



EU-Datenschutz- Grundverordnung (DSGVO)

Sind Sie bereit?





Inhalt

Vorwort und Einführung	3
Umfang der Studie	3
Wichtige Ergebnisse	4
Informationsstand bezüglich der DSGVO	5
Auswirkungen der DSGVO auf Unternehmen	5
Neue Vorschriften verursachen Aufwand für viele Unternehmen	5
Vorbereiten für die DSGVO	6
Implementieren von Compliance-Plänen für die DSGVO	6
Technologische Herausforderungen bei der DSGVO-Compliance	6
Aktuelle Hürden für die DSGVO-Compliance	7
Aktuelle Testing-Verfahren entsprechen nicht der Norm	7
Compliance-Lücken in aktuellen Prozessen	7
Löschen von Kundendaten „ohne Verzögerung“	8
Ermöglichen des Zugriffs von Kunden auf ihre Daten	8
Technologien zur Unterstützung der DSGVO-Compliance	9
Notwendigkeit von Investitionen in Technologien	9
Technologien zur Förderung von Compliance in Testumgebungen	9
Nutzung synthetisch erzeugter Daten	10
Pseudonymisierung	10
Fazit	11

Vorwort und Einführung

Vorwort

Die Datenschutz-Grundverordnung (DSGVO) ist eine neue Komponente der Rechtsordnung in der Europäischen Union (EU), die über Jahre verhandelt wurde. Sie wird allgemein als die größte Veränderung im Zusammenhang mit der digitalen Privatsphäre in Europa in den letzten 20 Jahren betrachtet. Im wachsenden digitalen Geschäftsumfeld von heute ist es so wichtig wie nie, dass eindeutige Gesetze mit Richtlinien festgelegt werden.

Im Juni 2016 wurde in Großbritannien ein Referendum abgehalten, bei dem die Mehrheit für den Austritt aus der EU gestimmt hat. Was bedeuten die Ergebnisse des Referendums für britische Unternehmen? Müssen sie sich weiterhin an die DSGVO halten?

Die britischen Befragten dieser Studie erkennen an, dass alle Unternehmen außerhalb der EU, die auf dem Europäischen Binnenmarkt Handel treiben möchten, die DSGVO bis zum 25. Mai 2018 umsetzen müssen, unabhängig von der Mitgliedschaft des jeweiligen Landes in der EU.

In diesem Dokument wird aufgezeigt, dass trotz dieser Einsicht viel Arbeit auf beiden Seiten des Atlantiks erledigt werden muss, um DSGVO-Compliance zu erreichen. In der DSGVO wurde die Definition persönlicher Daten erweitert, sodass es für IT- und Testing-Abteilungen von größter Wichtigkeit ist, in Testing- und Entwicklungsumgebungen persönliche Daten zu schützen.

Unternehmen werden Hilfe benötigen, und CA Technologies bietet ein Spektrum an Lösungen, die Unternehmen in ihren Programmen zur Einhaltung der DSGVO unterstützen können. Auf diese Weise wird die Wettbewerbsfähigkeit Ihres Unternehmens in der heutigen globalisierten, digitalen Welt gestärkt.

Christoph Luykx

Director, Government Relations EMEA

CA Technologies



Einführung

Dieses White Paper enthält die Ergebnisse einer von CA Technologies in Auftrag gegebenen Studie zur Analyse der Vorbereitungen in Unternehmen im Zusammenhang mit der Erfüllung der Compliance-Anforderungen für die DSGVO. Im Hinblick darauf, dass die DSGVO weitreichende Auswirkungen auf die Daten hat, die in Umgebungen außerhalb der Produktion verwendet werden, ging es CA Technologies in erster Linie darum zu verstehen, wie Unternehmen für die DSGVO planen und welche Prozesse und Technologien sie zur Unterstützung benötigen.

Umfang der Studie

Dieses Dokument basiert auf den Ergebnissen einer von Vanson Bourne durchgeführten Umfrage. Die Befragungen begannen in der Woche, in der die DSGVO angekündigt wurde (April 2016). Insgesamt wurden 200 B2B-Befragungen durchgeführt: 167 IT-Entscheidungsträger (ITDMs) und 33 Entscheidungsträger im Bereich Risiko und Compliance (RCDMs). 98 der 200 Befragten sind Personen der Vorstandsebene, die übrigen sind erfahrene Führungskräfte.

Die Befragten arbeiten in Unternehmen mit mindestens 500 Mitarbeitern, einem globalen Jahresumsatz von mehr als 1 Milliarde USD und u. a. aus den folgenden Wirtschaftssektoren:

- Finanzdienstleister (einschließlich Versicherungen)
- Fertigung
- Handel, Vertrieb und Transport
- Technologie und Telekommunikation
- Sonstige kommerzielle Sektoren
- Öffentlicher Sektor

Die Befragungen wurden online in Großbritannien (75) und den USA (125) durchgeführt. Anhand einer strengen, mehrschichtigen Vorauswahl wurde sichergestellt, dass nur geeignete Kandidaten teilnehmen konnten.

