Die Grundlagen für DSGVO-Compliance legen

EINFÜHRUNG

Die Datenschutz-Grundverordnung (DSGVO) trat im Mai 2018 in Kraft und verpflichtet Unternehmen aus der ganzen Welt, die personenbezogenen Daten (PBD) von Bürgern der Europäischen Union (EU) zu schützen. Obwohl die Verordnung bereits in Kraft getreten ist, haben viele Unternehmen noch immer Schwierigkeiten mit der angemessenen Implementierung von Schutzmechanismen innerhalb ihrer Systeme und Prozesse. SentryOne Produktmanager John Q. Martin behandelt die vier wichtigsten Rechte europäischer Bürger im Rahmen der DSGVO sowie die Maßnahmen, die Unternehmen ergreifen müssen, um DSGVO-Compliance zu erreichen.

Über den Autor

John ist ein Produktmanager bei SentryOne und arbeitet an Data DevOps-Lösungen. Er verfügt über mehr als ein Jahrzehnt an Erfahrung in der Arbeit mit Microsoft SQL Server und Data Platform-Technologien und weiß aus erster Hand, wann und wo sie eingesetzt oder nicht eingesetzt werden sollten. Johns Hauptinteressensfelder sind hohe Verfügbarkeit, Sicherheit und Systemleistung. Durch seine Arbeit als DBA, Datenbank-Entwickler, Business Intelligence-Entwickler und als Microsoft Premier Field Engineer (PFE), hatte John die Möglichkeit, mit großen und kleinen Kunden aus vielen verschiedenen Branchen zu interagieren. John ist außerdem ein Microsoft Data Platform MVP und ein Generaldirektor für PASS.

John Q. Martin
PRODUKTMANAGER

SentryOne

Die Grundlagen für DSGVO-Compliance legen

VON JOHN Q. MARTIN

Die DSGVO ist mehr als ein einfaches IT-Problem, sie ist auch ein geschäftliches Problem.

Obwohl IT-Lösungen ein wichtiger Bestandteil der DSGVO sind, wirken sich die Herausforderungen rund um die DSGVO auf viel mehr als die IT aus; es handelt sich dabei um ein geschäftliches Problem. Unternehmen müssen verstehen:

- Welche Daten sie erheben
- Weshalb sie diese Daten erheben
- In welchen Systemen sie Daten sammeln
- Wie sie diese Daten verwenden

Die DSGVO schützt die PBD von Bürgern der EU. Alle Unternehmen weltweit, die diese Daten erheben, müssen die DSGVO unabhängig von ihrem Unternehmensstandort einhalten und die aktive Zustimmung von betroffenen Personen einholen, um deren Daten zu erheben und zu benutzen.

Die Strafen für die Nicht-Einhaltung der DSGVO-Anforderungen können erheblich sein. Je nachdem, welcher Betrag höher ist, können Bußgelder in Höhe von maximal 4 Prozent des gesamten Jahresumsatzes eines Unternehmens oder 22 Millionen Euro verhängt werden.

> *„Die DSGVO soll EU-Bürgern dabei helfen, ihre Daten zu schützen und sich gewiss zu sein, dass die Menschen und Unternehmen, die Ihre Daten besitzen und verarbeiten, es nicht ohne ihre Zustimmung tun."*

EU-Bürger haben Rechte hinsichtlich der Erhebung und Nutzung ihrer Daten.

Die DSGVO schränkt ein, welche Daten von EU-Bürgern Unternehmen erheben und auf welche Weise sie diese Daten verwenden können. Unternehmen unterliegen oft Einschränkungen in der Verarbeitung und Nutzung von Daten, die ohne die Zustimmung der betroffenen Person erhoben wurden, sowie hinsichtlich der Dauer, für die diese Daten gespeichert werden können.

Unternehmen müssen außerdem bestimmen, ob sie ein „legitimes Interesse" an den Daten haben. Ein legitimes Interesse liegt vor, wenn die Daten erforderlich sind, um eine Unternehmensfunktion zu erfüllen, z. B. für den Vertragsabschluss oder Versand.

Personenbezogene Daten (PBD): Was gehört dazu?

PBD sind alle Informationen, die verwendet werden können, um eine Person zu identifizieren, einschließlich:

- **Persönlicher Daten**, z. B. Name, Adresse und E-Mail-Adresse
- **Andere identifizierende Daten**, z. B. eine IP-Adresse, die zu einer spezifischen Person zurückverfolgt werden kann
- **Sensible Daten** unter dem Europäischen Datenschutzgesetz, z. B. sexuelle Orientierung, politische Ausrichtung und Vorstrafen

Mehr Informationen darüber, um was es sich bei PBD handelt, finden Sie unter What is personal Data? auf der Website des Büros des britischen Informationsbeauftragten.

