RSA

RSA DATA PRIVACY & SECURITY REPORT

BUSINESS-DRIVEN SECURITY™

EINFÜHRUNG

Risiko und Sicherheit konvergieren

Cybersicherheits-Vorfälle nehmen extrem zu, ohne dass ein Ende in Sicht ist. Die Folgen hinsichtlich Betriebsunterbrechungen, Kosten und Datenschutzverletzungen haben weltweit eine Welle von Gesetzen und staatlichen Regulierungen ausgelöst.

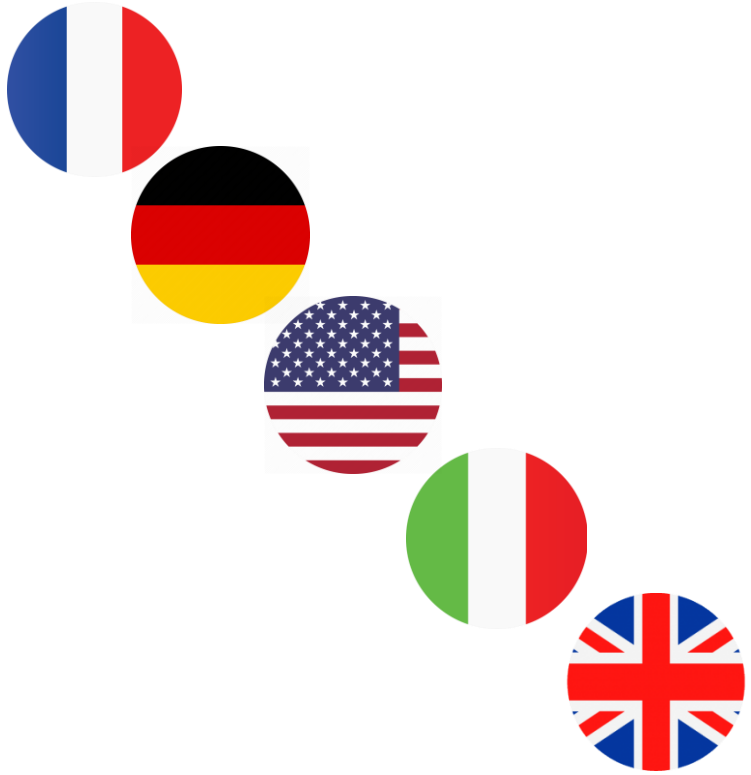
Die Einführung neuer Vorschriften steht bevor und die Verbraucher achten zunehmend darauf, was mit ihren Daten geschieht. Geschäftsrisiken und Cybersicherheit konvergieren. Vor diesem Hintergrund bewegen sich Unternehmen heute häufig auf unbekanntem Terrain. Vorschriften wie die Datenschutz-Grundverordnung der Europäischen Union (DSGVO) zwingen Risiko-, Sicherheits-, Compliance- und Geschäftsbereichs-Verantwortliche zu dem schwierigen Spagat zwischen Sicherheits- und Datenschutz-Zielen auf der einen Seite und Unternehmenswachstum und Innovation auf der anderen.

Eine Flut von Gesetzen und Vorschriften

Jedes Unternehmen, das personenbezogene Informationen von EU-Bürgern verarbeitet, unterliegt der DSGVO, die ab 25. Mai 2018 anzuwenden ist. Hauptziele der Verordnung sind, den europäischen Bürgern mehr Kontrolle und Transparenz hinsichtlich ihrer personenbezogenen Daten zu garantieren sowie den Datenschutz insgesamt zu stärken und zu vereinheitlichen. Allein im Jahr 2017 verabschiedeten 28 amerikanische Bundesstaaten Gesetze zur Cybersicherheit. Weltweit hat jedes bedeutende Land eine Form von Gesetz erlassen: China und Australien setzten im vergangenen Jahr Datenschutzregelungen in Kraft, in der Europäische Union – und in UK – gilt ab Mai 2018 die DSGVO. In Ermangelung allgemein verbindlicher Standards müssen Unternehmen jeder Größe Änderungen im Sicherheits- und Regulierungsumfeld ständig im Auge behalten und sich gegebenenfalls auf neue Vorschriften einstellen.

Die Erwartungen der Verbraucher an den Datenschutz und die entsprechenden Regulierungen machen so aus dem Cyberrisiko weltweit ein Unternehmensrisiko.