Wichtige Ergebnisse

Die DSGVO hat Auswirkungen auf Unternehmen

- Nur 46 % der Befragten sind vollständig über die DSGVO informiert.
- Nachdem sie mehr Informationen erhalten haben, sind 90 % der Meinung, dass die DSGVO Auswirkungen auf ihr Unternehmen haben wird.
- 89 % nannten mindestens einen Unternehmensbereich, den die DSGVO negativ beeinflussen wird.

Die Vorbereitung auf die DSGVO wird Zeit brauchen

- Es dauert durchschnittlich drei Monate, um einen Plan für die DSGVO-Compliance zu erstellen, und weitere drei Monate, ihn zu implementieren.
- Während der Implementierung wurden die Pläne durchschnittlich drei Mal überprüft.

Die meisten Unternehmen sind noch nicht bereit für die DSGVO

- 31 % geben an, dass die Testverfahren ihrer Unternehmen vollständig konform sind.
- Weniger als die Hälfte (46 %) sind äußerst zuversichtlich, dass ihr Unternehmen rechtzeitig vorbereitet sein wird.
- Nur ein Drittel (33 %) ist überzeugt, dass alle Kundendaten umgehend in allen Systemen und Anwendungen identifiziert werden können.
- 41 % denken, dass der Datenzugriff ausreichend differenziert beschränkt ist.
- Nur 34 % sind vollständig überzeugt, dass sie Kundendaten ohne Verzögerung löschen können.
- Nur 43 % wären vollständig in der Lage, einem Kunden die Daten in einem Format zur Verfügung zu stellen, das der Kunde nutzen und in andere Formate übertragen kann.

Unternehmen müssen für die Compliance in Technologien investieren

- 88 % geben an, dass technologische Herausforderungen ein Compliance-Risiko darstellen.
- 88 % der Befragten ist bewusst, dass ihr Unternehmen in neue Technologien oder Services investieren muss, um sich auf die Auswirkungen der DSGVO vorzubereiten.
- 58 % gehen davon aus, dass sie in Verschlüsselungstechnologien investieren müssen.
- 18 % nutzen gegenwärtig keine synthetische Datenerzeugung, könnten sie aber aufgrund der DSGVO einführen.



Informationsstand bezüglich der DSGVO

Die Europäische Union (EU) hat kürzlich einen neuen Rechtsakt beschlossen: die Datenschutz-Grundverordnung (DSGVO). Ziel der Verordnung ist eine Verbesserung des Schutzes persönlicher Daten, die von Unternehmen gespeichert werden. Wenn sie im Mai 2018 in Kraft tritt, muss sie von Unternehmen weltweit, die aus der EU stammende persönliche Daten besitzen, vollständig eingehalten werden. Daher müssen Unternehmen schon jetzt damit beginnen, die für die Datenverwaltung verwendeten Systeme zu überprüfen.

In der Woche, in der die DSGVO formal angenommen wurde (im April 2016), gaben nur 46 % der Befragten an, dass sie vollständig darüber informiert waren. Weitere 47 % wiesen einen gewissen Informationsstand auf, mussten aber Kenntnislücken eingestehen.

Auswirkungen der DSGVO auf Unternehmen

Es ist offensichtlich, dass viele Bereiche in den Unternehmen der Befragten von der DSGVO betroffen sein werden. Als den Befragten eine Definition der DSGVO gezeigt wurde, haben viele eingeräumt, dass sie beträchtliche Auswirkungen auf ihr Unternehmen haben wird. Mindestens neun von zehn gaben an, dass es Auswirkungen auf jeden der angegebenen Bereiche geben wird (Abbildung 2).

DSGVO-Auswirkungen

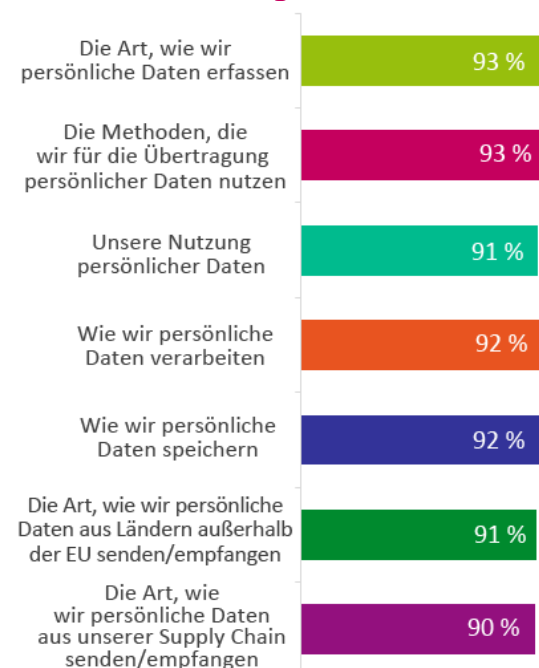


Abbildung 1: Analyse der Befragten, die angeben, dass jeder Bereich Auswirkungen auf ihr Unternehmen hat. Frage an alle 200 Befragten

