Countdown läuft: Unternehmen haben nur noch sechs Monate Zeit, um sich auf die neue Verordnung vorzubereiten. Doch viele Unternehmen wissen scheinbar noch nicht genau, was zur Einhaltung der Vorgaben erforderlich ist.

Viele Fragen sind noch offen: Welche Änderungen müssen wir an internen Prozessen vornehmen, um die Verordnung einzuhalten? Welche Technologien sollten Unternehmen einsetzen, um zu gewährleisten, dass die personenbezogenen Daten von EU-Bürgern geschützt sind? Wie können IT- und Sicherheitsexperten Datenschutz gemäß DSGVO in ihre Entwicklungsabläufe integrieren?

Eines ist jedoch sicher: Unternehmen müssen jetzt handeln, um die Kontrollen für Personen, Prozesse und Technologien bereitzustellen, die zum Schutz der personenbezogenen Daten von EU-Bürgern erforderlich sind. Datenschutz und Privatsphäre gelten zunehmend als geschäftlicher Vorteil. Die DSGVO bietet Unternehmen eine hervorragende Gelegenheit, von der Implementierung entsprechender Maßnahmen zu profitieren.

„Für die Handhabung dieser neuen Regeln sind in allen Unternehmen, die Kundendaten verarbeiten, wichtige Veränderungen notwendig. Gleichzeitig ist dies eine hervorragende Gelegenheit für Sicherheits-, Risiko-Management- und Datenschutzverantwortliche. Da der Datenschutz die Aufmerksamkeit der Unternehmensführung erhält und die entsprechenden Budgets aufgestockt werden, können die Verantwortlichen für Sicherheit, Risiko-Management und Datenschutz argumentieren, dass Datenschutz nicht nur eine Compliance-Vorgabe ist, sondern eine geschäftliche Wachstumsstrategie darstellt.“

„The EU General Data Protection Regulation (GDPR) Is Here“ (Die Datenschutzgrundverordnung der EU (DSGVO) tritt in Kraft), Blog-Beitrag von Forrester, April 2016, Enza Iannopollo.

WICHTIGE ERKENNTNISSE

Die wichtigsten Erkenntnisse aus unserer Untersuchung:

- **Datenschutzverletzungen sind heute Normalität**
- **Unternehmen sind wahrscheinlich schlechter vorbereitet als sie glauben**
- **Die Einhaltung der DSGVO steht nicht auf der Tagesordnung der Führungskräfte**
- **Viele Unternehmen bereiten sich auf die Folgen der Nichteinhaltung vor**