Die DSGVO gibt EU-Bürgern acht individuelle Rechte. Die folgenden vier Rechte haben das größte Potential, sich auf IT-Systeme auszuwirken:

Nr. 1 Recht auf Zugriff: Unternehmen müssen Daten bereitstellen, wenn sie von der betroffenen Person dazu aufgefordert werden.

Der Zugriff auf Daten ist eines der wichtigsten DSGVO-Rechte. Ein Bürger kann, in mündlicher oder schriftlicher Form, eine Anfrage an einen beliebigen Repräsentanten des Unternehmens einreichen, worauf das Unternehmen verpflichtet ist, den Erhalt dieser Anfrage zu bestätigen. Alle elektronischen Daten, einschließlich von Dokumenten in File-Shares oder E-Mails auf E-Mail-Servern, müssen dem Antragsteller innerhalb eines Kalendermonats nach Erhalt der Anfrage bereitgestellt werden; davon gibt es zwei Ausnahmen, die unten geschildert sind.

Ausnahmen von den Datenanfrage-Anforderungen der DSGVO	Optionen für das Unternehmen
Die Datenanfrage ist komplex Zum Beispiel, wenn die Daten über mehrere unterschiedliche Systeme verteilt sind	Beantragen Sie eine Verlängerung um drei Monate
Die Anfrage kompromittiert die PBD anderer betroffener Personen Zum Beispiel, E-Mails mit anderen Personen	• Entfernen Sie die PBD anderer betroffener Personen, bevor Sie dem Antragsteller die Daten bereitstellen, oder • Lehnen Sie ab, die beantragten Daten bereitzustellen, da die Art ihrer Darstellung den Schutz der Daten anderer betroffener Personen beeinträchtigt

Nr. 2 Recht auf Datenportabilität: Daten müssen in maschinenlesbarer Form zur Verfügung gestellt werden.

Das Recht auf Datenportabilität gibt Bürgern das Recht, auf alle elektronischen Daten in einem maschinenlesbaren Format zuzugreifen, einschließlich aller Daten, die über Google Analytics, Click-Through-Werbeanzeigen oder Standortdaten passiv erhoben wurden. Es umfasst keine Dokumente, die nur in Papierform vorliegen, oder zusätzliche Daten, die Unternehmen mit Hilfe der von der betroffenen Person bereitgestellten Daten erstellen. Falls diese erstellten Daten allerdings personenbezogener Natur sind und sich auf die betroffene Person beziehen, müssen auch diese Daten bereitgestellt werden.

Unternehmen sollten bereit sein, Daten in einem geläufigen, maschinenlesbaren Dateiformat bereitzustellen, z. B. in Comma Separated Values (CSV), Extensible Markup Language (XML) oder JavaScript Object Notation (JSON). Das Recht auf Datenportabilität ermöglicht der betroffenen Person auch, ein Unternehmen aufzufordern, ihre elektronisch gespeicherten Daten von einem Verantwortlichen an einen anderen zu übertragen.

Nr. 3 Recht auf Löschung: Die betroffene Person kann beantragen, aus dem System gelöscht zu werden.

Das Recht auf Löschung bedeutet, dass die betroffene Person im Rahmen der DSGVO zu jeder Zeit das Recht hat, aus dem System gelöscht oder vom System vergessen zu werden. Für bestimmte Fälle und Datentypen gibt es Ausnahmen, die es einem Unternehmen ermöglichen, eine solche Anfrage abzulehnen.

Eine Methode, die Speicherung von PBD wie E-Mail-Adressen, die im Rahmen von Verträgen benötigt werden, zu vermeiden, ist die Nutzung einer Verteilerliste. Beispielsweise können durch Verwendung einer E-Mail-Adresse wie DBATeam@CompanyA.com die Mitglieder dieser Liste mit der Zeit verändert werden, ohne im Rahmen des Vertrags PBD speichern zu müssen. Obwohl das eine effektive Lösung ist, kann sie die Sicherheit und Protokollierung beeinträchtigen, da ein Vertrag auf diese Weise an eine Liste von Personen anstelle einer spezifischen Person verschickt werden muss.

Nr. 4 Recht auf Berichtigung: Unternehmen müssen inkorrekte Daten berichtigen.

Das Recht auf Berichtigung erlaubt es der betroffenen Person, Falschinformationen zu identifizieren, die korrekten Daten bereitzustellen und, wenn möglich, nachzuweisen, dass die neuen Daten korrekt sind. Unternehmen müssen eine solche Anfrage im Laufe von 30 Kalendertagen erfüllen, es sei denn, es wird eine Verlängerung von bis zu drei Monaten für besonders komplizierte Datenänderungen beantragt, die mehrere Systeme involvieren. Backups fallen nicht unter das Recht auf Berichtigung oder Löschung; Backups bleiben unveränderlich.