Je besser der Informationsstand über die DSGVO unter den Befragten ist, desto größer sind die prognostizierten Auswirkungen auf das Unternehmen. IT-Entscheidungsträger (ITDMs) und Entscheidungsträger im Bereich Risiko und Compliance (RCDMs), die noch nicht umfassend über die DSGVO informiert sind, müssen noch herausfinden, welche Auswirkungen sich auf ihr Unternehmen ergeben. Dieses Wissen ist entscheidend, um sicherzustellen, dass sich Unternehmen rechtzeitig auf den DSGVO-Stichtag (25. Mai 2018) vorbereiten können.

Neue Vorschriften verursachen Aufwand für viele Unternehmen

89 % der Befragten nannten mindestens einen Bereich in ihrem Unternehmen, auf den die DSGVO einen negativen Einfluss haben wird. Tatsächlich gaben 96 % derjenigen mit umfassendem Kenntnisstand bezüglich der DSGVO zusätzlichen Aufwand an – im Unterschied zu 33 % bei den weniger gut informierten. Unternehmen, die schlecht über die DSGVO informiert sind, werden über den zur Sicherstellung von Compliance erforderlichen Aufwand überrascht sein.

Der von den Befragten angegebene wahrscheinlichste Aufwand bezieht sich auf IT-Ressourcen und Arbeitszeit (60 %), die von der DSGVO belastet sein werden. Die IT-Abteilung hält dies für wahrscheinlicher als die Abteilung für Risiko und Compliance (66 % bzw. 30 %).

Auswirkungen sind auch für den Bereich Schulungsressourcen (38 %) und entsprechende Budgets (37 %) wahrscheinlich, aber 34 % der Befragten haben für eine DSGVO -Compliance von beidem nicht genug zur Verfügung.

USA und Großbritannien im Vergleich

Zwar handelt es sich um eine EU-Vorschrift, dennoch verfügte ein ähnlicher Anteil der Befragten in Großbritannien und den USA über umfassende Informationen über die DSGVO (45 % bzw. 46 %).

Die Befragten in Großbritannien sehen die DSGVO eher als Belastung für Ressourcen. 93 % der britischen Befragten gaben an, dass es einen gewissen Aufwand bedeutet, mit sich ändernden Anforderungen von allgemeinen Datenschutzvorschriften – und deren Relevanz – auf dem aktuellen Stand zu bleiben, in den USA waren es 87 %.

Vorbereiten für die DSGVO

Implementieren von Compliance-Plänen für die DSGVO

Befragte aus Unternehmen, die bereits einen vollständigen Compliance-Plan umgesetzt haben, geben an, dass es durchschnittlich drei Monate gedauert hat, den Plan auszuarbeiten, und im Schnitt weitere drei Monate, ihn zu implementieren. Auch wenn dies insgesamt nur sechs Monate sind, ist die Mehrheit (54 %) nicht vollständig überzeugt, dass allein das Testing innerhalb der zweijährigen Implementierungsperiode konform sein wird.

Die Befragten, die mit ihren Compliance-Plänen bereits begonnen haben (auch wenn sie noch nicht unbedingt abgeschlossen sind), geben an, dass sie bisher Teile der Pläne durchschnittlich drei Mal geändert haben. Dies kann dazu beitragen, dass es für 89 % einen gewissen Aufwand für das Unternehmen bedeutet, mit sich ändernden Anforderungen von allgemeinen Datenschutzvorschriften – und deren Relevanz – auf dem aktuellen Stand zu bleiben.

Unternehmen, die noch nicht mit der Ausarbeitung eines Compliance-Plans begonnen haben, müssen dies bald tun, um rechtzeitig zum Stichtag fertig zu sein.

Technologische Herausforderungen bei der DSGVO-Compliance

DSGVO-Compliance ist nicht leicht zu erreichen. 88 % der Befragten geben an, dass technologische Herausforderungen ein Compliance-Risiko darstellen. Mehr als die Hälfte (54 %) sagen, dass in ihrem Unternehmen vertrauliche Daten nicht einheitlich gespeichert werden.

Befragte in der IT-Abteilung (92 %) halten es für wahrscheinlicher, dass technologische Herausforderungen Compliance-Risiken darstellen, als Mitarbeiter in der Abteilung Risiko und Compliance (70 %). Unter Umständen kann die IT-Abteilung technologische Herausforderungen besser einschätzen, aber die Abteilung Risiko und Compliance sollte die Compliance-Risiken besser kennen. In jedem Fall erwartet die Mehrheit aus beiden Abteilungen Herausforderungen.

