ERFOLGREICHE DSGVO-COMPLIANCE MIT SALESFORCE SHIELD

Dieses Dokument enthält Informationen zu diversen Bestimmungen der EU-Datenschutz-Grundverordnung (DSGVO bzw. GDPR, General Data Protection Regulation) und stellt keine Rechtsauskunft dar. Wir empfehlen Ihnen, Ihren eigenen Rechtsberater zu konsultieren und sich mit den Anforderungen basierend auf Ihren individuellen Umständen vertraut zu machen.

WAS IST SHIELD?

Bei Salesforce Shield (oder „Shield“) handelt es sich um eine Reihe von nativ in die Salesforce Platform integrierten Premium-Sicherheitsdiensten, die zu einem Aufpreis angeboten werden. Mithilfe von Shield haben Kunden einen besseren Überblick und mehr Kontrolle darüber, wie Nutzer mit Unternehmensdaten interagieren. Außerdem erhalten sie Informationen zum Zustand und Wert ihrer Daten, die bis zu zehn Jahre zurückreichen. Die Verschlüsselung von sogenannten Data at Rest ohne Beeinträchtigung der Geschäftsfunktionen ist ein weiterer Vorteil. Salesforce Shield ist deklarativ und kann mithilfe von Point-and-Click-Tools über die standardmäßige Verwaltungsoberfläche eingerichtet werden.

Shield kann den Salesforce Services als eine Sicherheitserweiterung hinzugefügt werden. Das schließt die Lightning Platform (ehemals Force.com), die Sales Cloud, die Service Cloud, und die Community Cloud sowie die Financial Services Cloud, die Health Cloud und Salesforce CPQ mit ein.

Wie kann Shield Kunden auf ihrem Weg zur DSGVO-Compliance helfen?*

Kunden sind im Rahmen ihrer Nutzung der Salesforce Services nicht zwingend auf Shield angewiesen, um die DSGVO einzuhalten. Shield kann sich jedoch als grundsätzliche Hilfe auf dem Weg hin zur Compliance erweisen.

Eine der wichtigsten Vorgaben der DSGVO besteht darin, dass Unternehmen angemessene organisatorische und technische Sicherheitsmaßnahmen zum Schutz von personenbezogenen Daten ergreifen müssen (Artikel 5(1)(f), Artikel 32).

Zu den organisatorischen Maßnahmen zählen Schulungsprogramme, Richtlinien und Verfahren. Zu den technischen Maßnahmen zählen die Benutzerauthentifizierung und logische Zugriffskontrollen.

Salesforce stellt bei der Ausführung unserer Services umfassende Sicherheitsmaßnahmen bereit. Diese werden in unserer Dokumentation zu den Themen Sicherheit, Datenschutz und Architektur beschrieben und umfassen beispielsweise Störfallmanagementverfahren und Notfallwiederherstellungspläne.

Darüber hinaus stellt Salesforce seinen Kunden eine umfangreiche Auswahl an Sicherheitsfunktionen zur Verfügung. Diese werden vom Kunden kontrolliert und können dazu verwendet werden, um die Bereitstellung von Salesforce zu erweitern, zum Beispiel durch eine Multifaktor-Authentifizierung und das Whitelisting von IP-Adressen. Shield ist ein weiterer Schritt, den Kunden ergreifen können, um den Schutz ihrer Daten noch weiter zu erhöhen.

* Bitte beachten Sie, dass die in diesem Dokument verwendeten Definitionen auf den in der DSGVO enthaltenen Definitionen basieren. Weitere Informationen über die DSGVO erhalten Sie auf der DSGVO-Webseite von Salesforce. Dort finden Sie ein Trailhead-Lernmodul, das Ihnen einen allgemeinen Überblick über die europäischen Datenschutzgesetze liefert, sowie mehrere Whitepaper.

