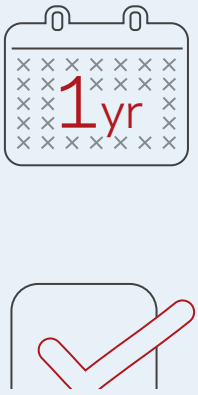
2017 VERITAS GDPR REPORT

Kapitel 2: Das Gefühl täuscht – nur ein Bruchteil aller Unternehmen ist bereit für die DSGVO

VERITAS™

The truth in information.



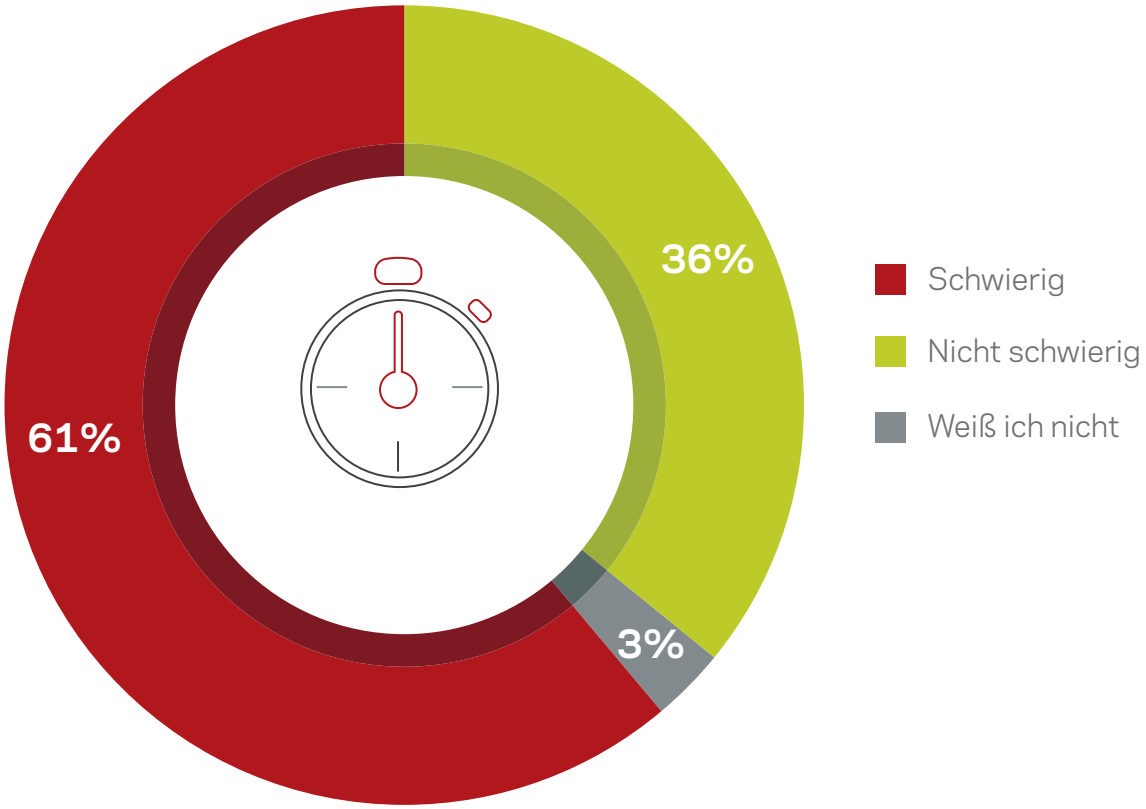
Die Uhr tickt - viel Zeit bleibt Unternehmen bis zum Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) nicht mehr. Umso erstaunlicher ist, dass nur 31 Prozent der Befragten in einer Veritas-Studie angaben, dass ihre Firma bereits konform zu den neuen Regelungen handelt. Bei genauerer Analyse zeigt sich: Der Großteil aus der Gruppe, die sich als gut vorbereitet oder „compliant“ einstuft, wiegt sich in falscher Sicherheit. Denn nur zwei Prozent der befragten Unternehmen sind tatsächlich dafür gewappnet, die Forderungen der Richtlinie zu erfüllen. Alle anderen aus dieser Gruppe haben in vielen Kernaufgaben noch erheblichen Nachholbedarf.

