Informatica

Kurzdarstellung

Datenschutz – Privacy by Design: California Consumer Privacy Act

Wichtige Statistiken

- 69 Prozent der Verbraucher weltweit sind bereit, sich gegen Unternehmen zu stellen, die den Datenschutz ihrer Meinung nach nicht ernst nehmen.
- 62 Prozent der Verbraucher suchen die Schuld bei Verstößen gegen den Datenschutz bei Unternehmen – und nicht bei Hackern.
- 83 Prozent der Verbraucher in den USA tätigen einige Monate lang nach einer Datenschutzverletzung oder einem schweren Sicherheitsvorfall keine Geschäfte mit dem betroffenen Unternehmen.
- 21 Prozent der Verbraucher in den USA wenden sich permanent von einem Unternehmen ab, bei dem ein Datenverlust aufgetreten ist.[1]

Schnellere Compliance, um das Vertrauen Ihrer Kunden zu stärken und Unternehmensrisiken zu verringern

Die Bewohner von Kalifornien erhalten neue Rechte zu ihren personenbezogenen Daten und legen Anforderungen an den Datenschutz fest

Die Datenschutzvorschrift California Consumer Privacy Act (CCPA) gehört zu der weltweit steigenden Anzahl an Datenschutzbestimmungen, die Einzelpersonen bestimmte Rechte einräumen, so dass sie die Nutzung ihrer personenbezogenen Informationen besser kontrollieren können.

Die CCPA räumt Verbrauchern Rechte hinsichtlich des Umgangs mit ihren personenbezogenen Daten ein und verhindert, dass Unternehmen gegen Verbraucher vorgehen, die sich zur Ausübung dieser Rechte entscheiden. Insbesondere sind Verbraucher dazu berechtigt, nachzufragen, welche personenbezogenen Daten Unternehmen zu ihnen erfasst haben, in welche Kategorie sie fallen und für welchen Zweck sie verwendet werden. Verbraucher können Unternehmen anweisen, ihre personenbezogenen Daten zu löschen oder festlegen, dass ihre personenbezogenen Daten nicht an Dritte weiterverkauft werden dürfen. Die CCPA schreibt zudem vor, dass Unternehmen geeignete Prozesse und Richtlinien zum Datenschutz implementieren und verwalten, die für die Art der gesammelten Daten angemessen sind. Die Vorschrift sieht auch ein privates Klagerecht vor (mit hohen Bußgeldern für Unternehmen), sofern Verstöße dagegen vorliegen, die zu unbefugtem Zugriff auf personenbezogene Daten führen, die unter das kalifornische Recht zur Benachrichtigung von Verstößen fallen.

Wichtige Aspekte des Datenschutzes

Für Datenschutz und -sicherheit zuständige Teams benötigen automatisierte Tools, um die Einhaltung des Datenschutzes effektiv zu verwalten. Leider sind Datenschutzbeauftragte oft frustriert, da sie nicht in der Lage sind, personenbezogene Daten zu ermitteln, zu finden und abzurufen, die Zusammenarbeit zwischen Business-, Datenschutz- und IT-Teams zu fördern und personenbezogene Daten effektiv zu schützen und zu überwachen.

Die Datenschutzlösungen von Informatica® zielen auf die Schaffung einer Grundlage ab, um Datenschutzbestimmungen zu unterstützen und das Vertrauen der Datennutzer zu erhöhen. Indem Unternehmen Compliance-Anforderungen proaktiv verwalten, können sie sicherstellen, dass Datenrisiken (z. B. Datenmissbrauch oder Datenverlust) beseitigt und überwacht werden und dass Stakeholder effektiv zusammenarbeiten können, um den Anforderungen an Datenschutz, Audits und Reporting gerecht zu werden.