Technologische Herausforderungen stellen Compliance-Risiken dar

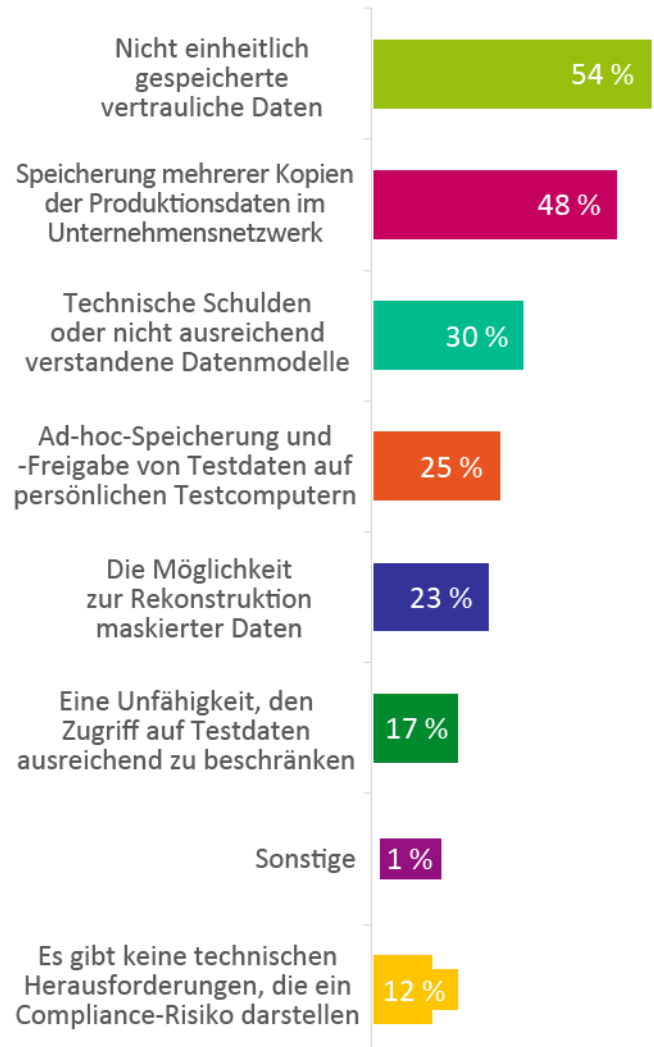


Abbildung 2: „Welche technologischen Herausforderungen können ein Compliance-Risiko für Ihr Unternehmen darstellen?“ Frage an alle 200 Befragten

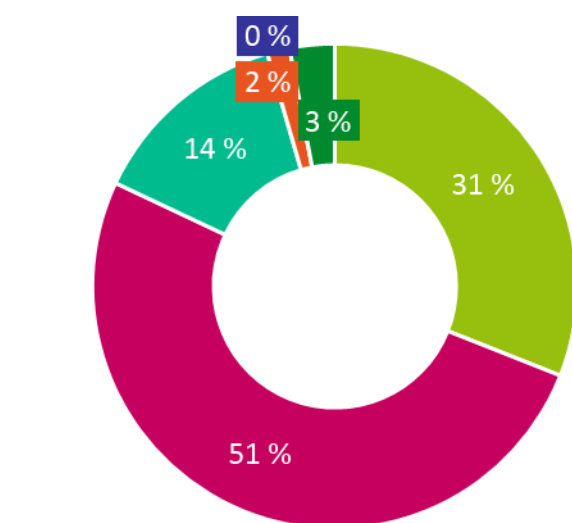
Ein hoher Prozentsatz der Befragten (88 %) gab an, dass technologische Herausforderungen ein Compliance-Risiko darstellen. Der Bereich, der die größten Herausforderungen mit sich bringt, ist das richtige Speichern vertraulicher Daten (54 %).

Aktuelle Hürden für die DSGVO-Compliance

Aktuelle Testing-Verfahren entsprechen nicht der Norm

Nur 31 % der Befragten geben an, dass die aktuellen Testing-Verfahren in ihrem Unternehmen im Hinblick auf Technologien, Prozesse und die Kultur der DSGVO entsprechen. In der Mehrzahl der Unternehmen ist für die DSGVO-Compliance noch viel Arbeit nötig. Und die muss in weniger als zwei Jahren erledigt sein.

Aktuelle Compliance



- Vollständige Compliance
- Überwiegende Compliance
- Erheblicher Verbesserungsbedarf
- Beträchtlicher Verbesserungsbedarf
- Technologie, Prozesse und Kultur müssen komplett erneuert werden
- Weiß nicht

Abbildung 3: „Was schätzen Sie, in welchem Umfang die aktuellen Testing-Verfahren Ihres Unternehmens im Hinblick auf Technologien, Prozesse und die Kultur der Datenschutz-Grundverordnung entsprechen.“ Frage an alle 200 Befragten

Weniger als die Hälfte der Befragten (46 %) ist sehr davon überzeugt, dass sie während der Implementierungsperiode Compliance erreichen. Dies legt nahe, dass die meisten Unternehmen Bedenken haben, ob sie den Stichtag 25. Mai 2018 halten können.