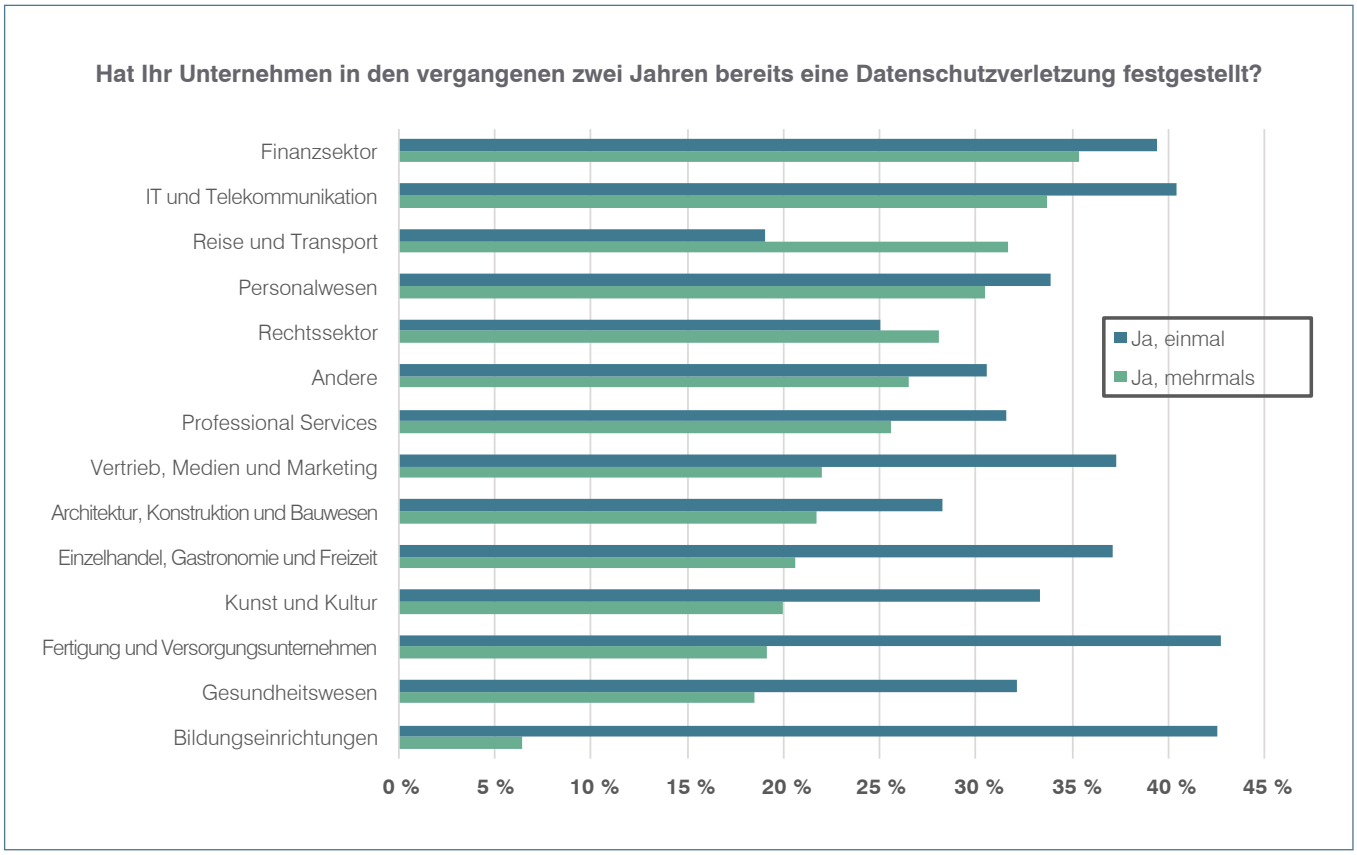
DATENSCHUTZVERLETZUNGEN SIND HEUTE NORMALITÄT

Cyberangriffe bestimmen seit längerer Zeit den Alltag von Sicherheitsexperten. In Anbetracht massiver Angriffe und Datenschutzverletzungen erhielt das Thema Datenschutz große öffentliche Aufmerksamkeit.

Aufgrund zweier aktueller medienwirksamer Angriffe ist es praktisch unmöglich, das Thema zu ignorieren. Die Equifax-Kompromittierung legte die Daten von mehr als 145 Millionen Amerikanern offen, und der WannaCry-Ransomware-Angriff infizierte über 200.000 Maschinen in 150 Ländern.

Datenschutzverletzungen sind heute erheblich häufiger als in der Vergangenheit und werden zudem häufiger gemeldet. Unternehmen gingen vielleicht früher einmal davon aus, dass Sicherheitsverletzungen nur einige wenige betreffen. Heute sind sich die meisten bewusst, dass es keine Frage mehr ist, ob es zu einem Angriff kommt, sondern wann.