ÜBER DIE UMFRAGE



Ziel der ersten **RSA® Umfrage zu Datenschutz und Datensicherheit** ist, den Wert zu ermitteln, den der durchschnittliche Verbraucher dem Datenschutz beimisst. Zudem wird untersucht, wie sich Datenerfassung, Datenspeicherung, Compliance und Sicherheitstrends auf Unternehmen auswirken.

Vor uns liegt ein weiteres Jahr mit zahlreichen Cyber- und Geschäftsrisiken. Die Unternehmen stellen sich auf die Datenschutzforderungen ihrer Kunden und auf die gesetzlichen Vorschriften ein, die weltweit gelten bzw. branchenspezifische Märkte regeln.

In diesem Zusammenhang fragten wir Verbraucher in Frankreich, Deutschland, Italien, im Vereinigten Königreich und in den Vereinigten Staaten nach dem Einfluss, den der Schutz der Privatsphäre, der Umgang mit Daten und die Einhaltung von Vorschriften auf ihre Beziehungen zu Unternehmen hat.

Einige der Reaktionen waren zu erwarten – den Verbrauchern ist der Schutz ihrer Bank- und Sicherheitsinformationen wichtig (die häufigste Antwort in allen Ländern) –, aber wir stießen auch auf überraschende Ergebnisse. So stellten wir fest, dass das Verbraucherverhalten weniger von der Angst vor Hackern als vielmehr vom Wunsch geprägt ist, Marketingmaßnahmen aus dem Weg zu gehen. Mehr als 40 % der Teilnehmer räumten ein, dass sie personenbezogene Daten und Informationen fälschen, wenn sie sich online für Produkte und Dienstleistungen registrieren.

Um die geschäftlichen Auswirkungen des Verbraucherverhaltens zu ermitteln, fragten wir auch, inwieweit die Konsumenten ein Unternehmen nach einer Datenschutzverletzung oder einem anderen Vorfall meiden würden.

Wir freuen uns, die Ergebnisse der RSA Umfrage zu Datenschutz und Datensicherheit präsentieren zu können.

Wir hoffen, diese Informationen sind für Sie interessant und aufschlussreich.

METHODE

Wir befragten über

7.500

VERBRAUCHER

FRANKREICH DEUTSCHLAND ITALIEN UK USA

Wenn nichts Gegenteiliges angegeben ist, stammen alle Zahlen von YouGov Plc.

GESAMTUMFANG DER STICHPROBE:

7.579

FRANKREICH	DEUTSCHLAND	ITALIEN	UK	USA
1.025	2.232	1.134	2.112	1.076

DIE UMFRAGE FAND ZWISCHEN DEM 15. DEZEMBER 2017 UND 3. JANUAR 2018 STATT

DIE UMFRAGE WURDE ONLINE DURCHGEFÜHRT

DIE ZAHLEN WURDEN GEWICHTET UND SIND FÜR ALLE ERWACHSENEN (ÜBER 18) IN DER JEWEILIGEN REGION REPRÄSENTATIV

RSA

HAUPTERKENNTNIS 1

Den Verbrauchern ist ihr finanzielles Wohl am wichtigsten … aber das könnte sich ändern.

Die Definition personenbezogener Informationen wird zwar laufend erweitert – die DSGVO bezieht alles von Namen, Fotos, Beiträgen in sozialen Medien, E-Mail-Adressen, Bankdaten und IP-Adressen bis hin zu genetischen Daten mit ein –, aber die größten Bedenken der Verbraucher in Bezug auf den Verlust personenbezogener Informationen beziehen sich eher auf traditionelle Finanz-, Sicherheits- und Identitätsdaten.

Jede demografische Gruppe in unserer Umfrage gab Finanz- und Bankinformationen als wichtigste Sorge in Bezug auf Datenverlust an. Aber jüngere Millennials (zwischen 18 und 24) hatten viel mehr Bedenken, dass sie mit gestohlenen personenbezogenen Informationen (Nachrichten oder Fotos) erpresst werden könnten.

