Gerüstet für die DSGVO

Cybersicherheit für Datenschutz

Ein Service von:

GERÜSTET FÜR DIE DSGVO
Datenschutz-Grundverordnung

Was ist die DSGVO?

Das Thema Datenschutz nimmt einen immer höheren Stellenwert ein. Das belegt auch die neue **Datenschutz-Grundverordnung (DSGVO)** der Europäischen Union. Hauptziel der Verordnung ist es, dass Anwender die Kontrolle über ihre personenbezogenen Daten zurückerlangen, anstatt diese den damit hantierenden Unternehmen oder Dienstanbietern zu überlassen. Doch obwohl die DSGVO in nicht allzu ferner Zukunft in Kraft tritt, sind viele Unternehmen noch nicht ausreichend auf die Einhaltung der strengeren Auflagen in Hinblick auf die Nutzung, Übermittlung und Speicherung von Kundendaten vorbereitet. Wir stellen Ihnen die DSGVO nachfolgend vor und erläutern, was diese für Ihre Cloudstrategie bedeutet.

Überblick

Der Schutz personenbezogener Daten steht in der Europäischen Union (EU) bereits seit 20 Jahren auf der Agenda. Mit der kürzlich ratifizierten DSGVO beginnt nun jedoch ein neues Zeitalter. Die Verordnung enthält gesetzliche Anforderungen, die in organisatorischer und technologischer Hinsicht weitreichende Anpassungen erforderlich machen. Ein weiterer wichtiger Punkt: **Der Geltungsbereich der DSGVO erstreckt sich auf alle Unternehmen weltweit, die Daten über Personen erheben oder verarbeiten, die innerhalb der EU leben**. Dazu zählen neben EU-Bürgern auch Touristen und Arbeitnehmer im Ausland. Für die Einhaltung der Bestimmungen der DSGVO ist nun der geographische Standort der natürlichen Person maßgebend, deren personenbezogene Daten erhoben wurden, und nicht der Sitz des Unternehmens, das die Daten erfasst. Hieraus ergeben sich **gravierende Konsequenzen für alle Unternehmen, die innerhalb Europas geschäftlich tätig sind** (inklusive Großbritannien nach dem Brexit). Das gilt sowohl für die EU als auch den Europäischen Wirtschaftsraum (EWR).

Die DSGVO räumt EU-Bürgern zudem das Recht ein, die Herausgabe ihrer personenbezogenen Daten zu verlangen. Unternehmen, die derartige Daten erheben und speichern, müssen einer solchen Bitte zwingend nachkommen. Außerdem kann die Einwilligung zur Nutzung widerrufen und somit effektiv eine Löschung der Daten beantragt werden. Artikel 12 der DSGVO, der die Rechte betroffener Personen und den transparenten Umgang mit derartigen Daten regelt, legt dar, dass die Einsehung oder Löschung personenbezogener Daten kostenfrei und unkompliziert zu beantragen sein muss und einem solchen Antrag „unverzüglich, in jedem Fall aber innerhalb eines Monats“ nachzukommen ist. Da die Umsetzung der Bestimmungen der DSGVO mit einem hohen Kosten- und Zeitaufwand verbunden ist, wurde das Datum, an dem ihre Einhaltung für Unternehmen verpflichtend ist, auf **Mai 2018** verschoben. Doch angesichts der enormen Tragweite der Verordnung sind Unternehmen bereits jetzt aufgerufen, ihren Umgang mit personenbezogenen Daten auf die Probe zu stellen.

Kerninhalte der DSGVO

Nachfolgend erläutern wir, was sich mit der DSGVO alles ändert – insbesondere im Vergleich zur vorhergehenden Datenschutzrichtlinie 95/46/EG, die 1995 in Kraft trat.

