VARONIS

DSGVO

EIN PRAXISLEITFADEN

Stellen Sie sich auf die DSGVO ein.

Entdecken, verwalten und schützen
Sie Ihre DSGVO-Daten mit Varonis.

Automatische Entdeckung und Klassifizierung von Daten, die unter die DSGVO fallen.

Einrichten von Zugriffskontrollen und Schutz regulierter Daten.

Aufbau einer DSGVO-Sicherheitsrichtlinie zur Erfüllung von Konformitätsanforderungen.

Die Varonis Datensicherheitsplattform bietet Transparenz in unsere unstrukturierten Datenstandorte, wer darauf Zugriff hat und wie sie genutzt werden. Wenn wir dabei entsprechende Richtlinien nutzen, sind wir in der Lage, uns einen vollen Überblick über EU-DSGVO zu verschaffen.

– Chief Information Security Officer, Gemeinnützige Organisation

Inhalt

Varonis Deutschland GmbH:
T +49 (0)89 3803 7990 **E** sales-germany@varonis.com **W** www.varonis.de

EU-DSGVO LEKTION 1

Was ist die EU-Datenschutz-Grundverordnung (DSGVO)?

Die EU-DSGVO ist eine Weiterentwicklung der bisherigen Datenschutzvorschrift der EU, der Datenschutz-Richtlinie. Die DSGVO gilt als einheitliche Rechtsnorm für die gesamte EU und über diese hinaus. Sie stellt neue Anforderungen an die Dokumentation von IT-Prozessen, die Durchführung von Risikobewertungen sowie an die Meldepflichten bei Datenschutzverletzungen. Dazu zählt auch eine strengere Datenminimierung. Mit ihr entsteht eine einheitliche Gesetzgebung zur Durchsetzung der Datenschutzvorschriften und -normen in Europa, und sie etabliert ein Recht auf den Schutz personenbezogener Daten.

Mit ihr wird das in Recht umgesetzt, was einem der gesunde Menschenverstand rät, insbesondere Ansätze des Datenschutzes ab Entwurfsebene: das Speichern der minimal benötigten Daten, löschen von nicht mehr benötigten Daten, Zugriffsbeschränkung und Schutz von Daten über deren gesamten Lebenszyklus.

Welche Datenarten sind geschützt?

Personenbezogene Daten die in den USA auch als persönlich identifizierbare Informationen (PII) bezeichnet werden. Das sind z. B. Namen, Adressen, Telefonnummern, Kontonummern und in neuerer Zeit auch E-Mails und IP-Adressen.

Für wen gilt sie?

Die DSGVO gilt für Unternehmen mit Sitz in der EU und für Unternehmen, die Daten von europäischen Bürgern speichern, unabhängig von deren physischer Anwesenheit im Land.

Welche Folgen hat das für Sie?

Es gibt jetzt neue Vorschriften und Anforderungen für das Aufzeichnen und Speichern personenbezogener Daten und für die Verarbeitung von Daten, neue Vorschriften für die Meldung von Datenschutzverletzungen, Sanktionen für Verstöße usw.

Welche neuen Anforderungen sind zu beachten?

Datenschutz durch Technikgestaltung - In der DSGVO wurde das Prinzip des Datenschutzes durch Technikgestaltung formalisiert.

Dazu gehört auch die Minimierung der Datenspeicherung und - aufbewahrung und die Notwendigkeit einer Einwilligung von Verbrauchern bei der Verarbeitung ihrer Daten.

Datenschutzfolgenabschätzungen - Wenn bestimmte stark gefährdende oder sensible, mit einer Person verbundene Daten verarbeitet werden sollen, müssen Unternehmen zunächst die damit verbundenen datenschutztechnischen Risiken analysieren.

Recht auf Löschung und Vergessenwerden - Bereits zu Zeiten der Datenschutz-Richtlinie gab es die Vorgabe, dass Verbraucher die Löschung ihrer Daten fordern konnten. Die DSGVO erweitert dieses Recht auf Daten, die im Internet veröffentlicht wurden. Dieses Recht, dem öffentlichen Blick verborgen zu bleiben und „vergessen“ zu werden, wird weiterhin kontrovers diskutiert.

Grenzübergreifend - Selbst wenn ein Unternehmen keine physische Präsenz innerhalb der EU unterhält, gelten alle Anforderungen der DSGVO, wenn es Daten von Datensubjekten der EU benutzt oder speichert (z. B. durch eine Website). Anders formuliert gilt das neue Recht über die Grenzen der EU hinaus. Das hat insbesondere für e Commerce-Unternehmen und andere cloudbasierte Geschäftsmodelle Konsequenzen.