80 %

DER TEILNEHMER GABEN FINANZ- & BANKINFORMATIONEN AN; DAMIT IST DIES DER WICHTIGSTE SORGENFAKTOR IN BEZUG AUF DATENVERLUST

76 %

DER TEILNEHMER GABEN SICHERHEITSINFORMATIONEN (PASSWÖRTER), 72 % AUSWEISDOKUMENTE (PASS, FÜHRERSCHEIN) ALS KRITERIEN AN, DIE IHNEN SORGEN BEREITEN

51 %

DER JÜNGEREN MILLENIALS (18-24 J.) IN DER UMFRAGE HABEN ANGST VOR ERPRESSUNG MIT PERSONENBEZOGENEN INFORMATIONEN

84 %

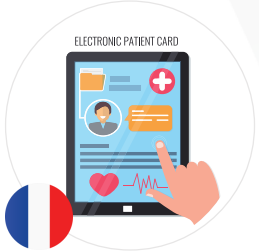
DER TEILNEHMER AUS DEM UK UND 81 % AUS ITALIEN GABEN SICHERHEITSINFORMATIONEN ALS SORGENFAKTOR AN; DAMIT LIEGEN BEIDE LÄNDER ÜBER DEM GLOBALEN DURCHSCHNITT

51 %

DER DEUTSCHEN TEILNEHMER LEGEN WERT AUF DEN SCHUTZ IHRER GENETISCHEN DATEN IM VERGLEICH ZU NUR 39 % IN ITALIEN UND FRANKREICH

46 %

DER AMERIKANISCHEN TEILNEHMER SORGEN SICH UM STANDORT-INFORMATIONEN, DAS IST DER HÖCHSTE PROZENTSATZ ALLER LÄNDER



45 %

DER FRANZÖSISCHEN TEILNEHMER GABEN MEDIZINISCHE DATEN ALS GRUND ZUR SORGE AN, IM VERGLEICH ZU 59 % ALLER BEFRAGTEN

RSA

HAUPTERKENNTNIS 2

Das Verbraucherbewusstsein in Bezug auf Datenerfassung und Sicherheitsverletzungen steigt: 73 % der Befragten gaben an, dass ihnen Datenschutzverletzungen mehr bewusst sind als noch vor fünf Jahren.

49 %

DER AMERIKANISCHEN TEILNEHMER GABEN AN, DASS IHNEN DATENSCHUTZVERLETZUNGEN WESENTLICH MEHR BEWUSST SIND ALS FRÜHER

62 %

ALLE TEILNEHMER ERKLÄRTEN, SIE WÜRDEN DEM BETREFFENDEN UNTERNEHMEN DEN VERLUST IHRER DATEN ANLASTEN UND DAMIT NOCH VOR DEN HACKERN. DIE VERBRAUCHER SIND IMMER BESSER INFORMIERT UND ERWARTEN DESHALB MEHR TRANSPARENZ UND REAKTIONSBEREITSCHAFT VON DEN VERANTWORTLICHEN FÜR IHRE DATEN

72 STUNDEN

EIN FAKTOR, DER DIE DATENTRANSPARENZ FÜR VERBRAUCHER IM KOMMENDEN JAHR ERHÖHT, SIND DIE NEUEN MELDE- UND BERICHTSPFLICHTEN BEZÜGLICH DATENSCHUTZVERLETZUNGEN

RSA

HAUPTERKENNTNIS 3

Die Einstellung der Verbraucher gegenüber Datenerfassung verändert sich. 41 % der Teilnehmer räumten ein, dass sie personenbezogene Daten und Informationen absichtlich fälschen, wenn sie sich online für Produkte oder Dienstleistungen registrieren.

59 %

DER TEILNEHMER, DIE DATEN FÄLSCHTEN, WOLLTEN DAMIT UNERWÜNSCHTE KOMMUNIKATION VERMEIDEN; 55 % ERKLÄRTEN, SIE WOLLTEN NICHT ZIEL VON MARKETINGMAßNAHMEN WERDEN

35 %

FÄLSCHTEN INFORMATIONEN WEGEN SICHERHEITSBEDENKEN

55 %

VERMEIDEN DIE WEITERGABE VON DATEN AN EIN UNTERNEHMEN, DAS DATEN OHNE EINWILLIGUNG VERKAUFT ODER MISSBRAUCHT HAT

54 %

WERDEN WENIGER WAHRSCHEINLICH PRODUKTE / DIENSTLEISTUNGEN VON EINEM UNTERNEHMEN KAUFEN, VON DEM SIE WISSEN, DASS ES MIT DATEN NICHT KORREKT UMGEGANGEN IST

78 %

DER TEILNEHMER BESCHRÄNKEN DIE MENGE AN PERSONENBEZOGENEN INFORMATIONEN, DIE SIE ONLINE STELLEN ODER AN UNTERNEHMEN WEITERGEBEN

HAUPTERKENNTNIS 3

(Forts.)