Die Datenschutz-Grundverordnung fällt nun in eine gänzlich neue Epoche, in der die Welt zunehmend mithilfe von Datenflüssen gesteuert wird. In diesem Kontext verfolgt sie das Ziel, alle EU-Bürger noch

effektiver vor einer Verletzung ihrer Datenschutzrechte zu bewahren. In ihren Grundprinzipien stimmt die Verordnung mit der Richtlinie 95/46/EG überein. Die meisten Änderungen betreffen aufsichtsrechtliche Bestimmungen. Die Kernpunkte der DSGVO und ihre Folgen für Geschäftstreibende werden nachfolgend dargelegt:

Größere territoriale Reichweite

(erweiterter räumlicher Geltungsbereich)
Die wohl bedeutendste Änderung der DSGVO betrifft ihren räumlichen Geltungsbereich: Zu ihrer Einhaltung verpflichtet sind alle Unternehmen, die personenbezogene Daten natürlicher Personen verarbeiten, welche sich im Hoheitsgebiet der Europäischen Union aufhalten. Der Firmenstandort spielt dabei keine Rolle. Der Anwendungsbereich der zuvor geltenden Richtlinie 95/46/EG war weniger eindeutig geregelt und an das Vorhandensein einer „Niederlassung" innerhalb der EU gekoppelt. Viel blieb demnach Auslegungssache und bedurfte gerichtlicher Klärung. Die DSGVO definiert ihren Anwendungsbereich hingegen unmissverständlich: Sie gilt in den Grenzen der EU für die Verarbeitung personenbezogener Daten durch sogenannte Verantwortliche und Auftragsverarbeiter – und das unabhängig davon, ob die Verarbeitung in der EU oder außerhalb davon stattfindet. Die Verordnung gilt demnach auch für die Verarbeitung personenbezogener Daten durch Verantwortliche oder Auftragsverarbeiter, die nicht in der EU ansässig sind, sofern sich die von der Verarbeitung betroffenen Personen in der EU aufhalten. Außerdem wird vorausgesetzt, dass dabei Waren oder Dienstleistungen gegenüber EU-Bürgern (ob kostenfrei oder kostenpflichtig) angeboten werden und die Überwachung von Verhalten innerhalb der EU erfolgt. Nicht innerhalb der EU ansässige Unternehmen, die Daten von EU-Bürgern verarbeiten, werden somit ebenfalls verpflichtet, einen Datenschutzbeauftragten für die EU zu stellen.

Geldbußen

Unternehmen, die gegen die Bestimmungen der DSGVO verstoßen, können mit einer Geldbuße von bis zu **4 Prozent des weltweit erzielten Jahresumsatzes oder 20 Millionen Euro** sanktioniert werden, je nachdem, welcher Betrag der höhere ist. Dieser Höchstsatz kann bei besonders schwerwiegenden Verstößen, beispielsweise bei fehlender Einwilligung eines Kunden zur Datenverarbeitung oder einem Verstoß gegen das Grundprinzip des „eingebauten Datenschutzes" (Privacy by Design) zum Tragen kommen. Die Höhe der Geldbuße richtet sich nach der Schwere des Verstoßes und wird stufenweise berechnet. So kann etwa gegen ein Unternehmen eine Strafzahlung in Höhe von 2 Prozent des Jahresumsatzes verhängt werden, wenn dessen Unterlagen unvollständig sind (Art. 28), Aufsichtsbehörden und betroffene Personen nicht über einen Verstoß benachrichtigt wurden oder keine Datenschutz-Folgenabschätzung erfolgte. Wichtig ist dabei, dass diese Regeln sowohl für Verantwortliche als auch für Auftragsverarbeiter gelten. Anbieter von Clouddiensten sind somit nicht von der DSGVO ausgenommen.

Einwilligung

Ein weiteres Anliegen der DSGVO ist es, Datenschutzbestimmungen von Unternehmen transparenter zu gestalten. Viele Datenschutzbestimmungen sind infolge von juristischem Fachjargon und verklausulierten Formulierungen nur schwer

verständlich und schützen eher den Urheber, als dass sie den Kunden informieren. Die neue Verordnung sieht vor, dass eine Einwilligung zur Datenverarbeitung nur dann zulässig ist, wenn die zugrunde liegenden Bedingungen in einer klar verständlichen und leicht zugänglichen Art und Weise verfasst wurden. Zudem muss die Einwilligung problemlos widerrufen werden können.