Im Rahmen unserer Umfrage gaben 64 Prozent an, dass sie in den vergangenen zwei Jahren mindestens eine Datenschutzverletzung festgestellt haben. Bei allen gemeldeten Kompromittierungen waren auch personenbezogene Daten betroffen. In Anbetracht der Häufigkeit dieser Vorfälle könnten fast zwei Drittel aller Unternehmen in Europa haftbar gemacht und mit Bußgeldern belegt werden. (Laut den Vorgaben der DSGVO müssen Unternehmen die Vertraulichkeit sowie Integrität personenbezogener Daten schützen und Datenschutzverletzungen innerhalb von 72 Stunden melden.)



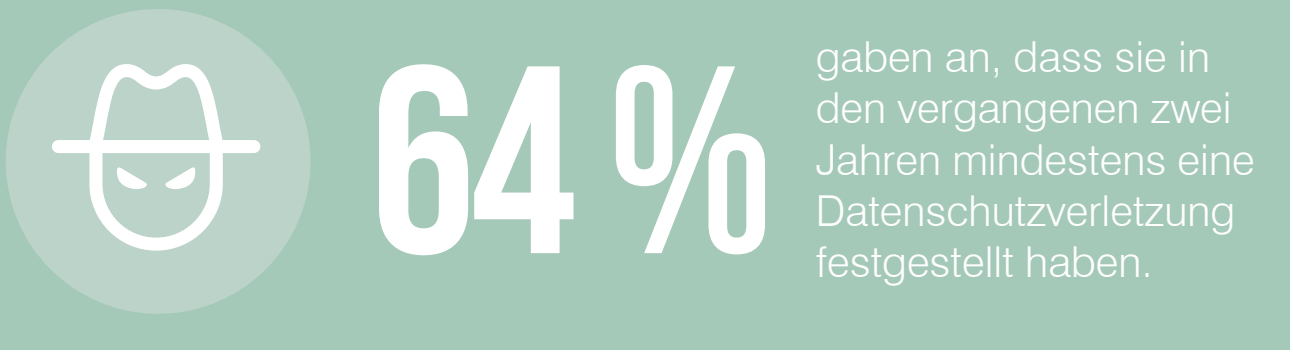
Von den drei in der Umfrage berücksichtigten Ländern lag der Anteil der Unternehmen mit mehreren Datenschutzverletzungen innerhalb der letzten zwei Jahre in Frankreich mit 29 Prozent am höchsten. Französische Unternehmen sind sich scheinbar auch am stärksten des Risikos von Datenschutzverletzungen bewusst. Etwa 78 Prozent der Befragten in Frankreich gaben an, dass ihr Unternehmen wahrscheinlich in den nächsten zwölf Monaten eine Datenschutzverletzung verzeichnen wird. Diese Meinung wurde von lediglich 54 Prozent der Befragten in Großbritannien und 46 Prozent der deutschen Umfrageteilnehmer geteilt.