82 %

DER TEILNEHMER AUS DEM UK GABEN AN, DASS SIE EIN UNTERNEHMEN BOYKOTTIEREN WÜRDEN, DAS WIEDERHOLT GEZEIGT HAT, DASS ES KEINE RÜCKSICHT AUF DEN SCHUTZ VON KUNDENDATEN NIMMT (72 % IN DEN USA, 69 % IN FRANKREICH, 64 % IN ITALIEN UND 57 % IN DEUTSCHLAND)

31 %

GLAUBEN, DASS UNTERNEHMEN, DIE MEHR DATEN ÜBER IHRE KUNDEN HABEN, BESSERE UND PERSONALISIERTERE PRODUKTE / DIENSTLEISTUNGEN ANBIETEN KÖNNEN, WOBEI NUR 26 % GERN DAZU BEREIT SIND, IHRE DATEN WEITERZUGEBEN, WENN SIE IM GEGENZUG DAFÜR EIN VERBESSERTES EINKAUFSERLEBNIS UND EINEN OPTIMIERTEN KUNDENSERVICE BEKOMMEN

50 %

KAUFEN WAHRSCHEINLICHER BEI EINEM UNTERNEHMEN, DAS NACHWEISEN KANN, DASS ES DATENSCHUTZ ERNST NIMMT (BEISPIELSWEISE, WENN ES KLARE INFORMATIONEN ZU SEINEN RICHTLINIEN IN BEZUG AUF DATENSCHUTZ UND SCHUTZ DER PRIVATSPHÄRE UND DIE VERWENDUNG DER DATEN BEREITSTELLEN KÖNNTE)

RSA

FAZIT

Was bedeutet das für die Unternehmen?

Wie die Umfrageergebnisse und die Datenschutzgesetze zeigen, sind Datenschutz und Datensicherheit ein wirklich globales Thema. Beispielsweise gilt die DSGVO für jedes Unternehmen, das Daten von EU-Bürgern verarbeitet, also auch für britische Firmen nach dem Brexit oder für US-amerikanische Cloud-Anbieter sowie für jedes andere Unternehmen, das Produkte oder Dienstleistungen an Bürger der EU verkauft.

Aufgrund der weitreichenden Folgen dieser Verordnung, aber auch wegen des steigenden Bewusstseins der Verbraucher und der potenziellen finanziellen Auswirkungen von Kundenbeschwerden und regulatorischen Maßnahmen, müssen die Unternehmen ihre Infrastruktur für die Datenerfassung und -verarbeitung jetzt auf den Prüfstand stellen und ihr zukünftiges Risikopotenzial analysieren.

Verstößt ein Unternehmen gegen die DSGVO – beispielsweise wegen mangelnder Kontrollmechanismen, des Verlusts von Kundendaten oder indem es betroffenen Personen ihre personenbezogenen Daten nicht innerhalb „einer angemessenen Frist“ zugänglich macht – riskiert es Geldbußen in Höhe von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes oder 20 Millionen Euro, je nachdem, welcher der Beträge höher ist.

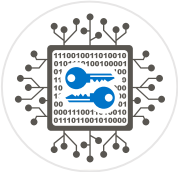
Die Unternehmen treiben die Digitalisierung weiter voran und nutzen vermehrt digitale Ressourcen, Services und Big Data. Damit steigt auch ihre Verantwortung für die routinemäßige Überwachung und den laufenden Schutz der Daten.

Mit der praktischen Umsetzung neuer Vorschriften wie der DSGVO werden die Gesamtkosten für Verstöße gegen Datenschutzgesetze höher, da Bußgeldzahlungen zu den anderen Kosten einer Datenschutzverletzung hinzukommen. Um dem vorzubeugen, müssen die Unternehmen wissen, wo ihre Daten gespeichert sind, wer Zugriff darauf hat und wie sie gesichert sind. Nur dann können sie das Risiko analysieren, das sie für ihr Unternehmen darstellen.

MAßNAHMEN, DIE UNTERNEHMEN HEUTE ERGREIFEN KÖNNEN

ANALYSIEREN SIE, WELCHE PERSONENBEZOGENEN DATEN SIE HEUTE VERARBEITEN:

Es geht nicht nur um das Wissen, wie personenbezogene Daten definiert sind, sondern auch darum, wo sie gespeichert sind, wie sie verwendet werden und welche Mitarbeiter Zugriff darauf haben. Setzen Sie Ihre Erkenntnisse über alle Aspekte des Datenschutzes in praktische Prozesse um.