Ausnahmen vom Recht auf Löschung

- Daten, die benötigt werden, um einen bestehenden Vertrag zu erfüllen; die Anfrage kann erfüllt werden, nachdem der Vertrag storniert wurde oder ausgelaufen ist
- Daten, die für Compliance-Zwecke benötigt werden, einschließlich von Steuerzwecken sowie Gesundheits- und Sicherheitsaufzeichnungen
- Nachrichtenartikel oder Aufzeichnungen von historischer Bedeutung

Unternehmen sind dazu verpflichtet, Aufzeichnungen zu führen und sie zu löschen, wenn sie nicht mehr gebraucht werden.

Diese Richtlinien können sich auch auf das Recovery Time Objective (RTO) auswirken, wenn ein System aus einem Backup wiederhergestellt werden muss. Unternehmen müssen planen, wie Veränderungen von Daten zwischen dem Zeitpunkt der Erstellung des Backups und dem Zeitpunkt, zu dem das Backup wiederhergestellt werden muss, verwaltet werden sollen. In Abhängigkeit von der Backup-Häufigkeit, kann die Menge der benötigten Zeit zur Implementierung von Datenänderungen erheblich sein.

Bereiten Sie sich auf Datenschutzverletzungen vor; implementieren Sie Prozesse für diesen Fall.

Wenn eine Datenschutzverletzung festgestellt wird, haben Unternehmen im Rahmen der DSGVO 72 Stunden nach deren Erkennung Zeit, einer zuständigen Behörde Bericht zu erstatten. Da die vorgeschriebene Zeitspanne kurz ist, müssen Unternehmen bereits vor Eintreten einer Datenschutzverletzung über fertige Kommunikationsprozesse verfügen.

In Abhängigkeit von der Schwere der Verletzung und dem Risiko für Betroffene, besteht auch eine Verpflichtung, die betroffenen Personen rechtzeitig zu benachrichtigen.

Alle Anforderungen rund um die Feststellung und Meldung von Datenschutzverletzungen hängen von der Verfügbarkeit etablierter und dokumentierter Prozesse und Verfahren ab, die definieren was eine Datenschutzverletzung ist und wie Mitarbeiter reagieren müssen. Eine schlechte Erkennungs- und Reaktionsplanung kann potentiell ernsthafte Konsequenzen für das Unternehmen haben.

Im Rahmen der Vorbereitung auf mögliche Datenschutzverletzungen, sollten Unternehmen einen Notfallfonds einrichten, um im Falle des Auftretens einer Verletzung einen forensischen Prüfer einstellen zu können. Die Ergebnisse des externen Experten werden dem Unternehmen mehr Glaubwürdigkeit in den Augen des Informationsbeauftragten verschaffen als eine Überprüfung durch einen unternehmensinternen Angestellten. Unternehmensinterne Angestellte sind – in Abhängigkeit von der Art und Größe des Unternehmens – in der Regel keine Experten und könnten wichtige Details übersehen oder sogar versuchen zu verheimlichen, was wirklich vorgefallen ist.

> *Wenn Sie akzeptieren, dass eine Datenschutzverletzung sich früher oder später ereignen wird, werden sie besser gewappnet sein, sie zu handhaben, sobald sie eintritt.*

Dokumentierung und Transparenz sind ausschlaggebend; Sie sollten wissen, wo Ihre Daten sich befinden.

Angesichts des starken Fokus auf PBD, ist es wichtig zu wissen, wo diese gespeichert werden, wer für sie zuständig ist und wo genau sie innerhalb Ihrer Systeme verwendet werden. Das kann nur erreicht werden, indem Sie effektive Dokumentation anlegen und pflegen. Es gibt drei wichtige Konzepte, die Sie verstehen und implementieren müssen, um sicherzustellen, dass Sie Fragen zum Umgang Ihres Unternehmens mit PBD beantworten können:

- **Daten-Wörterbuch:** Platzieren Sie zusätzliche Metadaten um Ihre Dateneinheiten, z. B. den Geschäftsinhaber, die Datenempfindlichkeit, die Klassifizierung, die zugehörigen Nutzungsbedingungen und andere Informationen, die Ihnen helfen, zu verstehen, wer verantwortlich ist, warum Sie über die Daten verfügen und wie sie behandelt werden sollten.
- **Systemweite Dokumentation:** Die Dokumentation einer einzelnen Datenbank oder Anwendung kann nützlich sein, aber viele heutige Datenplattform-Lösungen umfassen mehrere Technologien und Daten werden zwischen Abteilungen und Systemen geteilt. Zu wissen, was sich in einem Umfeld befindet, ist ausschlaggebend dafür, Fragen beantworten zu können und zu wissen, wann Sie handeln müssen. Können Sie ohne Schwierigkeiten alle SQL Server 2008/2008 R2-Server finden, die geupgradet werden müssen, bevor der Support im Juli 2019 endet? Kombinieren Sie diese Dokumentation mit einem effektiven Daten-Wörterbuch und Sie werden wissen, wo Daten gespeichert werden, wer für sie zuständig ist und welche Systeme Sie priorisieren sollten.
- **Datenherkunftsdokumentation:** Aufbauend auf den Grundlagen guter Dokumentation und eines Daten-Wörterbuchs, bringt es viele Vorteile, zu verstehen, auf welche Weise Daten durch Ihre Datenplattform fließen. Ein Verständnis der Datenherkunft wird es Ihnen ermöglichen, schnell zu identifizieren, ob vertrauliche Daten in Systemen landen, in denen Sie nicht sein sollten, oder in eine Tabelle in einem File-Share eingetragen werden, wodurch Sie die Einschätzung der Folgen von Veränderungen beschleunigen können, die Sie an einem System durchführen möchten, sowie deren Auswirkungen auf andere abhängige Systeme.

Checkliste: Sich auf DSGVO-Anfragen vorbereiten, bevor man sie erhält

- □ Wissen, wie einfach es ist, alle Daten zu identifizieren, die beantragt werden können.
  - Welche Systeme könnten Daten speichern?
  - Welche Suchmechanismen oder Dokumentationen können dabei helfen, die Daten zu finden?
  - In welchem Format stehen die Daten auf jedem System zur Verfügung?
- □ Wenn es mehrere Datensilos gibt, bestimmen Sie eine kleine Gruppe von Personen, die Daten systemübergreifend abfragen können. Auf diese Weise kann auf alle Daten zugegriffen werden, um die Anfragen betroffener Personen zu erfüllen, während auch die Anzahl der Personen, die Zugriff auf die Daten haben, aus Sicherheitsgründen eingegrenzt wird.
- □ Definieren Sie, wie Anfragen und Antworten protokolliert werden, sodass sie bei einer Prüfung präsentiert werden können.
- □ Stellen Sie sicher, dass die Daten in einem portablen Format wie CSV, XML oder JSON bereitgestellt werden können.
- □ Entwickeln Sie Prüfnachweise, die belegen, dass Sie die Anforderungen der DSGVO einhalten.
  - □ Verfolgen Sie nach, wann Anfragen von betroffenen Personen eingereicht wurden und welche Maßnahmen Sie ergriffen haben, um die Anfragen zu erfüllen.
  - □ Identifizieren Sie, wann Daten berichtigt wurden, einschließlich dessen, von was und zu was sie geändert wurden.
- □ Verstehen Sie den Aufbewahrungsplan für Backups, die falsche Informationen beinhalten könnten, einschließlich dessen, wie lange und warum sie aufbewahrt werden müssen.
- □ Verstehen Sie die Auswirkungen auf das RTO, um sicherzustellen, dass Datenänderungen, die seit dem letzten Backup durchgeführt wurden, nach einer Wiederherstellung ordnungsgemäß wieder in das System eingefügt werden.
- □ Implementieren Sie einen Plan für den Fall von Datenschutzverletzungen, einschließlich eines Kommunikationsplans und (wenn möglich) Notfallfonds, um einen forensischen Prüfer einstellen zu können.
- □ Testen Sie alle Prozesse, bevor sie benötigt werden, um sicherzustellen, dass sie wie erwartet und im erforderlichen Zeitrahmen funktionieren.
- □ Planen Sie, mit den Änderungen der DSGVO Schritt zu halten, sobald sie eintreten. Die DSGVO wird nach Abschluss laufender Gerichtsverfahren wahrscheinlich um weitere Anforderungen ergänzt.

Weitere Informationen

Benötigen Sie Hilfe dabei, Umfeld- und Datenherkunftsdokumentationen automatisch anstatt manuell zu erstellen? Probieren Sie SentryOne Doc xPress.

Über SentryOne

SentryOne ist ein Technologie-Unternehmen mit Sitz in Charlotte, dessen preisgekrönte Lösungen Microsoft-Datenspezialisten darin unterstützen, revolutionäre Durchbrüche in physischen, virtuellen und Cloud-Umfeldern zu erreichen. Das Team teilt seine Expertise unter blogs.sentryone.com und sqlperformance.com.

Die Grundlagen für DSGVO-Compliance legen

VON JOHN Q. MARTIN

Kontaktinformationen

+353 1 571 9490

sales@sentryone.com

EMEA Office

5 Harcourt Road

Dublin, D02 FW64, Irland

SentryOne