Meldung von Datenschutzverletzungen - Unternehmen müssen die für den Datenschutz zuständigen Aufsichtsbehörden innerhalb von 72 Stunden nach Entdeckung einer Verletzung des Schutzes personenbezogener Daten darüber informieren. Auch die betroffenen Personen müssen informiert werden, aber nur, wenn von den Daten ein „hohes Risiko für die Rechte und Freiheiten“ dieser Personen ausgeht.

Geldbußen - Schwere Verstöße können mit einer Geldbuße von bis zu 4 % des weltweit erzielten Umsatzes bestraft werden. Zu diesen Verstößen können auch Verletzungen der grundlegenden Prinzipien des Datenschutzes gehören - vor allem der Grundsätze des Datenschutzes durch Technikgestaltung. Eine geringere Geldbuße von bis zu 2 % der weltweit erzielten Umsätze kann verhängt werden, wenn ein Unternehmen keine ordnungsgemäßen Aufzeichnungen führt oder versäumt, die Aufsichtsbehörde und Datensubjekte über eine Datenschutzverletzung zu informieren.

Die DSGVO ist eine datenzentrierte Verordnung, weshalb sie einen datenzentrischen Sicherheitsansatz erforderlich macht. Die DSGVO macht deutlich, dass ein bewusster Umgang mit Ihren Daten -wo sensible Daten gespeichert werden, wer auf sie zugreift und wer auf sie zugreifen sollte - heute wichtiger ist als je zuvor

EU-DSGVO LEKTION 2

Datenschutz durch Technikgestaltung und Voreinstellungen

Datenschutz durch Technikgestaltung beschreibt eine Reihe von rechtlich verbindlichen Grundsätzen für die haftende Unternehmensleitung, deren Umsetzung Datenschutz und Datensicherheit sicherstellt

Aber die Datenschutz-Grundverordnung (DSGVO) greift noch weiter: Wenn Sie in der EU Geschäfte machen, werden diese Grundsätze rechtlich verpflichtend!

Datenschutz durch Technikgestaltung liefert gute allgemeine Empfehlungen für den Datenschutz, die sich in einem Wort zusammenfassen lassen: Minimierung.

Minimieren des Speicherns von Verbraucherdaten, minimieren des Personenkreises, dem Sie die Daten weitergeben, und minimieren der Aufbewahrungsdauer. Weniger ist mehr: Je weniger Daten ein Hacker erbeuten könnte, desto sicherer ist Ihr System.

Tatsächlich könnte man sagen, dass Sie auf dem besten Wege sind, die DSGVO zu meistern, wenn Sie die Grundsätze des Datenschutzes durch Technikgestaltung umsetzen.

Können Big Data und Datenschutz durch Technikgestaltung einvernehmlich koexistieren? Ja - mit wenigen grundlegenden Schritten können Sie dies erreichen:

Minimieren Sie die von Verbrauchern gesammelten Daten (insbesondere PII).

Bewahren Sie Daten nicht mehr auf, wenn sie ihren ursprünglichen Zweck erfüllt haben.

Geben Sie den Verbraucher Zugriff, Kontrolle und Transparenz über ihre Daten.

EU-DSGVO LEKTION 3

Das Recht auf Vergessenwerden

Das kontroverse „Recht auf Vergessenwerden“ ist in der EU jetzt Gesetz.

Für die meisten Unternehmen bezeichnet es einfach das Recht der Verbraucher, dass ihre Daten gelöscht werden.

Die DSGVO hat die bisherigen Regeln der Datenschutz-Richtlinie zum Löschen gestärkt und dann das Recht auf Vergessenwerden ergänzt. Die neue Formulierung würde den Verantwortlichen zwingen, angemessene Maßnahmen zu ergreifen, um Dritte über den Antrag auf Löschen der Informationen zu informieren.

In Artikel 17 DSGVO heißt es: „Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass die betreffenden personenbezogenen Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen, sofern einer der folgenden Gründe zutrifft: … Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig. … Die betroffene Person widerruft ihre Einwilligung, auf die sich die Verarbeitung … stützte, … Hat der Verantwortliche die personenbezogenen Daten öffentlich gemacht ist er … zu deren Löschung verpflichtet …“

Das bedeutet, dass z. B. der Anbieter eines sozialen Netzwerks, der personenbezogene Daten im Internet veröffentlicht, nicht nur die ursprünglichen Informationen löschen muss, sondern auch andere Websites kontaktieren muss, die diese Informationen möglicherweise kopiert haben.