Zeitgemäßer Datenschutz

Gleich ob Ihr Unternehmen Daten lokal oder in der Cloud speichert – in jedem Fall muss die Vertraulichkeit und Sicherheit erhobener Daten zu jedem Zeitpunkt gewahrt bleiben. Firmen sollten deshalb bereits jetzt damit beginnen, die Grundsätze der DSGVO umzusetzen, um Risiken zu minimieren, die aktuell im Hinblick auf den Datenschutz bestehen. Außerdem wird angeraten, alle Daten, die Ihr Unternehmen derzeit von Kunden speichert, auf die Probe zu stellen. So stellen Sie sicher, dass Sie nur tatsächlich benötigte Daten im jeweils vereinbarten Umfang erfassen. Unternehmen – insbesondere solche außerhalb von Europa, die Kundendaten zu Marketingzwecken speichern – müssen sich darauf einstellen, Datenbanken und darin enthaltene Kundendaten an der neuen Verordnung auszurichten. Bei der Entwicklung und Nutzung von Anwendungen, Dienstleistungen und Produkten, welche die Verarbeitung personenbezogener Daten umfassen, sollten im Hinblick auf deren Erhebung und Schutz strenge Kontrollverfahren implementiert werden. Wenn Sie bei der Datenerhebung proaktiv die Perspektive des Anwenders einnehmen, können Sie auch mit größerer Wahrscheinlichkeit zukünftigen Anfragen von Kunden nachkommen, die ihre Daten löschen möchten.

Gerüstet für 2018

In der Realität bieten Verordnungen der EU nicht selten eine Fülle an Interpretationsspielraum. Das stellt für Unternehmen und ihre IT-Teams eine enorme Herausforderung dar. Wie viele vergleichbare Regelwerke zum Datenschutz verpflichtet auch die DSGVO betroffene Unternehmen dazu, Best Practices anzuwenden und bestimmte Schutzmechanismen

zu etablieren, um die Sicherheit und den Schutz von Kundendaten zu gewährleisten. Sie legt hingegen nicht klar dar, welche Sicherheitslösungen dafür in Betracht kommen, was für IT-Abteilungen in vielerlei Hinsicht problematisch ist. In jedem Fall erfordert die DSGVO einen ganzheitlichen Ansatz zur Informationssicherheit – inklusive Best Practices, umfassender Dokumentation und effektiven Sicherheitstools.

Demgemäß werden nachfolgend einige **Best Practices** empfohlen, die Unternehmen in Vorbereitung auf das Inkrafttreten der neuen Verordnung im **Mai 2018** umsetzen sollten:

- Führen Sie einen Datenaudit durch, um herauszufinden, welche Daten sich in Ihrem Besitz befinden und wie sie verwendet werden.
- Klassifizieren Sie Daten nach ihrer Vertraulichkeit und trennen Sie sich von irrelevanten Kundendaten, um Risiken zu minimieren.
- Überwachen Sie die E-Mail-Archivierung und Datenbackups, um unbeabsichtigte (und vorsätzlich herbeigeführte) Datenschutzverletzungen zu verhindern.
- Sensibilisieren Sie Mitarbeiter und schulen Sie Anwender zu wichtigen Themen des Datenschutzes.
- Prüfen Sie kontinuierlich, welche Anwender eingeschränkten Zugriff auf Kundendaten besitzen sollten.
- Erwägen Sie die Nutzung von Zwei-Faktor-Authentifizierung für jeden Account mit sensiblem Datenzugang.
- Implementieren Sie einen mehrstufigen Sicherheitsansatz für E-Mails und Firmennetzwerke, um Cyberangriffe in Form von Phishing und Ransomware zu verhindern.
- Erarbeiten Sie einen Notfallplan, um Verstöße gegen Datenschutzbestimmungen innerhalb von 72 Stunden melden zu können.
- Ernennen Sie in Einklang mit den Anforderungen der DSGVO einen Datenschutzbeauftragten für Ihr Unternehmen.

Wie kann AppRiver helfen?

Das in der DSGVO verankerte Grundprinzip von „Privacy by Design“ meint Datenschutz, der bereits bei der Entwicklung eines Systems eingebaut und nicht erst nachträglich ergänzt wird. Im Wortlaut sieht die Verordnung dahingehend vor, dass „der Verantwortliche ... geeignete technische und organisatorische Maßnahmen [zu treffen hat] ..., um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.“ Die **Lösungen von AppRiver für fortschrittlichen Bedrohungsschutz** inklusive **E-Mail-Verschlüsselung** bieten kleinen und mittleren Unternehmen Schutz vor Sicherheitsverletzungen und Datenlecks. Dabei kommt ein mehrstufiger Sicherheitsansatz zum Einsatz.