In Bezug auf die betroffenen Branchen haben die Cyberkriminellen mindestens ein Merkmal mit ihren Kollegen in der physischen Welt gemeinsam: Geld zieht die meiste Aufmerksamkeit auf sich.

Etwa 35 Prozent der Finanzinstitute gaben an, dass sie in den vergangenen zwei Jahren mehrmals von Datenschutzverletzungen betroffen waren. Damit liegt der Anteil der betroffenen Unternehmen erheblich höher als in den Branchen Gesundheitswesen, Fertigung und Versorgungsunternehmen (19 Prozent).

Finanzinstitute verfügen über Prozesse und Technologien zur Erkennung sowie Behebung jeglicher Datenschutzverletzungen. Dies liegt vor allem an Branchenvorschriften wie zum Beispiel Sarbanes-Oxley (SOX) und den Auflagen der Financial Industry Regulatory Authority (FINRA).

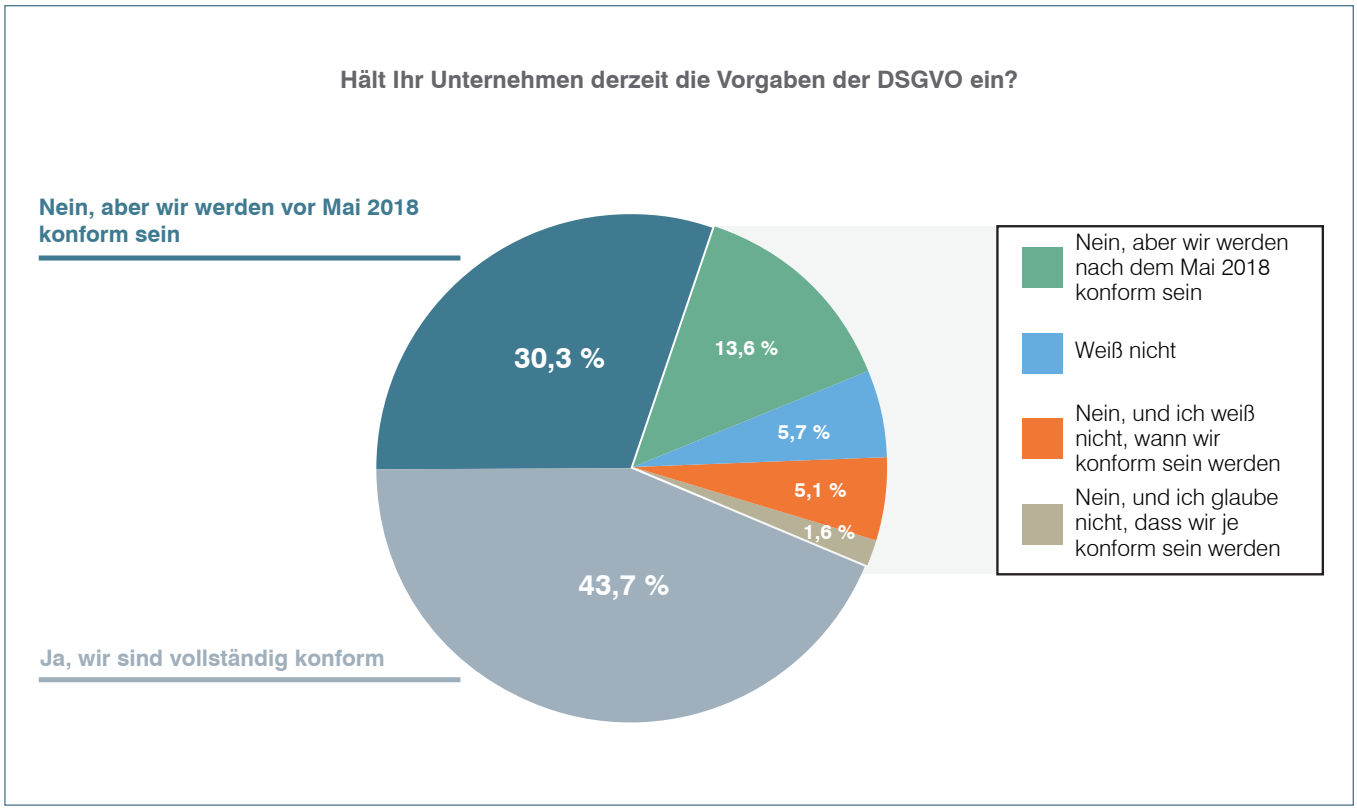
In anderen Branchen erfolgte die Anpassung nicht so schnell.