ERGREIFEN SIE DATENSCHUTZMAßNAHMEN AUF JEDER EBENE:

Etablieren Sie eine „Datenschutz-DNA“, indem Sie entsprechende Maßnahmen auf jeder Ebene umsetzen – auf der technologischen wie auf der geschäftlichen Ebene. Sie müssen einen wirklich ganzheitlichen Ansatz verfolgen, um Ihr Unternehmen erfolgreich auf die Sicherheitsrisiken einzustellen.

VERFOLGEN SIE EINEN RISIKOBASIERTEN ANSATZ:

Risiko-, Daten-, Sicherheits- und Compliance-Teams müssen gemeinsam mit Bereichsleitern am Schutz Ihres Unternehmens und vor allem am Schutz Ihrer Kundendaten arbeiten.

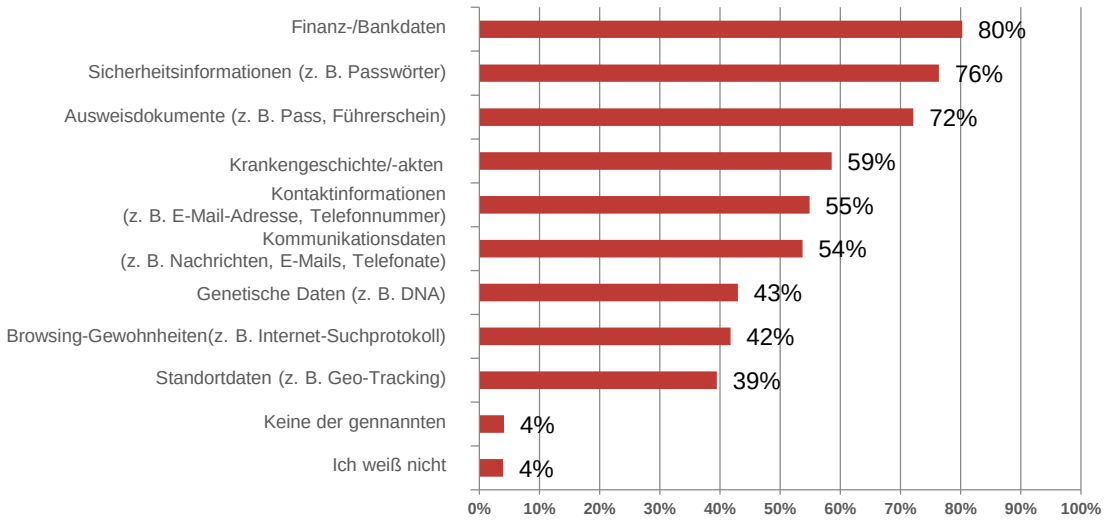
ACHTEN SIE AUF EINEN GEMISCHTEN ANSATZ:

Bei der Entwicklung Ihrer Strategie müssen sie die folgenden vier Punkte berücksichtigen: Reaktion auf Datenschutzverletzungen, Daten-Governance, Risikobewertung und Compliance-Management. Sind Sie auf jede Art von Datenschutzverletzung vorbereitet? Wie regeln Sie den Zugriff auf Ihre Daten? Wie dokumentieren Sie Ihre Datenverarbeitungsprozesse, damit sie entsprechende Governance-Regeln implementieren können? Ein wichtiger Faktor dabei ist die Bewertung der Risiken im Zusammenhang mit diesen Daten, um letztlich Ihre Compliance nachweisen zu können.