Das ist nicht einfach!

Was passiert, wenn der Datenverantwortliche personenbezogene Daten an andere Dritte weitergibt, z. B. einen cloudbasierten Dienst für Datenspeicherung und -verarbeitung?

Die EU-Verordnung gilt auch in diesen Fall: Als Auftragsverarbeiter muss auch der Cloud-Service nach Aufforderung durch den Verantwortlichen die personenbezogenen Daten löschen.

Der Verbraucher bzw. die betroffene Person kann jederzeit fordern, dass ein Unternehmen die über und von Ihm gespeicherten Daten löscht. In der EU sind die Daten das Eigentum der Bürger!

EU-DSGVO LEKTION 4

Wen betrifft die EU-DSGVO?

Zu den komplexeren Punkten rund um die neue DSGVO gehört das Konzept der „Extraterritorialität“. Gemäß Artikel 3 gilt die DSGVO für alle personenbezogenen Daten, die aus dem Gebiet der EU übertragen werden.

Wenn also unter der neuen Verordnung ein US-Unternehmen Daten von EU-Bürgern sammelt, unterliegt es denselben gesetzlichen Pflichten wie ein Unternehmen mit Sitz in Frankreich, Großbritannien oder Deutschland - auch wenn es dort gar keine Server oder Geschäftsräume unterhält.

Rechtsexperten merken an, dass es schwierig sein könnte, dies durchzusetzen. Wenn aber ein großes multinationales Unternehmen gegen eine der Vorschriften verstößt - z. B. die neue strenge Meldepflicht laut DSGVO bei Datenschutzverstößen - wird es mit großer Sicherheit in den Fokus der EU-Aufsichtsbehörden geraten.

Extraterritorialität ist offenkundig sehr relevant für zentrale Web-Dienste wie Suchmaschinen, soziale Netzwerke, e-Commerce, Online- Vermittlungen von Mietwohnungen usw.

Um zu verstehen wer betroffen sein dürfte, müssen Sie nur Ihre meistbenutzten Applikationen betrachten..

Veränderte Voraussetzungen

Bei der vorhergehenden Datenschutz-Richtlinie gab es kleine Lücken, durch die sich speichernde Unternehmen der Pflicht entziehen konnten, die Vorschriften einzuhalten. Eine übliche Vorgehensweise war, dass Dienst-oder App-Anbieter ihre Datenverarbeitung außerhalb der EU durchführten.

Die Überlegung dabei war, dass die Regeln nicht gelten, wenn sich die Hauptverarbeitung und die Server außerhalb des EU-Gebiets befänden.

Unternehmen wie Google, Facebook und andere Anbieter sozialer Netzwerke arbeiteten nach diesem Prinzip.

Nicht so schnell!

Diese Argumentation wurde bekannt, als Google mit ihr auf die Aufforderung einer spanischen Datenschutzbehörde reagierte, einen Eintrag in den Suchergebnissen zu löschen. Der Fall landete letztendlich vor dem höchsten Gericht der EU, dem europäischen Gerichtshof, der gegen Google urteilte.

Der lange Arm des EU-Rechts setzte sich durch: Der konkrete Eintrag der Suche wurde gelöscht.

Dieses Konzept des erweiterten räumlichen Geltungsbereichs ist in Artikel 3 der DSGVO ausdrücklich vorgesehen. Die DSGVO wird für Unternehmen mit Sitz in der EU und für Unternehmen gelten, die Daten von europäischen Bürgern sammeln, unabhängig von ihrer physischer Anwesenheit in der EU.

EU-DSGVO LEKTION 5

Was geschieht, wenn ich gegen die DSGVO verstoße?

Die DSGVO sieht gestaffelte Sanktionen mit erheblichen finanziellen Konsequenzen bei Verstößen vor - und die Regelungen der DSGVO gelten sowohl für Datenverantwortliche als auch für Auftragsverarbeiter. Große Cloud-Provider sind also im Hinblick auf die Durchsetzung der DSGVO nicht aus der Pflicht!.

Verstöße können mit einer Geldbuße von bis zu 4 % des weltweit erzielten Umsatzes bestraft werden.