IM FOLGENDEN WERDEN DIE DREI WICHTIGSTEN FUNKTIONEN VON SHIELD AUFGEFÜHRT:

- PLATTFORMVERSCHLÜSSELUNG
- EREIGNISÜBERWACHUNG
- FIELD AUDIT TRAIL

Dank dieser Funktionen ist Shield Kunden gleich in mehrfacher Hinsicht bei der Erfüllung ihrer gemäß der DSGVO anfallenden Verpflichtungen behilflich.

PLATTFORMVERSCHLÜSSELUNG

Was ist das?

Die Plattformverschlüsselung ermöglicht Kunden die Verschlüsselung ihrer sensiblen Data at Rest, ohne dabei wichtige Anwendungsfunktionen zu beeinträchtigen. Durch die Verschlüsselung werden die Informationen kodiert, sodass nur Personen mit dem richtigen Dekodierschlüssel darauf zugreifen können. Dadurch wird die Sicherheit der von Salesforce angebotenen Services noch weiter erhöht (siehe Dokumentation für die Bereiche Vertrauen und Compliance). Da der Service für die Plattformverschlüsselung in die Anwendungsschicht integriert ist, können wichtige Salesforce Anwendungsfunktionen auf die Verschlüsselung abgestimmt werden. Dadurch entsteht auch bei verschlüsselten Daten nur eine geringe Beeinflußung der Funktionen. (Nähere Einzelheiten erhalten Sie in unserer Implementierungsanleitung). Einige Partneranwendungen auf dem AppExchange können zudem (mit Genehmigung) Daten beinhalten und nutzen, die ein Kunde innerhalb seines Unternehmens verschlüsselt hat. Die Plattformverschlüsselung ist nativ in die Salesforce Platform integriert und lässt sich denkbar einfach über die standardmäßige Verwaltungsoberfläche oder die Schnittstelle für die Anwendungsprogrammierung einrichten.

Wie trägt die Plattformverschlüsselung zur Einhaltung der DSGVO-Anforderungen bei?

- **Sicherheitsmaßnahmen:** Auch wenn die DSGVO eine Verschlüsselung von Data at Rest nicht explizit vorschreibt, führt sie die Pseudonymisierung und Verschlüsselung von personenbezogenen Daten als Beispiel für „angemessene" technische Maßnahmen auf (Artikel 32(1)(a)). Salesforce bietet bei den meisten seiner Services eine Verschlüsselung der sogenannten „Data in Transit" – d. h. Daten, die sich auf dem Übertragungsweg befinden – an, und zwar ganz ohne Aufpreis für den Kunden. Shield bietet Ihnen die Möglichkeit, Data at Rest zu verschlüsseln. Das bedeutet, dass die Daten mithilfe komplexer und den Branchenstandards entsprechenden Verschlüsselungsalgorithmen verschlüsselt werden, wenn sie innerhalb von Salesforce gespeichert werden. Dank der Unkenntlichmachung von sensiblen personenbezogenen Daten (einschließlich personenbezogener Daten in Bezug auf Rasse, sexuelle Orientierung, Gesundheit usw.) kann sich die Plattformverschlüsselung bei der Einhaltung der DSGVO als ganz besonders hilfreich erweisen.
- **Verletzung des Schutzes personenbezogener Daten:** Die Plattformverschlüsselung kann sich auch im Falle einer Verletzung des Schutzes personenbezogener Daten als nützlich erweisen, wenn Kundendaten in ihrer verschlüsselten Form extrahiert werden – ganz gleich, in welchem Umfang. Gemäß der DSGVO ist die für die Daten verantwortliche Stelle dazu verpflichtet, die Datenschutzbehörde und/oder die betroffenen Individuen davon in Kenntnis zu setzen, wenn die Verletzung wahrscheinlich „ein Risiko für die Rechte und Freiheiten" der beteiligten Personen nach sich ziehen wird (Artikel 33 und 34). Wenn die an der Verletzung beteiligten Daten verschlüsselt sind, ist es weniger wahrscheinlich, dass die personenbezogenen Daten für jemanden sichtbar werden, der sie nicht sehen sollte. Dadurch werden die Auswirkungen der Verletzung begrenzt. Außerdem weist die DSGVO darauf hin, dass die Kommunikation mit den Datensubjekten nicht erforderlich ist, wenn die für die Daten verantwortliche Stelle angemessene technische und organisatorische Maßnahmen ergriffen hat. Dazu zählt zum Beispiel eine Verschlüsselung, durch die die Daten jeder Person gegenüber unkenntlich gemacht werden, die keine Befugnis für einen Zugriff auf diese Daten besitzt (Artikel 34(3)(a)). Eine Verschlüsselung kann in solchen Fällen also dazu beitragen, das Ausmaß möglicher Verlegenheiten oder weitergehende Untersuchungen des Vorfalls zu begrenzen.

