

RSA Archer® Privacy Program Management

Anwendungsfall für Compliance-Lösungen für Behörden und Unternehmen

Die Herausforderung

Seit vielen Jahren ringen Unternehmen mit der gewaltigen Aufgabe des Datenschutzes in ihrem Geschäftsbetrieb. Die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union (EU) und der California Consumer Privacy Act (CCPA) weisen darauf hin, wie wichtig der Schutz personenbezogener Daten ist und welche Konsequenzen es für Unternehmen haben kann, wenn hierfür keine angemessenen Maßnahmen ergriffen werden. Darüber hinaus ist der Datenschutz wichtig für das Management des Informationsrisikos und dabei spielt es keine Rolle, ob es sich um die Finanzdaten für den Gramm-Leach-Bliley Act (GLBA), um Patientendaten im Gesundheitswesen für den Health Insurance Portability and Accountability Act (HIPAA) oder einfach nur um den Kampf gegen die allgemeinen Risiken handelt, die von Datendieben ausgehen.

Heutzutage ist es mehr denn je so, dass Unternehmen in verschiedenster Weise mit dem Schutz sensibler und privater Informationen betraut sind. Unternehmen müssen ihrer Sorgfaltspflicht hinsichtlich der exakten Bestandspflege personenbezogener Daten, ihres Speicherorts sowie dem Wie und Wo der Übertragung und Verarbeitung nachkommen. Die zunehmende Customer Advocacy und Aufmerksamkeit haben dazu geführt, dass der Druck auf Unternehmen größer wird, den Kunden jederzeit die Möglichkeit zu bieten, über den Umfang der gespeicherten personenbezogenen Daten und deren Verwendung informiert zu werden. Aus diesem Grund bauen auch die Regulierungsbehörden ihre Kontrollen aus, um sicherzustellen, dass Unternehmen auf Anfragen bezüglich der Offenlegung von Daten zeitnah reagieren können und das „Recht auf Vergessenwerden“ der Kunden würdigen.

Unternehmen in jedem Markt sehen sich weiterhin dem Risiko von Datenschutzverletzungen und den verheerenden Auswirkungen ausgesetzt, den diese mit sich bringen können. In vielerlei Hinsicht unterstreichen die Verpflichtungen zur Einhaltung von Datenschutzbestimmungen lediglich die ohnehin schon drängende Notwendigkeit, proaktiv auf operative Sicherheitsprozesse und die Sorgfaltspflicht als wichtige Elemente eines soliden Programms für das Risikomanagement zu setzen. Unabhängig davon, ob es sich um die privaten Daten eines Bürgers oder das geistige Eigentum eines Unternehmens handelt, sind die Techniken und Ansätze häufig ähnlich. In der heutigen Welt des Datendiebstahls und der Unternehmensspionage müssen Unternehmen sämtliche sensiblen Daten schützen, um zu überleben.

Übersicht

Aufbauend auf den Funktionen, die der vorausgesetzte Anwendungsfall RSA Archer Data Governance bietet, unterstützt RSA Archer Privacy Program Management Unternehmen bei der Identifizierung und Bewertung der Datenschutzauswirkungen und -risiken, die von Datenverarbeitungsaktivitäten ausgehen, in die personenbezogene Daten (Personally Identifiable Information, PII) involviert sind.

RSA Archer Privacy Program Management wurde entwickelt, damit Unternehmen Datenverarbeitungsaktivitäten gruppieren können, um die Auswirkungen des Datenschutzes bewerten und die Kommunikation mit den Datenschutzbehörden bei Bestimmungsverstößen und Datenschutzverletzungen nachverfolgen zu können. Chief Privacy Officers, Data Privacy Officers (DPOs) und für den Datenschutz zuständige Teams profitieren außerdem von einem zentralen Repository mit Informationen, die erforderlich sind, um das Engagement für die DSGVO-Compliance in Bezug auf das Datenschutzprogramm des Unternehmens zu demonstrieren.

RSA Archer Privacy Program Management wurde entwickelt, damit Unternehmen den Umgang mit personenbezogenen Daten verbessern, die Kommunikation mit den Regulierungsbehörden dokumentieren und die Auswirkungen des Managements von PII auf das Datenschutzrisiko bewerten können. Mit höherer Sorgfalt und besseren Programmen können Unternehmen die Einhaltung ihrer Compliance-Pflichten nachweisen. Die Einrichtung eines effektiven

Datenschutzmanagementprogramm kann sich auch positiv auf den Nettogewinn des Unternehmens auswirken, da das Risiko von Geldbußen und Strafen wegen der Nichteinhaltung von Compliance-Vorgaben sinkt.