Ein Unternehmen kann eine Geldbuße von bis zu 2 % seines weltweit erzielten Umsatzes auferlegt bekommen, wenn es keine ordentlichen Aufzeichnungen führt (Art. 30), die Aufsichtsbehörden und betroffenen Personen nicht über Datenschutzverletzungen informiert (Art. 33 und 34) oder keine Folgenabschätzungen vornimmt (Art. 35).

Dabei ist zu bedenken, dass die Meldung einer Datenschutzverletzung gemäß DSGVO mehr umfasst als den einfachen Hinweis, dass es einen Vorfall gegeben hat. Sie müssen die Datenkategorien, betroffenen Datensätze und die geschätzte Anzahl der Betroffenen angeben.

Sie müssen also recht detaillierte Erkenntnisse darüber haben, was Hacker und Insider getan haben.

Schwerwiegendere Verstöße werden mit einer Geldbuße von bis zu 4 % der globalen Umsätze geahndet. Zu diesen Verstößen zählen Verstöße gegen die grundlegenden Prinzipien der Datensicherheit (Art. 5) und das Einwilligungsprinzip (Art. 7) - also die Missachtung der zentralen Konzepte des Datenschutzes durch Technikgestaltung gemäß Verordnung.

Eine Methode, mit der die Gestalter der DSGVO deren Implementation sicherstellen wollen, ist die Pflicht für Unternehmen, einen Datenschutzbeauftragten zu benennen. Der Datenschutzbeauftragte ist für die Einrichtung von Zugriffskontrollen, Minderung von Risiken, Sicherung der Compliance, Beantwortung von Anfragen und die Meldung von Datenschutzverletzungen innerhalb von 72 Stunden sowie die Entwicklung einer robusten Datenschutzrichtlinie verantwortlich.

EU-DSGVO LEKTION 6

Die nächsten Schritte - der Weg zum Ziel

Artikel 25

Datenschutz durch Technikgestaltung und Voreinstellungen

BEDEUTUNG

Rechenschaftspflicht und Datenschutz durch Technikgestaltung als Teil der Unternehmenskultur integrieren.

SO HILFT VARONIS

Identifizieren, wer Zugriff auf regulierte Daten hat und wer Zugriff haben sollte. Verwalten von Berechtigungen, automatische Beseitigung von Risiken, wie globale Zugriffsgruppen und inkonsistente ACLs*. Einführung des Prinzips der minimalen Rechtevergabe.

*ACL=Access Contral List, d.h. Zugriffsteuerungsliste

Artikel 30

Verzeichnis von Verarbeitungstätigkeiten

BEDEUTUNG

Umsetzen technischer und struktureller Maßnahmen für die vorschriftsmäßige Verarbeitung personenbezogener Daten.

SO HILFT VARONIS

Finden, identifizieren und klassifizieren von sensiblen und von der DSGVO betroffenen Daten. Überwachen, analysieren und Berichterstellung von Benutzeraktivitäten mit diesen Daten. Erstellen und Automatisieren von Datenspeicherungsrichtlinien, Durchführen von Datensicherheits-überprüfungen und Berichterstellung nach Datentyp, Zugriffsaktivität und mehr.

Artikel 17

Das Recht auf Löschen und „Vergessenwerden“

BEDEUTUNG

Möglichkeit zur Erkennung und Ansteuerung bestimmter Daten und automatisiertes Löschen.

SO HILFT VARONIS

Finden, identifizieren und klassifizieren von sensiblen und von der DSGVO betroffenen Daten. Erstellen und Automatisieren von Datenspeicherungsrichtlinien. Konfigurieren von End-to-End-Migrationsregeln anhand definierter Kriterien. Diese dienen zur schnellen und sicheren Ausführung komplexer Datenmigrationen sowie zur einfachen Implementierung und Durchsetzung von Richtlinien zu Datenaufbewahrung und -löschung.

Artikel 32

Sicherheit der Verarbeitung

BEDEUTUNG

Zugriff nach dem Prinzip eines Privilegienmodells auf Basis der minimalen Rechtevergabe. Einführung von Rechenschaftspflicht durch Zuständigkeitsverteilung und Berichterstellung über Implementierung und Erfolg von Richtlinien und Prozessen.

SO HILFT VARONIS

Risikosenkung und Verwaltung von Zugriffskontrollen: Automatisierung und Durchsetzung des Prinzips der minimalen Rechtevergabe durch Anspruchsprüfungen und aktiv durchgesetzte ethische Grenzen und Sicherheitsrichtlinien.

Artikel 33

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

BEDEUTUNG

Verhindern und Melden von Datenschutzverletzungen; Einführen eines Notfallplans.