VORBEREITUNG AUF DIE DSGVO: WAHRNEHMUNG UND REALITÄT UNTERSCHEIDEN SICH

Fast zwei Drittel der Umfrageteilnehmer geben zu, dass sie in den vergangenen zwei Jahren eine Datenschutzverletzung verzeichnet haben. Trotz dieser Tatsache sind die Unternehmen optimistisch, dass sie bis zum Inkrafttreten der DSGVO im Mai 2018 die Vorgaben einhalten werden.

Laut der Umfrage sind 44 Prozent der Unternehmen in Großbritannien, Frankreich und Deutschland der Meinung, dass sie die Auflagen der DSGVO bereits vollständig erfüllen. Weitere 30 Prozent glauben, dass sie vor Mai 2018 konform sein werden.

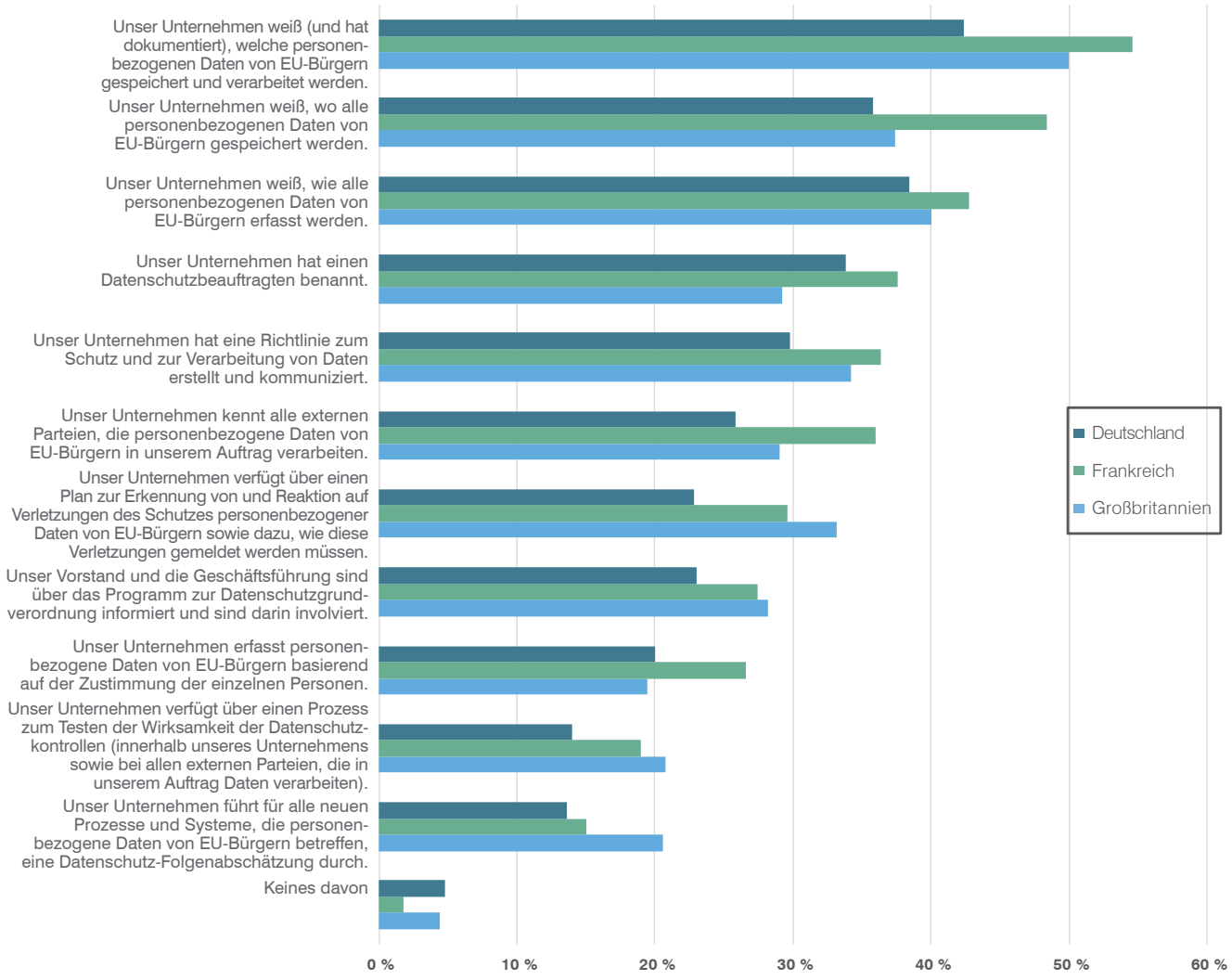


Dieser Optimismus kann bestenfalls als naiv bezeichnet werden.

Nur 49 Prozent der befragten Unternehmen kennen und dokumentieren die von ihnen verarbeiteten personenbezogenen Daten zu EU-Bürgern. Und obwohl sie zwei Jahre für die Vorbereitung Zeit hatten (die DSGVO wurde im April 2016 verabschiedet), haben erst 40 Prozent eine Selbstbewertung des Stands ihrer Vorbereitung durchgeführt.

Nur 28 Prozent der Unternehmen verfügen über einen Plan zur Erkennung und Abwehr von Verletzungen des Schutzes personenbezogener Daten von EU-Bürgern sowie dazu, wie diese Verletzungen gemeldet werden müssen. Die Situation wird sich nicht so schnell verbessern. Das Marktforschungsunternehmen Gartner sagt voraus, dass bis Ende 2018 mehr als die Hälfte der von der DSGVO betroffenen Unternehmen nicht vollständig konform sein werden.

Welche der folgenden Aussagen beschreibt die in Ihrem Unternehmen eingesetzte Strategie zur Datenkontrolle? (Wählen Sie alle zutreffenden Antworten.)



Beim Branchenvergleich zeigte unsere Umfrage, dass Gesundheitsunternehmen bei der Vorbereitung auf die DSGVO zurückliegen. Diese Erkenntnis ist nicht überraschend, aber beunruhigend. Die von öffentlichen und privaten Gesundheitsanbietern erfassten Daten sind äußerst sensibel – und für Cyberkriminelle enorm wertvoll: Mit medizinischen Daten lassen sich auf dem Schwarzmarkt zehnmal höhere Preise erzielen als mit einer Kreditkartennummer.

Viele Gesundheitsunternehmen verwenden Cloud-Technologien, um ihre Patienten auf innovative Weise unterstützen zu können. Sie erfassen und speichern immer mehr Datensätze digital, verwenden aber weiterhin physische Patientenakten. Die Herausforderungen in Bezug auf die DSGVO liegen für sie woanders: Die Umgebungen von Gesundheitsanbietern sind komplex. Sie nutzen häufig alte IT-Technik, die für neue Cyberangriffe anfällig sein kann, und sie arbeiten mit besonders sensiblen Daten. Aufgrund separater Datenspeicher wissen sie in einigen Fällen nicht einmal, wo sich all die personenbezogenen Daten befinden.

Derzeit geht es in Bezug auf die DSGVO vor allem darum, wie Unternehmen die verschiedenen Grundsätze der Verordnung interpretieren. Diese Unklarheit – und das unangemessene Vertrauen der Unternehmen in ihre eigenen Fähigkeiten zur Einhaltung der DSGVO – führen zu einer gewissen Trägheit sowie dazu, dass Unternehmen nicht die erforderlichen Compliance-Maßnahmen ergreifen.

