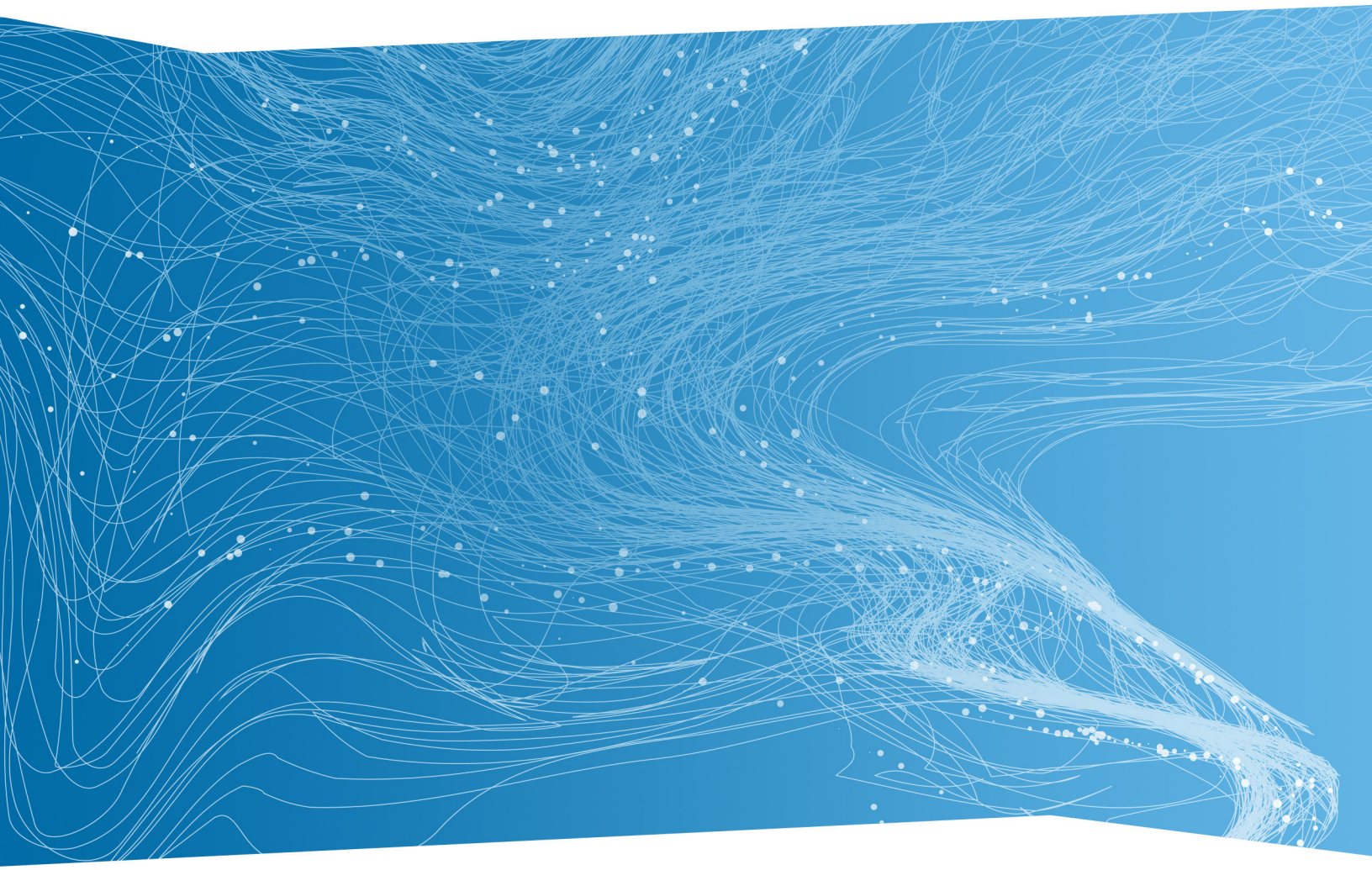
RSA



WHITEPAPER

DSGVO-ÜBERLEBENSSTRATEGIEN: 5 WEGE ZUR VORBEREITUNG

RSA

Unternehmen auf der ganzen Welt blicken sorgenvoll auf die künftige Umsetzung der Datenschutz-Grundverordnung (DSGVO), die das Potenzial für einen gewaltigen Umbruch mit sich bringt. Diejenigen, die die Vorbereitung für diese monumentale Verschiebung darin, wie personenbezogene Daten erhoben, gespeichert und geschützt werden, nicht zur Priorität erhoben haben – was laut einer PwC-Umfrage[1] auf ca. die Hälfte der multinationalen US-Unternehmen zutrifft –, sehen sich einer sehr realen Gefahr von Schäden gegenüber, wenn die DSGVO am 25. Mai 2018 in Kraft tritt. Potenzielle Geldstrafen für Verstöße können eine Höhe von mehreren Millionen Euro erreichen, sodass diese finanziellen Einbußen für manche Unternehmen sogar das Ende bedeuten könnten. Noch haben sie Zeit, sich vorzubereiten, aber da nur noch einige Monate zur Verfügung stehen, ist es wichtig, schnell zu handeln. In diesem Whitepaper werden fünf grundlegende Schritte beschrieben, die Unternehmen dabei helfen können, ein Framework für das DSGVO-Risikomanagement einzurichten.