Wo liegen Unternehmen falsch?

Die DSGVO stellt Firmen vor eine Reihe von Pflichtaufgaben, eine der wichtigsten: Sobald es ein Datenleck gibt, müssen Firmen es unmittelbar erkennen und neben den Behörden auch diejenigen informieren, deren persönliche Daten vom Vorfall betroffen sind. Dazu sind entsprechende technologische und organisatorische Maßnahmen nötig. Aber 48 Prozent der Befragten, die ihre Firma als gut vorbereitet einstuften, gaben zugleich zu, keinen Überblick über Vorfälle zu haben, bei denen personenbezogenen Daten verloren gehen.

Wie können Firmen ohne Überblick das Mandat aus der Richtlinie erfüllen und Betroffene innerhalb von 72 Stunden informieren? Sie werden daran scheitern. Mehr als 60 Prozent der Befragten geben auch zu, dass die zeitliche Frist von 72 Stunden für sie zu knapp bemessen ist, um Datenlecks zu finden und zu melden. Wer hierbei scheitert, verstößt gegen eine der wichtigsten Forderungen der Richtlinie. Bei solch gravierenden Regelverstößen betragen die Strafen bis zu vier Prozent des Jahresumsatzes oder bis zu 20 Millionen Euro – je nachdem, welcher Betrag höher ist.

Wie schwierig ist es für Ihr Unternehmen, ein Datenleck binnen 72 Stunden zu identifizieren und zu melden?



Grafik 1: "Wie schwierig ist es für Ihr Unternehmen, ein Datenleck binnen 72 Stunden zu identifizieren und zu melden?" Angaben der 279 Befragten, die ihr Unternehmen als bereits GDPR- compliant eingestuft haben

Ehemalige Mitarbeiter: Die innere Gefahr

Sobald ein Mitarbeiter die Firma verlässt, sollten idealerweise alle seine Zugriffsprivilegien auf Unternehmensdaten erlöschen. Im Idealfall werden seine Zugänge beschränkt, sobald seine Kündigung eingegangen ist. Die Hälfte der Studienteilnehmer räumt jedoch ein, dass ehemalige Kollegen noch immer auf Firmendaten zugreifen können.