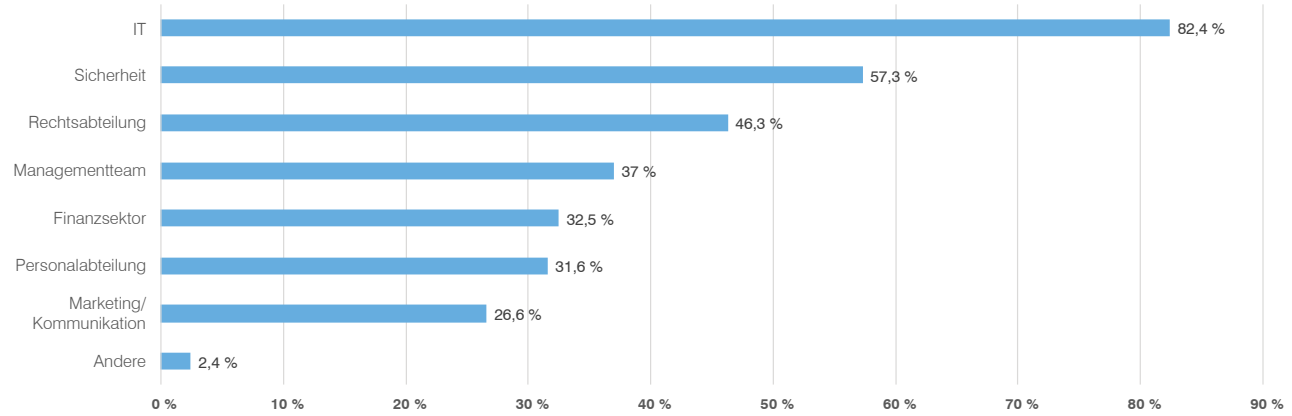
DIE EINHALTUNG DER DSGVO STEHT NICHT AUF DER TAGESORDNUNG DER FÜHRUNGSKRÄFTE

Entsprechend den Vorgaben der DSGVO liegt die Verantwortung bei mehreren internen sowie externen Verantwortlichen. Viele Unternehmen sind sich über die Zuständigkeiten nicht im Klaren. Das führt dazu, dass keine Prozesse zur Gewährleistung der Compliance implementiert werden.

In der Mehrzahl der Unternehmen (74 Prozent) wurde ein abteilungsübergreifendes Team gebildet, das die Compliance mit der DSGVO voranbringen soll. Doch nur 26 Prozent der IT-Entscheidungsträger gaben an, dass der Vorstand und die Geschäftsführung das DSGVO-Programm kennen und darin eingebunden sind.

Wenn sich die Führungsebene nicht einbringt und beteiligt, wird es Unternehmen schwer fallen, die erforderlichen Änderungen zu implementieren.

An Projektteams zur Erreichung der DSGVO-Compliance beteiligte Abteilungen (Wählen Sie alle zutreffenden Antworten.)



In den meisten Unternehmen sind die Sicherheits- und IT-Abteilungen für die Gewährleistung der DSGVO-Compliance verantwortlich. Laut unserer Umfrage sind in 82 Prozent der Unternehmen die IT-Teams in die Einführung von Compliance-Maßnahmen involviert, die Marketing-Teams hingegen nur bei 27 Prozent der Unternehmen. In den meisten Fällen sind CIOs verantwortlich, aber die DSGVO betrifft nicht nur die IT- und Sicherheitsinitiativen, sondern alle Abteilungen.

Die wichtige Rolle der IT für die Compliance spiegelt sich in wachsenden Investitionen wider. Etwa 66 Prozent der IT-Entscheidungsträger gaben an, dass ihre Budgets in Vorbereitung auf den Mai 2018 erhöht wurden. Gleichzeitig sagen 57 Prozent, dass Compliance und Vorschriften bei ihren Sicherheitsprogrammen eine wichtige Rolle spielen. Diese Zahlen weisen darauf hin, dass sich die DSGVO für Sicherheits- und IT-Teams hervorragend eignet, um Aufmerksamkeit bei der Unternehmensführung zu erhalten.

Die DSGVO rückt die Bedeutung effektiver Abwehrmaßnahmen gegen Cyberangriffe ins Rampenlicht, denn sie bietet den IT- und Sicherheitsexperten der Unternehmen die Chance, die Mittel zu erhalten, um innovative Sicherheitsstrategien und entsprechend leistungsfähige Lösungen zur Verbesserung der Cybersicherheit entwickeln und implementieren zu können. Darüber hinaus steigen durch die DSGVO die Anforderungen an die Unternehmen bei der Einhaltung rechtlicher Vorgaben, und Datenschutz wird zugleich immer wichtiger für den wirtschaftlichen Erfolg des Unternehmens.

26 %

der IT-Entscheidungsträger gaben an, dass der Vorstand und die Geschäftsführung das DSGVO-Programm kennen und darin eingebunden sind.

66 %

der IT-Entscheidungsträger gaben an, dass ihre Budgets in Vorbereitung auf den Mai 2018 erhöht wurden.

57 %

der IT-Entscheidungsträger sagen, dass Compliance und Vorschriften bei ihren Sicherheitsprogrammen eine wichtige Rolle spielen.

VIELE UNTERNEHMEN BEREITEN SICH AUF DIE NICHT-COMPLIANCE VOR

In dieser Phase geht es bei der DSGVO einzig und allein um die Interpretation. Das ist wahrscheinlich der Grund dafür, warum sich viele Unternehmen mehr auf die Risikominimierung konzentrieren, statt vollständige Compliance anzuvisieren.

Unternehmen sind sich bewusst, dass sie fortschrittliche Informations- und Cybersicherheitskontrolle benötigen. Sie wissen auch, dass von ihnen erwartet wird, die DSGVO einzuhalten. Doch da die Verordnung als äußerst komplex wahrgenommen wird, bereiten sich einige lieber auf die Nicht-Compliance vor.