1. WISSEN, WAS KOMMT

Es mag selbstverständlich klingen, aber der erste Schritt in der Vorbereitung auf die DSGVO ist es, ein klares Bewusstsein und Verständnis der Verordnung und ihrer Anforderungen zu entwickeln, insbesondere im Hinblick darauf, wie sich diese Anforderungen in Ihrem Unternehmen auswirken. Kurz gesagt: Die DSGVO (1) gilt für alle Unternehmen, die personenbezogene Daten von Bürgern der EU verarbeiten, unabhängig davon, ob diese Unternehmen in der EU ansässig sind, und (2) erfordert Datenschutzkontrollen, die rund um Prozesse für die Erfassung, die Speicherung und den Schutz von Daten implementiert werden. Was bedeutet das genau? Es führt kein Weg daran vorbei: Die einzige Möglichkeit, die Auswirkungen für Ihr Unternehmen vollständig zu erfassen, ist, die Verordnung selbst (ja, alle 99 Artikel) im Detail, vorzugsweise mit Unterstützung durch rechtliche und behördliche Experten, zu überprüfen.

2. UNTERSUCHEN DER AKTUELLEN BEDINGUNGEN

Bevor Sie DSGVO-Anforderungen für den Umgang mit personenbezogenen Daten erfüllen können, müssen Sie wissen, was Sie zu tun haben – welche Daten in Ihrem Unternehmen dem Schutz durch die DSGVO unterliegen, wo sie gespeichert sind und wie sie genutzt werden. Das klingt nicht nur nach einer Menge Arbeit, das ist es auch. Und der Prozess wird noch schwieriger durch die Tatsache, dass Daten heute genauso häufig in der Cloud wie in einem Rechenzentrum vor Ort gespeichert werden. Automatisierte Tools können zwar dabei helfen, die Herausforderung der genauen Identifizierung der Art und Menge der Daten in der IT-Infrastruktur zu meistern, es hängt jedoch viel von den Data-Governance-Prozessen ab, die Sie implementieren, unabhängig davon, ob die Daten vor Ort oder in der Cloud gespeichert werden.

3. ÜBERPRÜFEN DES BEREITSCHAFTSSTATUS

Sobald eine vollständige Inventarisierung der Daten, die durch das Unternehmen fließen, durchgeführt wurde, ist es Zeit, sich um die Art und Weise zu kümmern, wie personenbezogene Daten bereits geschützt werden. In den meisten Unternehmen werden wahrscheinlich Maßnahmen zum Schutz von Daten getroffen, z. B. Verschlüsselungsverfahren, und diese Maßnahmen spielen möglicherweise eine wichtige Rolle bei der Erfüllung einiger DSGVO-Anforderungen für den Schutz der Daten, die im Unternehmen gesammelt und gespeichert werden. Andere bestehende Maßnahmen zum Schutz von Daten, die Unternehmen bereits eingeleitet haben dürften, beinhalten Bewertungen der Auswirkungen des Datenschutzes, formale Data-Governance-Policies sowie Datenbackup- und -aufbewahrungs-Policies und -Tools.

[1] PwC GDPR Preparedness Pulse Survey, Dezember 2016

4. MANAGEN VON DRITTANBIETER-RISIKEN

Jedes Unternehmen, das in der Public Cloud arbeitet – ob ganz oder teilweise – oder das Beziehungen zu Lieferanten und Auftragnehmern unterhält, die die gemeinsame Nutzung von Daten beinhalten, findet sein DSGVO-Risiko erschwert durch das Vorhandensein von Drittanbietern. Das Dokumentieren von Drittanbieterengagement, die Bewertung des Risikos, das die Drittanbieter darstellen, und die Optimierung von Drittanbieter-Governance sind alles wichtige und notwendige Aspekte des DSGVO-Risikomanagements.