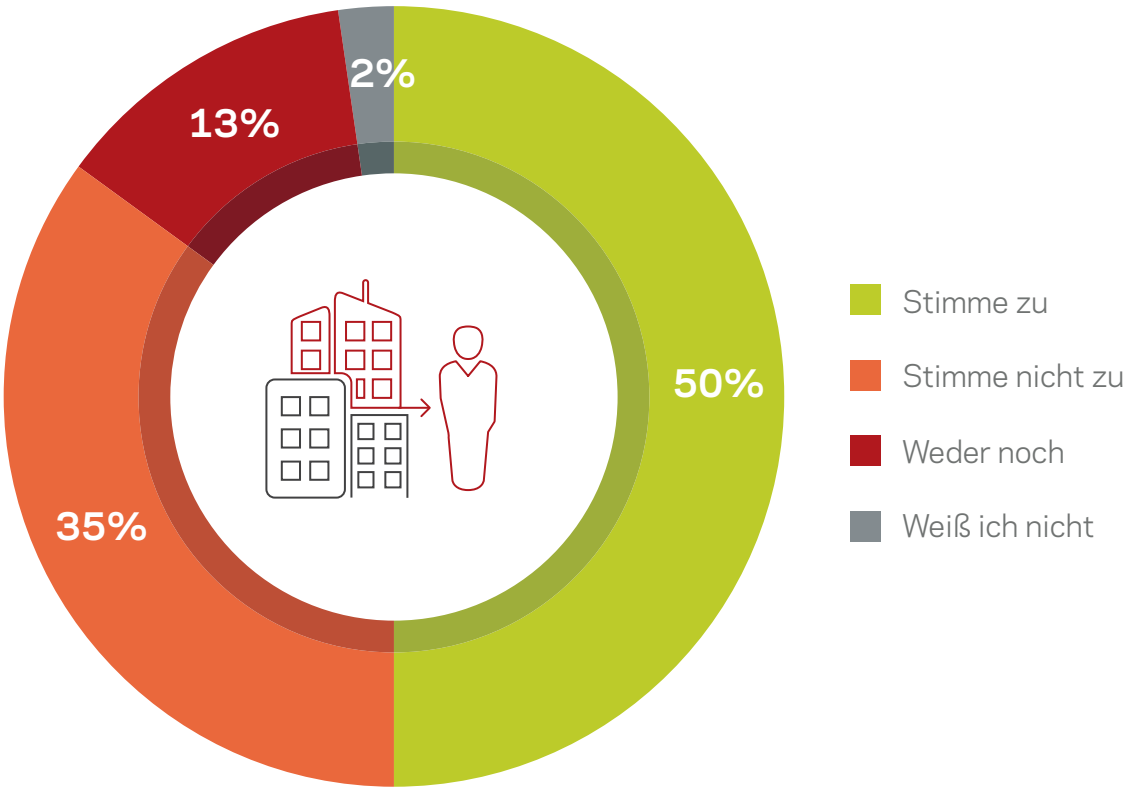
Wegen dieser Form des unkontrollierten Zugriffs riskieren Unternehmen, dass ein Ex-Mitarbeiter ihr Netz ungehindert betreten kann. Außerdem schaffen sie die Basis dafür, dass vertrauliche Informationen in die Hände von Unbefugten geraten können. Beide Szenarien verstoßen eindeutig gegen die Regelungen der DSGVO. Auch die Mitarbeiter können ein Risiko sein, sollten ihre Zugänge nicht klar geregelt sein. Immerhin geben rund 60 Prozent der Befragten in der Studie an, dass ihr Unternehmen die internen Zugriffe auf personenbezogene Daten nicht vollständig überblicken und sie so dieses Risiko nur unvollständig bewerten können.

Mag auch die Gefahr gering sein, die von den eigenen Mitarbeitern ausgeht, anders liegt der Fall bei ehemaligem Personal. Ihre Zugriffsprivilegien auf Firmendaten sollten in dem Moment erlöschen, in dem sie die Firma verlassen - und eingeschränkt werden, sobald sie ihre Kündigung einreichen.

Schuldfrage: Wer ist zuständig für Daten in der Cloud?

Immer mehr Unternehmen legen Daten in der Cloud ab. Dabei nutzt ein Großteil, ganze 94 Prozent der befragten Verantwortlichen, so genannte Hybrid-Cloud-Strukturen, in denen Daten sowohl on-premise als auch in einer Public- oder Private-Cloud-Umgebung gelagert sind. Auch in dieser Struktur müssen Unternehmen sämtliche DSGVO-Auflagen erfüllen - auch bei allen in der Cloud gespeicherten Informationen. Nur denkt die Hälfte der Befragten (49 Prozent), dass ihr Cloud Service Provider (CSP) für die Compliance in der Cloud verantwortlich sei. Eine falsche Annahme, denn Unternehmen sind als so genannte Data Controller juristisch genauso in der Pflicht wie der Data Processor, in dem Fall der Cloud-Dienstleister. Beide sind

Ehemalige Mitarbeiter meines Unternehmens können noch auf Unternehmensdaten zugreifen



Grafik 2: "In welchem Ausmaß stimmen Sie den folgenden Aussagen zu? Ehemalige Mitarbeiter meines Unternehmens können auf Unternehmensdaten zugreifen" Angaben der 279 Befragten, die ihr Unternehmen als bereits GDPR- compliant eingestuft haben

also dafür verantwortlich, die DSGVO technisch und organisatorisch zu erfüllen. Diese falsche Annahme könnte Firmen Millionen kosten und ihre Marke schädigen, sobald ernste Vorfälle auftreten.