Befragte der Vorstandsebene (52 %) sind eher sehr davon überzeugt, dass ihr Unternehmen den Termin einhalten kann, als die erfahrenen Führungskräfte mit 40 %.

In der gesamten Studie unterscheiden sich die Ansichten der Vorstände und der erfahrenen Führungskräfte. Die Ursache könnte sein, dass letztere näher dran sind und die tatsächliche Situation besser kennen als die Vorstände, die möglicherweise eher ihre Hoffnungen zum Ausdruck bringen.

Compliance-Lücken in aktuellen Prozessen

Die Prozesse der meisten befragten Unternehmen sind mit der DSGVO nicht konform.

Nur ein Drittel (33 %) der Befragten ist wirklich überzeugt, dass alle Kundendaten umgehend (innerhalb von zehn Geschäftstagen) in allen Systemen und Anwendungen des Unternehmens ermittelt werden können. Die Mehrheit ist also nicht überzeugt, dass ihr Unternehmen derzeit dazu in der Lage ist. Es sind 42 % der Befragten aus dem Vorstand, die davon überzeugt sind, dass es in ihrem Unternehmen möglich ist, aber nur 25 % der erfahrenen Führungskräfte. Hoffen die Vorstände, dass sie bereits dazu in der Lage sind, oder wissen sie nur nicht, was es bedeutet?

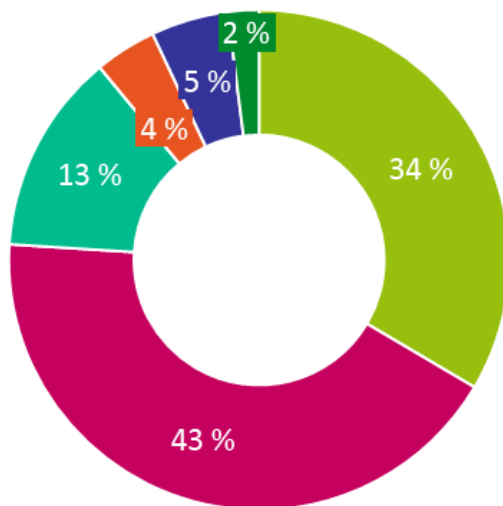
Nur 41 % geben an, dass aktuelle Prozesse und Technologien den Datenzugriff im durch die Vorschrift geforderten Umfang beschränken können. Dies bedeutet wiederum, dass die Mehrheit in diesem Bereich nicht auf die DSGVO vorbereitet ist. Die Vorstände scheinen eher anzunehmen, dass ihr Unternehmen in diesem Bereich bereits Compliance erreicht hat. Zumindest gibt die Hälfte (50 %) dies an, im Vergleich zu 31 % der erfahrenen Führungskräfte. Dies legt wiederum nahe, dass die Vorstände ein geschöntes Bild von den Vorbereitungen ihrer Unternehmen im Hinblick auf die DSGVO haben.

Löschen von Kundendaten „ohne Verzögerung“

Eines der Hauptmerkmale der DSGVO ist das „Recht auf Vergessenwerden“. Damit hat der Dateneinhaber (z. B. Kunden) das Recht, den Datenverwalter (z. B. Unternehmen) in bestimmten Situationen aufzufordern, seine persönlichen Daten zu löschen.

Nur etwa ein Drittel (34 %) der Befragten ist überzeugt, dass ihr Unternehmen jedes Vorkommen von Kundendaten (auch Testdaten) ohne Verzögerung löschen kann, wenn ein Kunde dies wünscht. Weitere 43 % sind zuversichtlich, denken aber nicht, dass wirklich alle Daten abgedeckt werden. Und das wäre ein Verstoß gegen die Vorschrift. Auch hier müssen die meisten Unternehmen noch Maßnahmen ergreifen, um DSGVO-Compliance zu erreichen.

Löschen von Daten



- Vollständig überzeugt
- Zuversichtlich, dass wir schnell genug wären, aber nicht überzeugt, dass wir alle Daten abdecken
- Zuversichtlich, dass wir es könnten – aber nicht schnell genug
- Zuversichtlich, dass es möglich wäre – es sind aber mehr Informationen nötig
- Nicht überzeugt
- Weiß nicht

Abbildung 4: „Wenn ein Kunde beantragt, dass jedes Vorkommen persönlicher Daten (auch Testdaten) „ohne Verzögerung“ gelöscht wird, wie zuversichtlich sind Sie, dass Ihr Unternehmen dem gegenwärtig nachkommen kann?“ Frage an alle 200 Befragten

Ermöglichen des Zugriffs von Kunden auf ihre Daten

Ein weiteres Hauptmerkmal der DSGVO ist das „Recht auf Datenportabilität“: Dateneinhaber sollen in der Lage sein, ihre persönlichen Daten zwischen Service Providern zu übertragen, und Unternehmen müssen dies ermöglichen.