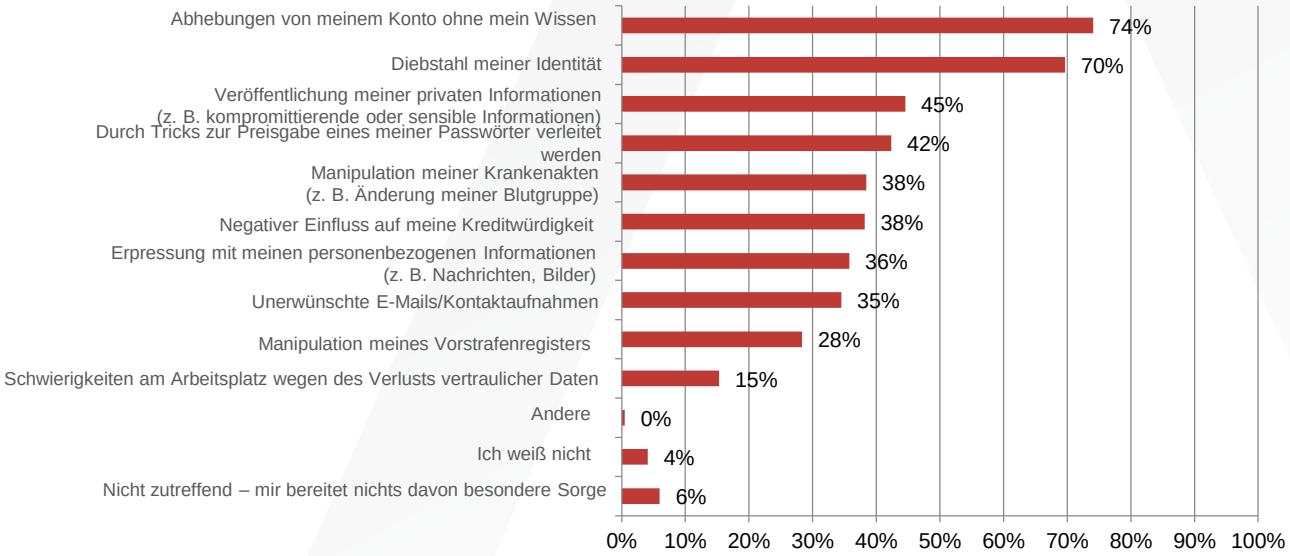
Weitere Informationen zur DSGVO und zum Datenschutz finden Sie hier:
https://www.rsa.com/de-de/solutions/gdpr-compliance-with-rsa

ALLE ERGEBNISSE DER STUDIE

Welche der folgenden Arten persönlicher Informationen/Daten möchten Sie geschützt wissen?

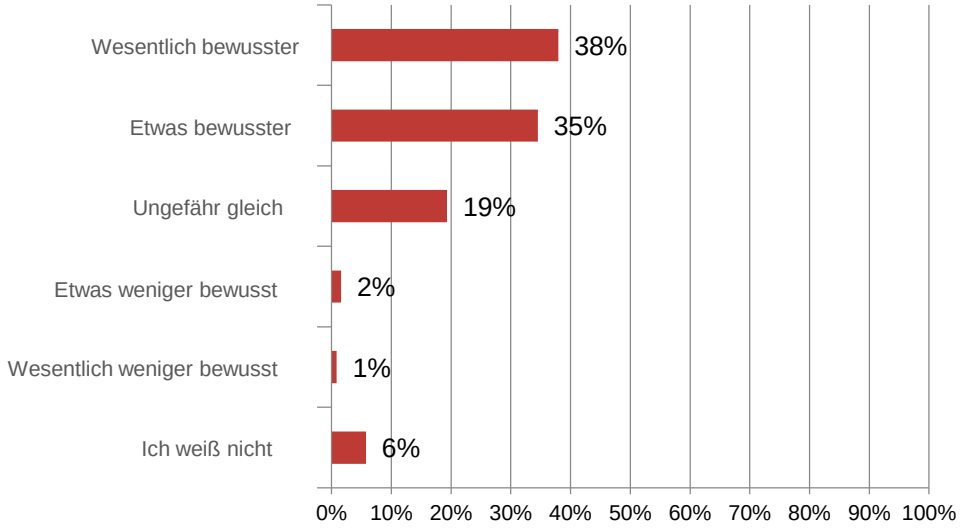


In Bezug auf welchen der folgenden Faktoren (falls zutreffend) haben Sie Bedenken?