Alltagsbürde: das „Recht auf Vergessenwerden“

Im Januar wird eine EU-Kampagne die Bürger über ihre neuen Rechte unter der DSGVO aufklären. Es ist wahrscheinlich, dass mehr Kunden danach fragen werden, ihre personenbezogenen Daten zu löschen. Ihre Daten liegen wahrscheinlich in einer strukturierten gepflegten Datenbank, könnten zugleich aber an anderer Stelle repliziert, in einer Excel erfasst und auf einem Rechner eines Mitarbeiters gespeichert sein. Fast 20 Prozent der Befragten bekennen, dass ihr Unternehmen nicht in der Lage sei, Datenbestände zu löschen oder zu säubern. Viele von ihnen haben weder eine Suchfunktion installiert oder wissen, wo Informationen gespeichert sind. Zudem klassifizieren Firmen ihre Daten nicht klar genug.

Rund 13 Prozent der Befragten, die angeblich schon DSGVO-compliant sind, gaben in der Umfrage auch an, dass ihr Unternehmen...

- **...nicht in der Lage sei, personenbezogene Daten effektiv zu suchen oder zu analysieren und auch explizite sowie implizierte Referenzen zu einer Person aufzuspüren.**
- **...keine akkurate Übersicht über alle Speicherorte seiner Daten hat.**
- **...die Speicherorte für Daten und ihre -quellen nicht klar definiert hat.**

Viele Unternehmen werden es daher schwer haben, ad hoc Kundendaten zu suchen, zu finden und zu löschen, sollten Kunden das „Recht auf Vergessenwerden“ in Anspruch nehmen. Auf diese Weise riskieren sie, gegen eine der Hauptforderungen in der neuen DSGVO zu verstoßen. Schließlich müssen sie nicht nur sicherstellen, personenbezogene Daten zu löschen. Sie sind zugleich angehalten, personenbezogene Daten dem vorher klar definierten Zweck entsprechend zu erfassen und zu bearbeiten.

So zeigt sich, dass Unternehmen noch an vielen Stellen nachjustieren müssen, damit sie DSGVO-compliant werden. Der Umgang mit Datenlecks, die Daten und Zugriffe ehemaliger Mitarbeiter, Datenspeicher in der Cloud und die große Alltagsfrage, wie das Recht auf Vergessenwerden umzusetzen ist – dies sind nur einige Aspekte, auf die sich Unternehmen auf ihrem Weg zur Einhaltung der DSGVO konzentrieren sollten – denn viel Zeit bleibt bis zum Inkrafttreten nicht mehr.

Informationen darüber, wie Veritas Ihrem Unternehmen helfen kann, DSGVO-compliant zu werden, finden Sie unter:
veritas.com/gdpr

Methodik

Veritas hat den unabhängigen Marktforscher Vanson Bourne beauftragt, die Studie durchzuführen. Im Februar und März 2017 wurden dazu 900 Führungskräfte aus Australien, Deutschland, Frankreich, Japan, Singapur, Südkorea, den USA und dem Vereinigten Königreich interviewt. Die Befragten kamen aus Unternehmen mit mindestens 1000 Mitarbeitern aus verschiedenen Sektoren. Ein Kriterium war, dass die Organisation geschäftliche Beziehungen im EU-Raum unterhält.

Die Befragung wurde online durchgeführt. Um sicherzustellen, dass nur passende Kandidaten teilnehmen, wurde ein Multi-Level-Screening gewählt.

VERITAS™

The truth in information.