Wenn ein Kunde Zugriff auf jedes Vorkommen seiner Daten in einem Format fordert, das er nutzen und in andere Formate übertragen kann, geben nur 43 % der Befragten an, dass ihr Unternehmen dies gegenwärtig vollständig gewährleisten kann. Ein ähnlicher Anteil (44 %) ist dazu in der Lage, aber nur in ein oder zwei Formaten, die möglicherweise vom Kunden nicht gewünscht oder für ihn nicht lesbar sind. Weitere 10 % haben derzeit keine entsprechenden Möglichkeiten. Wieder wird offensichtlich, dass Unternehmen ihre Arbeitsweise ändern müssen, um die DSGVO einzuhalten.

USA und Großbritannien im Vergleich

Die Befragten in den USA sind eher überzeugt, dass ihr Unternehmen rechtzeitig bereit ist und dass sie Compliance bereits erreicht haben, als die britischen Befragten. Für die Befragten in den USA gilt:

- Sie sind eher überzeugt, dass das Testing innerhalb der zweijährigen Implementierungsperiode konform sein wird – 49 % in den USA verglichen mit 41 % in Großbritannien.
- Sie sind überzeugt, dass der gesamte Inhalt unverzüglich (innerhalb von zehn Geschäftstagen) in allen Systemen und Anwendungen des Unternehmens ermittelt werden kann – 38 % in den USA verglichen mit 24 % in Großbritannien.
- Sie haben den Datenzugriff ausreichend differenziert beschränkt – dies geben 44 % in den USA an, verglichen mit 35 % in Großbritannien.
- Sie sind überzeugt, dass sie jedes Vorkommen persönlicher Daten (auch Testdaten) gegenwärtig „ohne Verzögerung“ löschen können – 36 % in den USA meinen das, verglichen mit 29 % in Großbritannien.
- Sie können Daten in einem Format bereitstellen, das für Kunden nutzbar und in andere Formate übertragbar ist – 47 % der Befragten in den USA sagen das, verglichen mit 36 % in Großbritannien.

Technologien zur Unterstützung der DSGVO-Compliance

Notwendigkeit von Investitionen in Technologien

88 % der Befragten ist bewusst, dass ihr Unternehmen in weitere Technologien investieren muss, um DSGVO-Compliance zu erreichen. Sie planen Investitionen in verschiedenen Bereichen, darunter Verschlüsselungstechnologien (58 %), Analyse- und Reporting-Technologien (49 %) und Testdatenmanagement (47 %).

39 % der Befragten aus Vorständen schätzen, dass beträchtliche Investitionen erforderlich sein werden, aber nur weniger als die Hälfte dieses Anteils (16 %) der erfahrenen Führungskräfte denken, dass dies für ihr Unternehmen zutrifft. Dies ist überraschend, da die Befragten der Vorstandsebene eher annehmen, dass ihr Unternehmen in verschiedenen Bereichen bereits Compliance erreicht hat.

Technologien zur Förderung von Compliance in Testumgebungen

In vielen Unternehmen gibt es Verfahren (grün in der Abbildung 5 unten) oder sind Verfahren geplant (pink, unten), um Compliance in Testumgebungen sicherzustellen. Auch wenn einige Unternehmen noch keine entsprechenden Pläne haben, ist es ermutigend, dass die meisten in dieser Gruppe wissen, dass sie etwas unternehmen müssen (blau gegenüber orange).

Zwar haben viele einige dieser Verfahren bereits implementiert, es darf aber nicht vergessen werden, dass 88 % angegeben haben, technologische Herausforderungen würden ein Compliance-Risiko darstellen (Abbildung 3), und mehr als die Hälfte speichert vertrauliche Daten im Unternehmen nicht einheitlich.