salesforce

EREIGNISÜBERWACHUNG

Was ist das?

Die Ereignisüberwachung liefert Kunden einen umfassenden Überblick über ihre Salesforce Anwendungen und Apps. Dadurch können sie ohne Weiteres sehen, auf welche Daten die Nutzer zugreifen, von welcher IP-Adresse der Zugriff erfolgt und welche Aktionen im Hinblick auf diese Daten durchgeführt werden. Der Funktionsumfang beinhaltet eine Nachverfolgung, mit der ermittelt werden kann, wann ein Nutzer die Verantwortung ändert, eine Liste aktualisiert oder wertvolle sensible Daten exportiert. Kunden greifen über APIs einfach auf tägliche Protokolle zu, aus denen die Aktivitäten für die vergangenen 30 Tage hervorgehen. Im Falle eines Datenverlustes können Kunden auf eine Reihe von Protokollen zugreifen, mit denen sie anhand von Analysen mühelos verdächtige Aktivitäten identifizieren können, anstatt tausende Zeilen von Protokolldaten manuell zu durchforsten, um die Bedrohung zu ermitteln. Darüber hinaus lassen sich mit der Transaktionsabsicherung, einer anpassbaren Ereignisüberwachungsfunktion, Nutzeraktionen ermitteln und feststellen, ob dabei versucht wurde, sich über ein zweites Gerät anzumelden oder der Export einer Reihe von Aufzeichnungen angestrebt wurde. Diese Aktionen können in Echtzeit und basierend auf vorab festgelegten Regeln beurteilt werden. Dadurch ist die IT-Abteilung in der Lage, ungewöhnliches Verhalten zu ermitteln und unverzüglich Maßnahmen zu ergreifen.

Wie trägt die Ereignisüberwachung zur Einhaltung der DSGVO-Anforderungen bei?

- **Sicherheit und Datenintegrität:**
  Wie oben bereits erwähnt wurde, ist eine ausreichende Sicherheit wichtig, damit ein ordnungsgemäßer und den Vorgaben der DSGVO entsprechender Schutz der personenbezogenen Daten gewährleistet ist. Neben der Verschlüsselung sind in der DSGVO noch weitere Beispiele für Maßnahmen aufgeführt, die als „angemessen“ betrachtet werden. Dazu zählen jene, die es „ermöglichen, die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Verarbeitungssysteme und des Service sicherzustellen“ (Artikel 32(1)(b)). Die Ereignisüberwachung ermöglicht es Kunden, die Protokolldaten zu überwachen und verdächtige Aktivitäten schnell zu identifizieren. Dadurch werden sie bei der Erhaltung der Integrität der personenbezogenen Daten und ihrer Systeme unterstützt.
- **Verletzung des Schutzes personenbezogener Daten:**
  Dank der Ereignisüberwachung können Kunden alle Bedrohungen im Blick behalten und schnell darauf reagieren. Sie ermöglicht es Kunden, die Schäden zu minimieren und die Bedrohung schnellstmöglich zu beseitigen. Auf diese Weise werden die Auswirkungen auf die Datensubjekte begrenzt. Die für die Transaktionsabsicherung bestimmte Funktion ermöglicht es Kunden, ihr Sicherheitsprofil anzupassen, um in Echtzeit auf bestimmte Bedrohungen reagieren zu können, mit denen ihr Unternehmen gemeinhin konfrontiert wird. Das hilft Kunden dabei, ihre Richtlinien besser durchzusetzen, zum Beispiel, indem sie die entsprechende Aktivität unterbinden oder einen bestimmten Nutzer über die unerwünschte Aktivität informieren.