39 %

der Unternehmen gaben an, dass sie finanziell auf die Bußgelder vorbereitet sind, die nach dem Inkrafttreten der DSGVO verhängt werden können.

24 %

der Befragten sagten, dass sie für den Fall einer Sicherheitsverletzung eine Versicherung gegen Datenschutzverletzungen abgeschlossen haben.

Einige Unternehmen glauben, dass sie die finanziellen Risiken der Nichteinhaltung von DSGVO-Auflagen nach Mai 2018 kennen. In unserer Umfrage gaben 39 Prozent der Unternehmen an, dass sie finanziell auf die Bußgelder vorbereitet sind, die nach dem Inkrafttreten der DSGVO verhängt werden können.

Einige Unternehmen haben entschieden, die Risiken zu übertragen: Fast ein Viertel (24 Prozent) der Befragten hat für den Fall einer Sicherheitsverletzung eine Versicherung gegen Datenschutzverletzungen abgeschlossen.

Diese Versicherung kann die Kosten einer Sicherheitsverletzung senken. Dies umfasst auch sekundäre Kosten wie den Aufwand für die Eindämmung, Kommunikation, Untersuchung und Beseitigung. Die Bußgelder für die Nichteinhaltung der DSGVO-Grundsätze sind bei diesen Versicherungen jedoch in vielen Fällen nicht abgedeckt. Daher benötigen Sie mehrere Schutzebenen, einschließlich technischer und organisatorischer Maßnahmen zum Schutz der Integrität und Vertraulichkeit der personenbezogenen Daten von EU-Bürgern.

VORBEREITUNG AUF DIE DSGVO: SCHUTZ IHRER WICHTIGEN RESSOURCEN

Bevor Unternehmen vollständige Compliance anstreben können, müssen sie zunächst die Auflagen vollständig verstehen. Alle Regelungen und Vorgaben der DSGVO fallen unter einen von sieben Grundsätzen.

Dabei besagt Grundsatz 6 (Integrität und Vertraulichkeit), dass personenbezogene Daten möglichst anonymisiert werden sollen. Mit dieser Anonymisierung soll gewährleistet werden, dass EU-Bürger mithilfe dieser Daten nicht mehr identifiziert werden können. Für Daten, die nicht anonymisiert werden können, schreibt die DSGVO technische sowie organisatorische Maßnahmen vor, die die Verarbeitung aller personenbezogenen Daten kontrollieren.

Die Verantwortung für den Schutz der Daten liegt jetzt nicht mehr nur bei den Unternehmen, die die Daten von EU-Bürgern erfassen. Laut DSGVO sind externe Datenverarbeiter dafür verantwortlich, dass die ihnen anvertrauten Daten vertraulich bleiben. Laut unserer Umfrage kennen nur 30 Prozent der Unternehmen alle externen Parteien, die in ihrem Namen personenbezogene Daten von EU-Bürgern verarbeiten.

Laut dem „2017 Verizon Data Breach Investigations Report“ (Verizon-Untersuchungsbericht zu Datenkompromittierungen für 2017) erfolgen mehr als 80 Prozent der Datenschutzverletzungen aufgrund von Datendiebstahl durch Cyberkriminelle. Dennoch zeigt unsere Umfrage, dass nur 46 Prozent der Unternehmen hochentwickelte Sicherheitslösungen verwenden, um solche Diebstähle zu verhindern. Mehr noch: 9 Prozent der Unternehmen haben nicht vor, eine entsprechende Lösung zu implementieren, sodass sie vollständig ungeschützt sind.

43 %

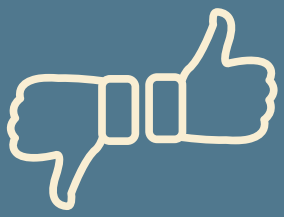
der Unternehmen verschlüsseln derzeit alle personenbezogenen Daten von EU-Bürgern, und 29 Prozent wollen die Verschlüsselung bis Mai 2018 einführen. Diese Zahlen sind erschreckend, da Unternehmen auf den Einsatz von Lösungen verzichten, mit denen sie ihre wichtigsten Ressourcen identifizieren und schützen können.

33,5 %

der Umfrageteilnehmer haben eine Richtlinie zum Schutz und zur Verarbeitung von Daten erstellt und kommuniziert.

30,3 %

der Umfrageteilnehmer kennen alle externen Parteien, die personenbezogene Daten von EU-Bürgern in ihrem Auftrag verarbeiten.



17,9 %

der Umfrageteilnehmer verfügen über einen Prozess zum Testen der Wirksamkeit von Datenschutzkontrollen

(einschließlich externer Parteien, die in ihrem Auftrag Daten verarbeiten).