Sicherstellen von Compliance in Testumgebungen

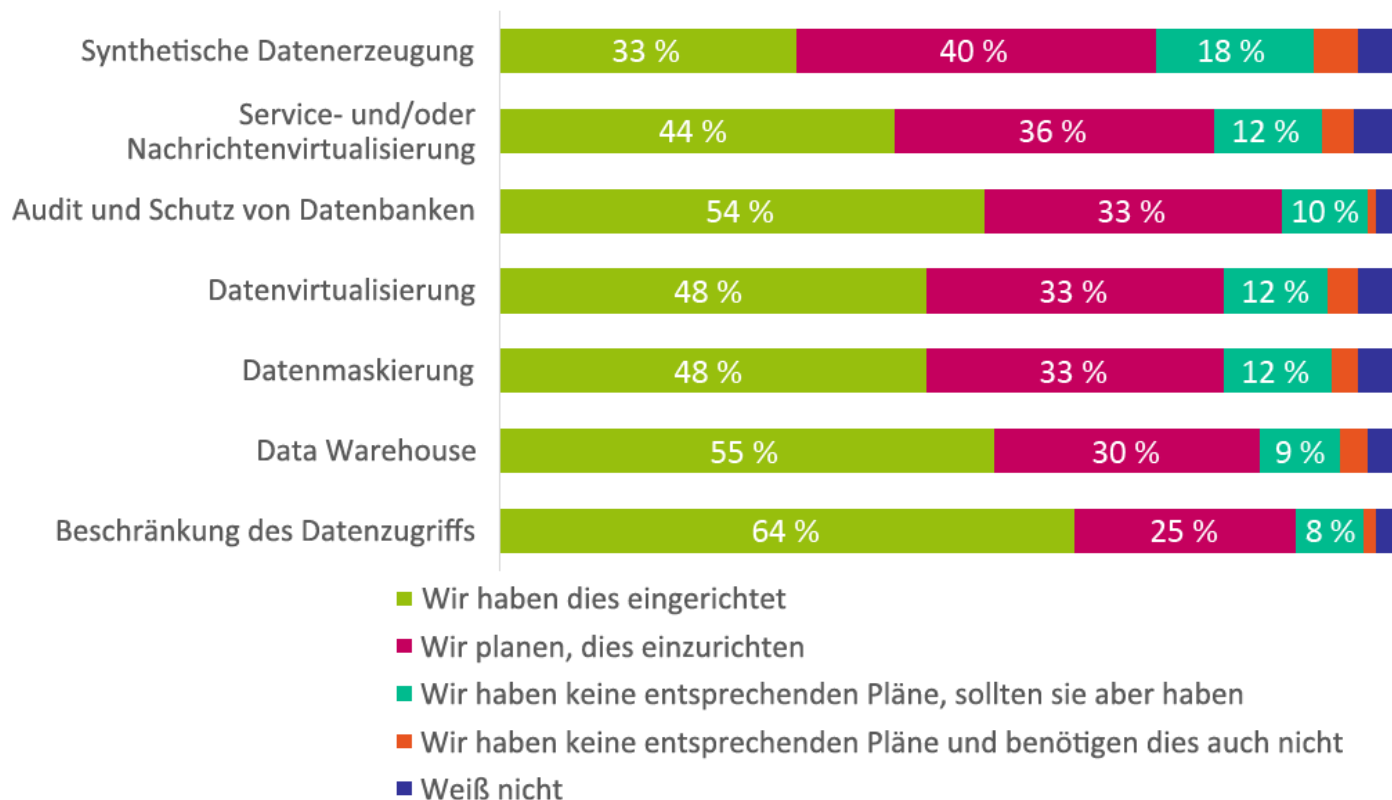


Abbildung 5: „Welche aktuellen Verfahren sind implementiert/halten Sie in Ihrem Unternehmen für erforderlich, um Compliance von Testumgebungen sicherzustellen?“ Frage an alle 200 Befragten

Nutzung synthetisch erzeugter Daten

Nur in 19 % der Unternehmen von Befragten werden synthetisch erzeugte Daten genutzt (ohne zusätzliche Nutzung maskierter Daten), aber weitere 18 % geben an, dass die DSGVO zu deren Einführung Anlass geben könnte.

Eine Mischung aus Datenmaskierung und synthetischen Daten ist die gängigste Lösung für DSGVO-Compliance.

58 % der Befragten sagen, dass ihr Unternehmen eine Kombination aus Datenmaskierung und synthetischer Datenerzeugung implementieren wird, um DSGVO-Compliance im Zusammenhang mit der Verwendung persönlicher Informationen nachzuweisen.

Die Befragten der Vorstände (65 %) denken eher, dass ihre Unternehmen die Implementierung einer Kombination aus Datenmaskierung und synthetischer Datenerzeugung als Beleg für Compliance planen. Bei den erfahrenen Führungskräften ist es nur etwas über die Hälfte (51 %), die angibt, ihre Unternehmen würden dies planen.

Allerdings sagen 7 % der Befragten, dass im Hinblick auf Maßnahmen ihres Unternehmens für die Compliance keine Entscheidungen oder Gespräche erfolgt sind. Die Unternehmen müssen mit der Planung beginnen, um vor dem Stichtag Compliance sicherzustellen.

Pseudonymisierung

Definition: Die Verarbeitung persönlicher Daten auf eine solche Art und Weise, dass die Daten ohne die Nutzung zusätzlicher Informationen keinem bestimmten Dateninhaber mehr zugeordnet werden können, solange solche zusätzlichen Informationen gesondert und unter Zuhilfenahme technischer und organisatorischer Maßnahmen aufbewahrt werden, um sicherzustellen, dass sie keiner identifizierten oder identifizierbaren Person zugeschrieben werden können.

Von den Unternehmen, die gegenwärtig Daten maskieren, sind sich 13 % nicht bewusst, dass die Prozesse des Unternehmens im Hinblick auf die DSGVO überprüft werden müssen. Nur 39 % gehen davon aus, dass die aktuellen Prozesse und Technologien für die Pseudonymisierung den Standards entsprechen. Auch hier müssen die meisten Unternehmen noch Maßnahmen ergreifen, um DSGVO-Compliance sicherzustellen.