[1] https://www.infosecurity-magazine.com/news/fifth-consumers-never-return

Die Datenschutzlösungen von Informatica geben Unternehmen die Möglichkeit, (1) Data-Governance-Richtlinien zu verwalten, (2) personenbezogene und sensible Daten zu ermitteln und zu verwalten, (3) einzelne Identitäten mit personenbezogenen Daten zu verknüpfen, (4) Datenrisiken zu analysieren und nachzuverfolgen, (5) Maßnahmen zu ergreifen, um personenbezogene Informationen zu schützen und Anfragen und Zustimmungen von Datensubjekten zu verwalten und (6) die Verbesserung des Datenschutzes nachzuverfolgen und Datenschutzmaßnahmen und -status zu kommunizieren.

Compliance mit der CCPA ist alles andere als einfach. Daher benötigen Unternehmen bessere Erkenntnisse und müssen personenbezogene Daten besser schützen, um Bewohnern von Kalifornien (CA) den Grad an Kontrolle und Schutz zu gewährleisten, der ihnen laut CCPA zusteht. In der folgenden Tabelle werden wichtige Daten- und Sicherheitsaspekte aufgeführt, die erfüllt werden müssen, um CCPA-Compliance sicherzustellen:

Datenschutzanforderungen	Ergebnisse
1. Festlegen, wie unser Unternehmen personenbezogene Daten der Bewohner von Kalifornien verarbeitet (Data-Governance-Richtlinien)	• Definitionen erstellen, die für die personenbezogenen Daten der Bewohner von Kalifornien gelten • Festlegen, welche Daten erfasst und wie sie verwendet werden
2. Wo genau befinden sich personenbezogene Daten der Bewohner von Kalifornien? (Personenbezogene Daten ermitteln und klassifizieren)	• Ermitteln, wo genau sich personenbezogene Daten der Bewohner von Kalifornien befinden, insbesondere Daten, die unter das kalifornische Gesetz zur Benachrichtigung von Verstößen fallen
3. Verzeichnis mit Identitäten erstellen (so dass die Identitäten der Bewohner von Kalifornien mit ihren personenbezogenen Daten verknüpft werden)	• Schnell auf Anfragen zur Ausübung der Rechte von Bewohnern von Kalifornien reagieren • Schnell feststellen können, wo genau Daten im Unternehmen verbreitet werden
4. Festlegen, wie personenbezogene Daten der Bewohner von Kalifornien geschützt werden (dabei wird das Sicherheitsrisiko analysiert, dem die Daten der Bewohner von Kalifornien ausgesetzt sind)	• Nachvollziehen, an welchen Stellen die Gefahr besteht, dass Daten der Bewohner von Kalifornien missbraucht oder unbefugt abgerufen werden, Priorisieren und Planen von Abhilfemaßnahmen, insbesondere hinsichtlich Daten, die unter das kalifornische Gesetz zur Benachrichtigung von Verstößen fallen • Ermitteln, welcher Grad an Sicherheit für verschiedene Arten von Daten der Bewohner von Kalifornien erforderlich ist
5. Personenbezogene Daten der Bewohner von Kalifornien schützen und auf Anfragen zur Ausübung von Rechten reagieren (Datensicherheit, Verarbeitung von Rechten)	• Anfragen zu Datenlöschung und Datenverkauf unterstützen • Schutz der Daten der Bewohner von Kalifornien während des laufenden Betriebs, in der Entwicklungs-, Test- und Analytics-Phase
6. Fortschritte nachverfolgen und wissen, wie der aktuelle Grad an Compliance mit den Vorgaben der CCPA lautet (messen, kommunizieren, zusammenarbeiten)	• Auf Statusanfragen reagieren • Den Fortschritt des CCPA-Programms nachverfolgen

Informationen zu Informatica

Die digitale Transformation ändert unsere Erwartungshaltung hin zu besserem Service und schnellerer Lieferung zu geringeren Kosten. Unternehmen müssen sich neu orientieren, um wettbewerbsfähig zu bleiben. Dabei spielen Daten eine zentrale Rolle.