5. BEREITSEIN FÜR SCHNELLES HANDELN

Eine Schlüsselanforderung der DSGVO ist die 72-Stunden-Berichterstattungsregel bei Verstößen, die besagt, dass jede Datenschutzverletzung innerhalb von 72 Stunden gemeldet werden muss, nachdem der Verstoß dem Unternehmen bekannt wurde. Um möglichst schnell handeln zu können, wenn das Gesetz in Kraft tritt, muss bereits jetzt eine effektive Planung erfolgen. Das bedeutet, darüber nachzudenken, welche Fähigkeiten vorhanden sind, um den Umfang und die Auswirkungen eines Verstoßes innerhalb von 72 Stunden zu bestimmen. Dies ist besonders wichtig angesichts der Tatsache, dass man heute davon ausgeht, dass Verstöße innerhalb von Minuten passieren können, jedoch oft erst nach Monaten entdeckt werden.[2]

In den noch verbleibenden Monaten, bevor die DSGVO in Kraft tritt, können Unternehmen viel tun, um Pläne und Vorbereitungen zu treffen, damit die Auswirkungen auf den Betrieb minimiert werden. Hier erfahren Sie, wie RSA Archer bei der Umsetzung von DSGVO-Governance, -Risiko- und -Compliancelösungen in Ihrem Unternehmen helfen kann: rsa.com/gdpr.

INFORMATIONEN ÜBER RSA

RSA bietet Business-Driven Security™-Lösungen, die den Geschäftskontext auf einzigartige Weise mit Sicherheits-Incidents in Verbindung bringen, um Unternehmen dabei zu unterstützen, Risiken zu managen und die wichtigsten Ressourcen zu schützen. RSA-Lösungen sollen Unternehmen die effektive Erkennung und Abwehr erweiterter Angriffe, die Verwaltung von Benutzeridentitäten und -zugriffen sowie die Verringerung von Geschäftsrisiken, Betrug und Cyberkriminalität ermöglichen. RSA schützt Millionen von Benutzern auf der ganzen Welt und unterstützt mehr als 90 % der Fortune 500-Unternehmen dabei, in einer unsicheren und hochriskanten Welt erfolgreich zu sein. Weitere Informationen finden Sie unter rsa.com.

[2] Verizon Data Breach Investigations Report 2017

RSA

Inhalt und Haftungsausschluss

Dieses Whitepaper dient nur für allgemeine Informationszwecke und sollte nicht als Ersatz für eine Beratung durch professionelle Berater verwendet werden. Die Erwähnung von RSA-Produkten oder -Services erfolgt nur zu Informationszwecken. RSA Security LLC, EMC Corporation, Dell, Inc. und ihre Tochtergesellschaften (kollektiv „RSA") übernehmen keine ausdrückliche oder implizierte Haftung in Bezug auf die Richtigkeit und Vollständigkeit der enthaltenen Informationen. RSA ist nicht für in diesem Whitepaper enthaltene Fehler oder Auslassungen verantwortlich und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen vorzunehmen. Durch dieses Whitepaper entstehen keine vertraglichen Verpflichtungen, weder direkt noch indirekt. Sämtliche in diesem Whitepaper bereitgestellten Informationen zu RSA und Drittanbietern werden ohne Gewähr zur Verfügung gestellt. RSA SCHLIESST JEGLICHE AUSDRÜCKLICHE ODER IMPLIZITE HAFTUNG AUS, DIES BEZIEHT SICH AUF JEGLICHE INFORMATIONEN (EINSCHLIESSLICH SOFTWARE, PRODUKTE ODER SERVICES), DIE DURCH DIESES WHITEPAPER ZUR VERFÜGUNG GESTELLT WERDEN, EINSCHLIESSLICH DER IMPLIZITEN GARANTIEN DER ALLGEMEINEN GEBRAUCHSTAUGLICHKEIT UND TAUGLICHKEIT FÜR EINEN BESTIMMTEN ZWECK UND NICHTVERLETZUNG VON RECHTEN. In manchen Ländern ist der Ausschluss der Haftung für Garantien nicht zulässig. Die oben stehenden Ausschlussklauseln treffen daher unter Umständen nicht auf Sie zu. RSA übernimmt keinerlei Haftung für Schäden und leistet auch keinen Schadensersatz für direkte, spezielle, indirekte, zufällige oder Folgeschäden oder Schäden durch entgangene Gewinne, entgangene Einnahmen oder Verlust der Verwendbarkeit, Kosten für Ersatzprodukte, Verlust oder Beschädigung von Daten im Zusammenhang mit der Nutzung oder Unmöglichkeit der Nutzung der RSA-Websites, Produkte oder Services von RSA. Hierzu zählen Schäden, die aus der Nutzung der oder dem Vertrauen auf die Dokumente oder Informationen in diesem Whitepaper hervorgehen, auch wenn RSA von der Möglichkeit solcher Schäden unterrichtet wurde. Dieses Whitepaper darf ohne eine vorherige schriftliche Zustimmung durch RSA nicht vervielfältigt werden.