Eingebaute Sicherheit und Vertraulichkeit

Die Sicherheit und Vertraulichkeit von Kundendaten muss laut DSGVO von Anfang an gewährleistet sein. Im Rahmen der Verordnung werden Unternehmen verpflichtet, einen lückenlosen Datenschutzplan zu erarbeiten. Durch die Dokumentation sämtlicher Bestandteile Ihres Sicherheitsmodells und Ihrer Datenschutzrichtlinie kann Ihr Unternehmen potenziellen und bestehenden Kunden die Gewissheit bieten, dass der bereitgestellte Schutz in Einklang mit der Intention der Verordnung steht.

Prüfung und Überwachung Ihres Netzwerks

Praktisch jedes Unternehmen nutzt heutzutage Informationstechnik in Form von Computern, Netzwerken und Daten. Zum Schutz dieser Vermögenswerte ist es notwendig, dass Unternehmen jeder Größe

GERÜSTET FÜR DIE DSGVO
Datenschutz-Grundverordnung

IT-Sicherheitsaudits durchführen. Dadurch erhalten sie Informationen über den Status ihres Netzwerks, vorhandene Sicherheitslücken und die besten Strategien im Umgang mit Bedrohungen.
Wenn Sie **SecureSurf®** bereits in Ihrem Netzwerk implementiert haben, empfiehlt es sich, mit den verfügbaren Überwachungsoptionen einen Netzwerkaudit durchzuführen und die Netzwerknutzung sowie Bedrohungen zu analysieren. In einem Bericht werden Sie über die Integrität des Netzwerks und identifizierte Malware informiert. Wird Malware entdeckt, blockiert **SecureSurf®** den Versuch automatisch und gibt Ihnen die Möglichkeit, die Infizierung zu beheben. Erstellen Sie außerdem eine Bestandsliste der Vermögenswerte Ihres Unternehmens, um zu entscheiden, was geschützt werden muss. Diese Liste sollte in jedem Fall zumindest PCs, Mobiltelefone, Laptops, Router, VoIP-Telefone, IP PBXs, Netzwerkgeräte und Drucker enthalten.

Mehrschichtige Sicherheit

Mehrschichtige Ansätze zur Sicherung von Netzwerken haben sich in der Praxis bewährt. Ihr Unternehmen sollte durch eine kombinierte Lösung für E-Mail- und Websicherheit und zusätzlichen Antivirus-Schutz für Endgeräte alle Sicherheitslücken schließen. Plattformen für Webschutz, wie **SecureSurf®**, ergänzen **SecureTide®** E-Mail-Sicherheit und Antivirus-Schutz für Endgeräte, indem Malware an der Quelle blockiert wird. Außerdem werden Netzwerke nach vorhandener Malware durchsucht, die bisher unerkannt geblieben ist und Kontakt zum Server der Bedrohungsurheber aufnehmen könnte. In jedem Netzwerk gibt es Sicherheitslücken. Durch die passende Kombination aus **E-Mail-Sicherheit**, **Netzwerk- und Antivirus-Schutz für Endgeräte sowie Websicherheit** kann ein Unternehmen diese Lücken schließen und eingehenden sowie ausgehenden Datenverkehr überwachen.

E-Mail-Verschlüsselung

Häufig bewältigen E-Mails eine lange Reise durch den digitalen Äther, bevor sie Ihr Postfach erreichen. Mit **CipherPost Pro®** von AppRiver verhindern Sie, dass Unbefugte Einblick in sensible Kommunikation erlangen. **CipherPost Pro verschlüsselt** per einfachem Mausklick Nachrichten, sobald diese Ihr Postfach verlassen. Nur der vorgesehene Empfänger kann die Nachricht mit dem richtigen Kennwort lesen. Somit bleiben Vertraulichkeit und Schutz von Kundendaten bei der E-Mail-Übermittlung stets gewahrt. Die Verschlüsselungsmechanismen von CipherPost Pro bieten lückenlose **E-Mail-Sicherheit von Posteingang zu Posteingang** – unabhängig davon, über welche Kanäle die Nachricht versendet wird.
CipherPost Pro® hilft Ihnen dabei, die rechenschaftspflichtigen Anforderungen gemäß **Art. 5 Abs. 2 DSGVO** zu erfüllen. Zudem können Sie sich optional den **Eingang von E-Mails bescheinigen lassen**, um jederzeit den Status aller verschlüsselten E-Mails prüfen und verifizieren zu können.

Verwandte Lösungen

SecureTide® – *Spam- und Virenschutz*
SecureSurf® – *Web- und Netzwerkschutz*
CipherPost Pro® – *E-Mail-Verschlüsselung*