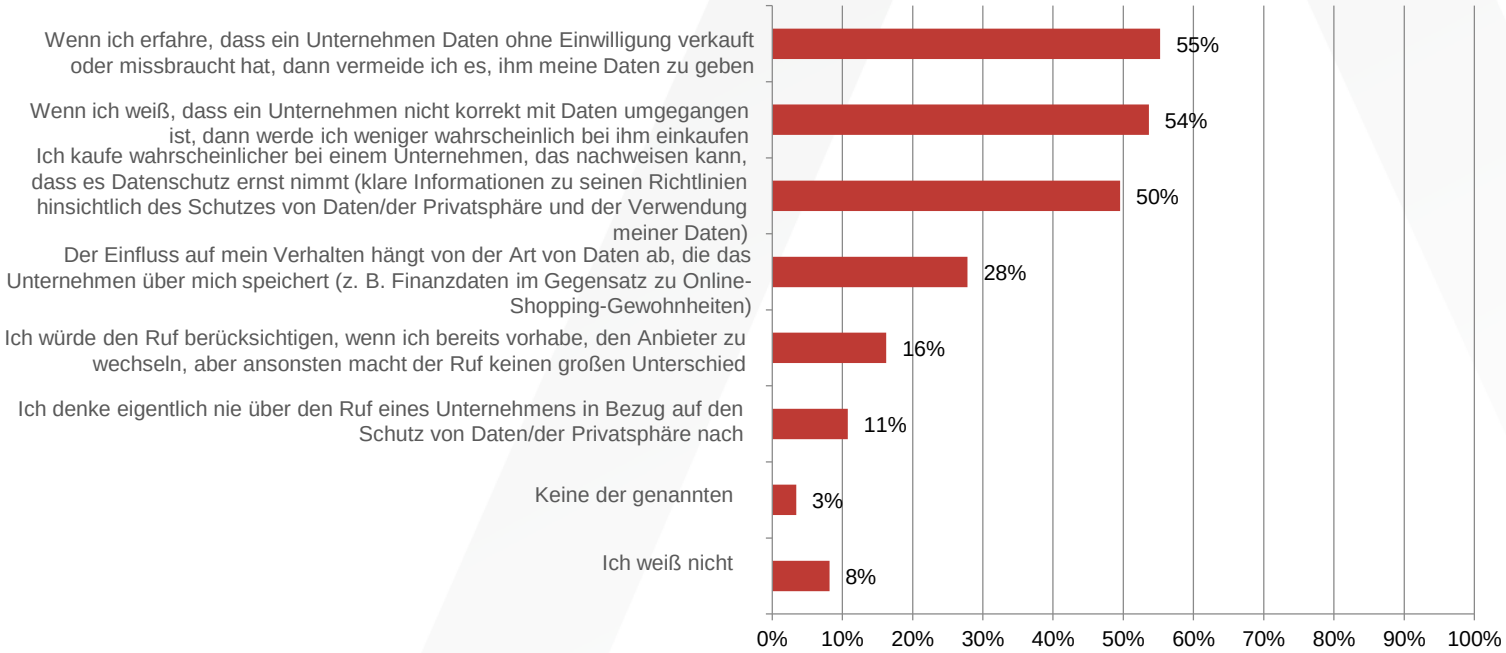


ALLE ERGEBNISSE DER STUDIE

Würden Sie sagen, dass Ihnen im Vergleich zu fünf Jahren (d. h. 2012) Datenschutzverletzungen heute stärker oder weniger bewusst sind?