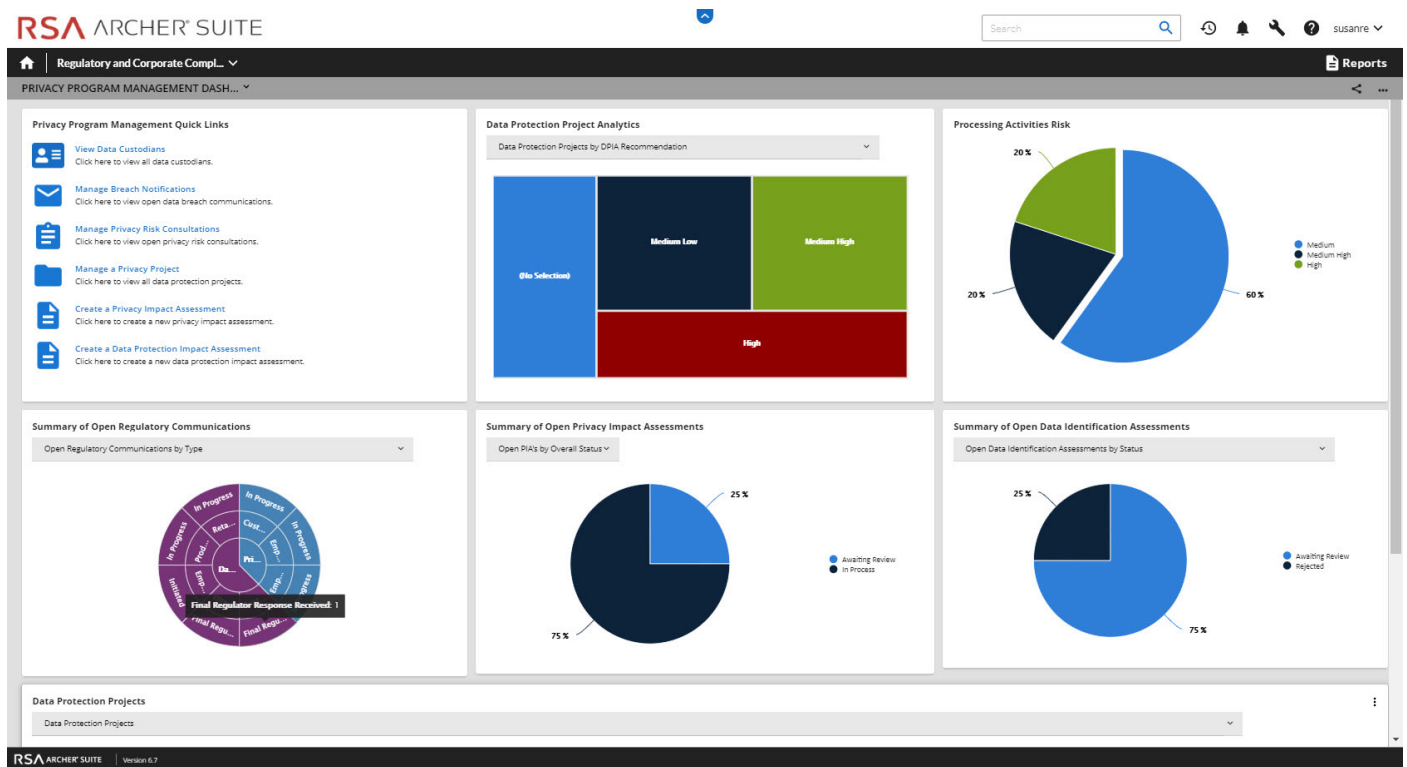
Hauptmerkmale

- Nachverfolgung und Archivierung der Kommunikation mit Aufsichtsbehörden in Bezug auf Datenschutzfragen
- Aufrechterhaltung des Bewertungsrahmens für Umgebungen mit personenbezogenen und sensiblen Daten
- Durchführung von Datenschutz-Folgenabschätzungen (PIAs) und Data Protection Impact Assessments (DPIAs)
- Ermittlung der Betriebsbedingungen, die eine DPIA gemäß den Artikeln 35 und 36 der DSGVO erfordern können

Hauptvorteile

RSA Archer Privacy Program Management wurde entwickelt, um Ihre Datenschutz- und/oder Rechtsteams zu unterstützen:

- Demonstration der Verantwortlichkeit und des Engagements für die DSGVO-Compliance im gesamten Unternehmen
- Konfiguration von Dashboards, um das Datenschutzprogramm effektiv zu überwachen
- Verbesserung des Verständnisses, der Transparenz und der Statusnachverfolgung für personenbezogene und vertrauliche Informationen mit Bewertungen der Datenidentifikation
- Durchführung konsistenter DPIAs und PIAs



Informationen über RSA

Die RSA Archer® Suite ermöglicht Unternehmen das umfassende Management von Geschäftsrisiken und das vertrauensvolle Ergreifen digitaler Chancen. Die Suite ist Teil des RSA-Portfolios von geschäftsorientierten Sicherheitslösungen, die einen einheitlichen Ansatz für das Management digitaler Risiken bieten, der sich durch integrierte Transparenz, automatisierte Einblicke und koordinierte Aktionen auszeichnet. RSA schützt Millionen von Nutzern auf der ganzen Welt und trägt dazu bei, dass mehr als 90 Prozent der Fortune 500-Unternehmen Erfolg haben und sich kontinuierlich an Informationsänderungen anpassen. Weitere Informationen finden Sie unter rsa.com/de-de.