DER COUNTDOWN LÄUFT

Die Unternehmen scheinen vor Herausforderungen zu stehen, die sie nicht bewältigen können: Ihnen drohen erhebliche Bußgelder. Sie müssen proaktiv Maßnahmen treffen, um Compliance-Vorschriften einzuhalten. Und sie müssen gleichzeitig Unklarheiten in Bezug auf die tatsächlichen Vorgaben umschiffen.

Die Verordnung tritt bereits in sechs Monaten in Kraft. Daher müssen Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten und noch kein DSGVO-Programm implementiert haben, dringend handeln.

Unsere Umfrage zeigt, dass Unternehmen bei der Vorbereitung auf die DSGVO unterschiedliche Ansätze verfolgen. Gleichzeitig wird deutlich, dass Wahrnehmung und Realität deutlich voneinander abweichen. Unternehmen glauben, dass sie bis zum Stichtag im Mai 2018 die DSGVO einhalten werden. Unsere Umfrageergebnisse sowie andere Studien stellen das jedoch in Frage.

Die Einhaltung der DSGVO ist zweifellos ein komplexes Unterfangen, sollte jedoch nicht als Last empfunden werden. Tatsächlich betrachten 46 Prozent der befragten Unternehmen die DSGVO als Wettbewerbsvorteil, mit dem die Unternehmen durch den verantwortungsvollen Umgang mit persönlichen Daten in der Öffentlichkeit punkten können. Mit Compliance lassen sich das Vertrauen der Kunden gewinnen und Kundentreue erreichen. Darüber hinaus unterstützt Compliance die digitale Transformation auf sichere und konforme Weise.

46 % der befragten Unternehmen betrachten die Einhaltung der DSGVO als Wettbewerbsvorteil, da sie das Engagement für Datenschutz unterstreicht.

FAZIT

Die Zahl der Datenschutzverletzungen war noch nie so hoch. Deshalb ist es an der Zeit, alle personenbezogenen Daten von EU-Bürgern zu identifizieren sowie zu schützen und damit die Einhaltung der DSGVO voranzutreiben. Unternehmen, die das nicht leisten können oder wollen, müssen mit schwerwiegenden Konsequenzen rechnen.

Ein auf Compliance und Standards aufbauendes Framework ist zudem geeignet, mehr Kunden anzusprechen und zu binden. Durch die Einhaltung der DSGVO können Unternehmen zeigen, dass sie in Sicherheit, Datenschutz sowie Kundendienst investieren. Und durch den Aufbau des Vertrauens bei ihren Kunden können sie sich vom Wettbewerb abheben und auf dem zunehmend von Wettbewerb geprägten, globalen Markt wachsen.

Zum Schließen der Lücke zur Einhaltung der Datenschutzgrundverordnung empfehlen wir einen vierstufigen Ansatz:

1. **Erkennen und Klassifizieren aller personenbezogenen Daten**
2. **Erstellen eines Plans zum Schließen aller gefunden Lücken in den Schutzmaßnahmen**
3. **Schutz aller personenbezogenen Daten durch die Entwicklung und Implementierung wirksamer Sicherheitskontrollen**
4. **Verbesserte Sicherheitskontrollen: Überwachen, Erkennen, Beheben und Melden aller Richtlinienverstöße und externen Bedrohungen**

Weitere Informationen dazu, wie Sie Ihr Unternehmen für die DSGVO fit machen können, erhalten Sie unter **proofpoint.com/GDPR**.

INFORMATIONEN ZU PROOFPOINT

Proofpoint, Inc. (NASDAQ: PFPT) ist ein Cybersicherheitsunternehmen der nächsten Generation, das Unternehmen dabei unterstützt, die Arbeitsabläufe ihrer Mitarbeiter vor hochentwickelten Bedrohungen und Compliance-Risiken zu schützen. Dank Proofpoint können Cybersicherheitsexperten ihre Benutzer vor raffinierten und zielgerichteten Angriffen (per E-Mail, Mobilgeräte-Apps und Social Media) schützen, wichtige Informationen absichern und ihre Sicherheitsteams mit den notwendigen Bedrohungsdaten sowie Tools ausstatten, um bei Zwischenfällen schnell zu reagieren. Führende Unternehmen aller Größen, darunter mehr als 50 Prozent der Fortune 100, nutzen Proofpoint-Lösungen. Diese wurden für moderne IT-Umgebungen mit Mobilgeräten und Social Media konzipiert und nutzen die Möglichkeiten der Cloud sowie eine Big-Data-Analyseplattform zur Abwehr aktueller raffinierter Bedrohungen.

proofpoint®

www.proofpoint.com/de