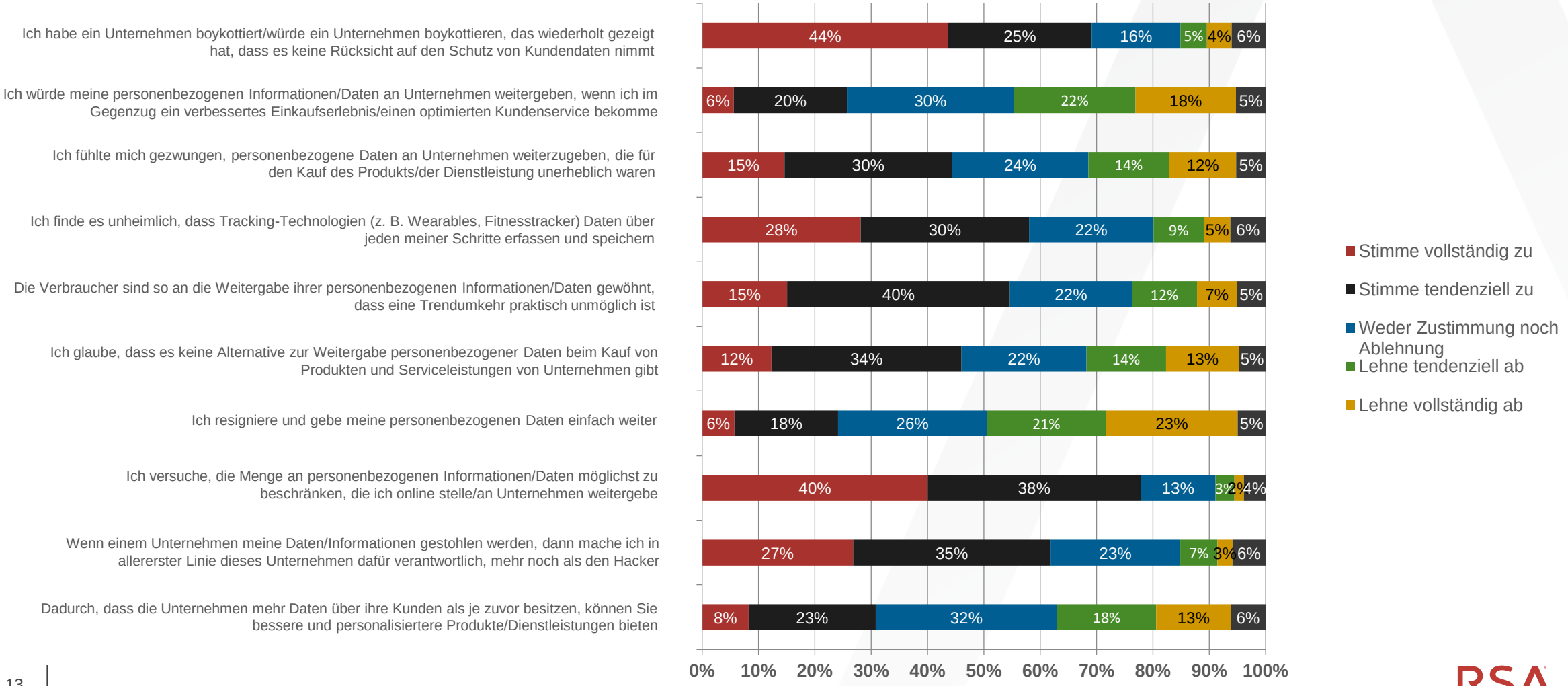


Welche der folgenden Aussagen trifft auf Sie zu?



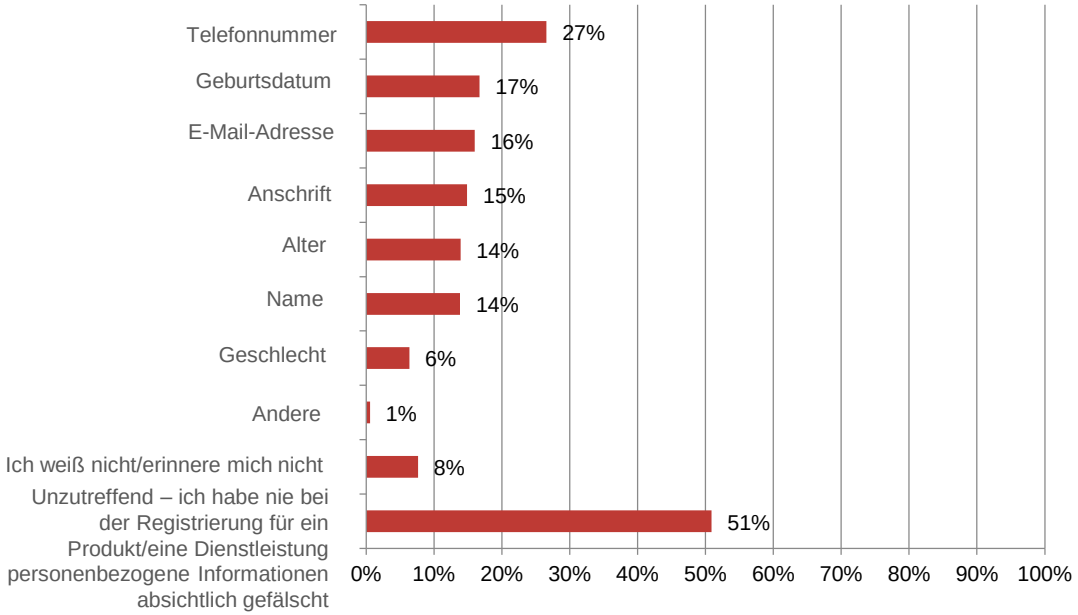
ALLE ERGEBNISSE DER STUDIE

Inwieweit, wenn überhaupt, stimmen Sie den folgenden Aussagen zu?



ALLE ERGEBNISSE DER STUDIE

Welche der folgenden personenbezogenen Informationen haben Sie bei der Registrierung für ein Produkt/eine Dienstleistung schon einmal absichtlich gefälscht



Sie haben angegeben, dass Sie bei der Registrierung für ein Produkt/eine Dienstleistung Informationen absichtlich gefälscht haben ... Welchen der folgenden Gründe hatten Sie?