FIELD AUDIT TRAIL

Was ist das?

Der Field Audit Trail bietet Kunden einen Überblick über den bisherigen zeitlichen Verlauf und erweitert die aktuell in den Feldverlaufsaufzeichnungen verfügbaren Daten. Kunden können sozusagen in der Zeit zurückgehen und sich die Änderungen an ihren Audit-Trail-Daten für bis zu 60 Felder pro Objekt anzeigen lassen – und zwar für jeden Zeitpunkt innerhalb der letzten zehn Jahre. Der Field Audit Trail ist auf eine maximale Skalierbarkeit ausgelegt und ermöglicht Kunden den Zugriff auf Audit-Daten. Kunden können diese Daten auch verwenden, um relevante Richtlinien für die Datenaufbewahrung zu erstellen.

Wie trägt der Field Audit Trail zur Einhaltung der DSGVO-Anforderungen bei?

- **Aufbewahrung:**
  Eines der in der DSGVO aufgeführten Grundprinzipien besteht darin, dass personenbezogene Daten nur „so lange wie unbedingt notwendig“ zum Zwecke der Verarbeitung aufbewahrt werden dürfen. Dabei handelt es sich um das Prinzip der „Datenaufbewahrung“ (Artikel 5(1)(e)). Der Field Audit Trail kann Kunden dabei helfen, ihren mit der Datenaufbewahrung einhergehenden Verpflichtungen nachzukommen, indem er ihnen die aktive Verwaltung ihrer Daten über einen gewissen Zeitraum und die Erstellung von entsprechenden Datenaufbewahrungsrichtlinien ermöglicht.
- **Sicherheit und Datenintegrität:**
  Wie bereits erwähnt, wird in der DSGVO hervorgehoben, dass Maßnahmen, die es „ermöglichen, die kontinuierliche Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit“ der Verarbeitungssysteme sicherzustellen, als „angemessen“ betrachtet werden, um bestimmte personenbezogene Daten abzusichern. Sollten personenbezogene Daten unsachgemäß geändert worden oder verloren gegangen sein, ermöglicht es der Field Audit Trail Kunden, eine aktuelle Kopie abzurufen. Dadurch werden sie dabei unterstützt, die Verfügbarkeit und Ausfallsicherheit ihrer personenbezogenen Daten zu gewährleisten.
- **Verantwortlichkeit:**
  Die DSGVO schreibt vor, dass Unternehmen nachweisen können müssen, dass sie personenbezogene Daten gemäß den gesetzlichen Bestimmungen behandeln (Artikel 24). Der Field Audit Trail hilft Kunden dabei, dies zu erreichen, da sie mit seiner Hilfe nachweisen können, welche und für wie lange das Unternehmen Daten auf der Salesforce Platform gespeichert hat.

salesforce

WOHER WISSEN KUNDEN, OB SIE SHIELD BENÖTIGEN?

Kunden müssen selbst bestimmen, wie sie den von der DSGVO auferlegten Verpflichtungen im Hinblick auf Sicherheit und Compliance, basierend auf ihren individuellen Gegebenheiten nachkommen wollen.

Die meisten Salesforce Kunden sichern ihre Daten effektiv mithilfe der standardmäßigen Sicherheitsfunktionen von Salesforce ab. Einige Kunden könnten jedoch zu dem Schluss kommen, dass sie den Schutz ihrer Daten mithilfe von Shield erhöhen müssen.
Diese Analyse hängt von verschiedenen Faktoren ab, zum Beispiel von der Branche des Kunden, den regulatorischen Anforderungen, den internen Compliance-Richtlinien und der Art der mithilfe der Salesforce Services verarbeiteten Daten.