Wieder denken die Befragten der Vorstände (46 %) eher, dass ihr Unternehmen in diesem Bereich bereits Compliance erreicht hat, verglichen mit 31 % der erfahrenen Führungskräfte, die dies annehmen.

Diejenigen mit einem besseren DSGVO-Informationsstand geben eher an, dass ihr Unternehmen gegenwärtig den Standards entspricht. In diesen Unternehmen wurden möglicherweise schon Maßnahmen zur Sicherstellung von Compliance ergriffen.

USA und Großbritannien im Vergleich

Befragte in den USA stimmen eher zu, dass beträchtliche Investitionen erforderlich sein werden (31 % derjenigen in den USA verglichen mit 20 % in Großbritannien).

Allerdings werden 15 % der Befragten in Großbritannien von der Datenmaskierung auf synthetische Datenerzeugung umstellen, um die Verwendung von Produktionsdaten zu vermeiden, verglichen mit 7 % in den USA.

Fazit

In Anbetracht der Tatsache, dass die DSGVO erst kürzlich formal angekündigt wurde, gibt es bereits einen recht ordentlichen Kenntnisstand unter den Befragten. Nachdem sie über die Vorschrift informiert wurden, haben 88 % angegeben, dass es für ihr Unternehmen technologische Herausforderungen bedeutet, DSGVO-konform zu werden. Es wird anerkannt, dass zur Einhaltung der DSGVO viel Arbeit nötig sein wird.

Viele der Befragten haben aktuell Lücken bei der DSGVO-Compliance in ihrem Unternehmen aufgezeigt. Unter Berücksichtigung der Erkenntnis, dass es technologische Herausforderungen gibt, ist es keine Überraschung, dass 88 % in Technologien investieren müssen, um die DSGVO einzuhalten. In Verschlüsselungstechnologien werden 58 % investieren, und ein beträchtlicher Anteil ist der Meinung, dass die DSGVO ausschlaggebend dafür sein kann, andere Technologien wie die synthetische Datenerzeugung innerhalb einer Lösung für das Testdatenmanagement einzuführen (18 %).

Neue Anforderungen durch die DSGVO bedeuten Aufwand für die Unternehmen der Befragten. Vorbereitungen werden bei einigen bereits getroffen, es bleibt aber noch viel zu tun. Die Planung und Implementierung für die DSGVO (plus Überarbeitung) dauert sechs Monate. Wenn Unternehmen nicht bald damit beginnen, einen Compliance-Plan aufzustellen, können sie vor dem Stichtag im Mai 2018 in Zeitnot geraten.

Eine Einarbeitung in die neue Vorschrift selbst ist notwendig, ebenso wie die erforderliche Unterstützung bei Technologien. Wie immer sind es nur wenige, die von den Prozessen ihres Unternehmens überzeugt sind oder angeben, dass ihr Unternehmen mit Elementen der DSGVO bereits konform ist. Nur 31 % halten ihr Unternehmen im Hinblick auf aktuelle Testing-Verfahren für vollständig konform. 39 % denken, dass die aktuellen Richtlinien für die Pseudonymisierung den Standards entsprechen. In der Mehrzahl der Unternehmen ist zur Sicherstellung von Compliance noch Arbeit nötig.

Auch wenn die DSGVO eine europäische Vorschrift ist, bereiten sich US-Unternehmen auf die Auswirkungen vor. Die Vorschrift betrifft Unternehmen weltweit. Daher ist es nicht verwunderlich, dass 31 % der Befragten in den USA zustimmen, beträchtliche Investitionen in Technologien wären zur Förderung der DSGVO-Compliance erforderlich.

Alle Unternehmen sollten Pläne für die DSGVO-Compliance umsetzen, bevor es zu spät ist.

Wenn Sie mehr über die DSGVO und die Maßnahmen, die Ihr Unternehmen ergreifen sollte, erfahren möchten, sehen Sie sich den Webcast von CA Technologies und Vanson Bourne an:

[„Are You GDPR Ready? Get the Vanson Bourne Readiness Survey Results“](#)



Informationen zu CA Technologies:

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht im Mittelpunkt jedes Unternehmens in allen Branchen. Ob Planung, Entwicklung, Management oder Security – CA Technologies arbeitet weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen abwickeln und kommunizieren, in mobilen, privaten und öffentlichen Cloud-Umgebungen oder in verteilten Systemen und Mainframe-Umgebungen neu zu gestalten. Weitere Informationen finden Sie unter ca.com/de.

CS200-215379

Informationen über Vanson Bourne:

Vanson Bourne ist ein unabhängiger Spezialist für Marktforschung für den Technologiesektor. Strenge Forschungsprinzipien und unsere Fähigkeit, die Meinungen von erfahrenen Entscheidungsträgern in technischen und geschäftlichen Funktionen in allen Branchen und den wichtigsten Märkten abzufragen, bilden das Fundament unseres Rufs für zuverlässige und glaubwürdige forschungsbasierte Analysen. Weitere Informationen finden Sie unter www.vansonbourne.com