SO HILFT VARONIS

Benachrichtigung bei verdächtigen Verhaltensweisen und potenziellen Datenlecks. Erkennen von Datenschutzverstößen und Malware-Aktivitäten. Überwachen von Richtlinienverstößen.

Artikel 35

Datenschutz-Folgenabschätzung

BEDEUTUNG

Quantifizieren von Datenschutz-Risikoprofilen.

SO HILFT VARONIS

Überwachung und Bewertung Ihres Datenschutz- und Sicherheitsstatus durch Datenrisikobeurteilung: Identifizieren und Sperren sensibler Daten. Analyse von Konten mit verdächtigen Bewegungen, Auffinden von Malware-Aktivitäten und mehr.

Worauf sollten Sie sich konzentrieren, um Konformität mit der EU-Datenschutz Grundverordnung zu erreichen?

Datenklassifizierung - Schaffen Sie Klarheit darüber, wo personenbezogene Daten in Ihrem System gespeichert werden, insbesondere in unstrukturierten Formaten in Dokumenten, Präsentationen und Spreadsheets. Das ist ein entscheidender Schritt für den Datenschutz und eine gute Vorbereitung, um Aufforderungen zur Berichtigung und Löschung personenbezogener Daten erfüllen zu können.

Metadaten - Aufgrund der Anforderung im Hinblick auf die Minimierung der Datenspeicherung benötigen Sie grundlegende Informationen darüber, wann, warum und wofür Daten gesammelt wurden. Der Bestand personenbezogener Daten in IT-Systemen sollte regelmäßig daraufhin untersucht werden.

Governance - Die DSGVO hebt hervor, wie wichtig es ist, auf die Grundlagen zu achten. Bei Unternehmensdaten gehört dazu auch die Kenntnis darüber, wer im Dateisystem des Unternehmens auf personenbezogene Daten zugreift, und wer dazu berechtigt sein sollte.

Die Dateiberechtigungen sollten auf Basis der tatsächlichen Rollen von Mitarbeitern beschränkt sein, z. B. durch rollenbasierte Zugriffskontrollen.

Überwachung - Durch die Pflichtmeldungen bei Datenschutzverletzungen entsteht eine neue, weit höhere Anforderung für Datenverantwortliche. Gemäß der DSGVO sollte das Mantra der IT-Sicherheit „pausenlose Überwachung“ lauten. Sie müssen ungewöhnliche Zugriffsmuster mit Dateien abgleichen, die personenbezogene Daten enthalten und Datenlecks sofort der zuständigen Aufsichtsbehörde melden. Bei Unterlassung können enorme Geldbußen verhängt werden, insbesondere für multinationale Unternehmen mit hohen Umsatzerlösen auf globaler Ebene.

Varonis unterstützt Unternehmen bei der Erfüllung von DSGVO-Konformitätsanforderungen: Automatische Entdeckung und Klassifizierung von DSGVO-Daten mit über 250 exklusiven Mustern zur Erkennung der von der DSGVO betroffenen Daten. Überwachung und Meldung verdächtiger Verhaltensweisen und ungewöhnlicher Aktivitäten. Einrichten von Zugriffskontrollen und Datenschutzrichtlinien sowie Aufbau einer einheitlichen Datensicherheitsstrategie zum Schutz von Kundendaten.

Varonis ist ein führender Technologieanbieter auf dem Gebiet der Datensicherheit und -analyse, spezialisiert auf Software für Datensicherheit, Governance, Compliance, Klassifizierung und Analysen. Varonis erkennt Insider-Risiken und Cyberangriffe durch Analysieren der Dateiaktivitäten und des Benutzerverhaltens, beugt durch Sperren sensibler Daten Katastrophen vor und sorgt durch Automatisierung für einen sicheren Zustand.

Wir unterstützen tausende von Kunden dabei, sich vor Sicherheitsverletzungen zu schützen.

NASA ING Nasdaq CHAMPAGNE BOLLINGER DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH L'ORÉAL

Vereinbaren Sie eine DSGVO-Bereitschaftsprüfung

Datenrisikobeurteilung

Sie erhalten Ihr Risikoprofil, entdecken Sicherheitslücken und beheben echte Sicherheitsprobleme.

info.varonis.com/gdpr-risk-assessment-de

Live Demo

Richten Sie Varonis in Ihrer eigenen Umgebung ein, um zu beobachten, wie Ransomware gestoppt und Ihre Daten geschützt werden.

varonis.com/demo-de

VARONIS