Als führender Anbieter für Enterprise Cloud Data Management unterstützt Informatica Sie dabei, sich als intelligenter Vorreiter zu etablieren – völlig unabhängig davon, in welcher Branche, Kategorie oder Nische Sie tätig sind. Wir ermöglichen es Ihnen, agiler zu werden, neue Wachstumsmöglichkeiten wahrzunehmen und Innovationen voranzutreiben. Informatica ist zu 100 % auf Daten fokussiert, und bietet Unternehmen vielseitige Lösungen, um sich am Markt durchzusetzen.

Wir laden Sie ein, das gesamte Angebot von Informatica zu erkunden – und das Potenzial der Daten zu nutzen um Ihre nächste intelligente Innovation auf den Weg zu bringen.

Die Datenschutzlösungen von Informatica basieren auf KI und der branchenführenden, intelligenten Datenplattform. Daher bieten sie zahlreiche Funktionen, um die datenzentrierten Vorgaben der CCPA zu erfüllen:

1. **Festlegung und Verwaltung von Data-Governance-Richtlinien**
   Data Governance, um Richtlinien, Verantwortlichkeiten, Prozesse und Datendefinitionen auf Geschäfts- und IT-Seite festzulegen, zu dokumentieren und zu messen. Mit dem Axon™ Governance Task Framework und visuellen Workflows können Unternehmen wichtige Business User ermitteln und sie mit den Daten und Prozessen in Beziehung setzen, deren Eigentümer sie sind.

2. **Ermittlung, Klassifizierung und Verständnis personenbezogener und sensibler Daten**
   Nutzung von KI, damit personenbezogene Daten und Metadaten in einer Unternehmensübersicht angezeigt und analysiert werden können, so dass Unternehmen schnell all ihre Datenumgebungen auffinden, klassifizieren und verstehen können sowie auch Multi-Cloud-Umgebungen, Hadoop, relationale und Dateispeichersysteme sowie strukturierte und unstrukturierte Daten.

3. **Verknüpfung von Identitäten**
   In dem Verzeichnis für Datensubjekte werden Identitäten mit personenbezogenen Daten verknüpft, so dass Unternehmen schnell ermitteln können, welche personenbezogenen Daten zu welcher Einzelperson gehören (Kunde, Mitarbeiter usw.). Dadurch können Zugriffsrechte von Datensubjekten einfacher unterstützt werden und zudem lässt sich diese Funktion in Systeme zum Consent Management integrieren.

4. **Analyse von Datenrisiken, Festlegung von Schutzmaßnahmen**
   Analyse des Risikos, dem personenbezogene Daten ausgesetzt sind (Wahrscheinlichkeit des Datenmissbrauchs oder des Datenverlusts). Es werden anpassbare Modelle zur den Auswirkungen von Risiken bereitgestellt, damit Unternehmen Abhilfemaßnahmen priorisieren und Ressourcen und Investitionen sinnvoll einsetzen können. Risiken werden kontinuierlich gemessen und aufgezeichnet, um wichtige Risikoindikatoren für Datenschutz- und -sicherheitsprogramme bereitzustellen.

5. **Schutz von Daten und Verwaltung der Rechte von Datensubjekten und Consent Management**
   Anonymisierung und Pseudonymisierung personenbezogener Daten, um sicherzustellen, dass Unternehmen Zugriff und Abruf der personenbezogenen Informationen von Kunden und Mitarbeitern kontrollieren können. Es wird eine 360-Grad-Ansicht der Daten von Datensubjekten und ihrer Zustimmungen erstellt, indem Data Lineage, historische Daten und Aufbewahrungsfristen erfasst und dokumentiert werden. Gleichzeitig werden die Rechte von Datensubjekten durch Workflows und Maßnahmen unterstützt.

6. **Messung, Kommunikation und Compliance mit Audit-Vorgaben**
   Umfassende Visualisierungsfunktionen sorgen für globale Datenerkenntnisse, um Entscheidungsträger zu unterstützen. Darüber hinaus werden detaillierte Ansichten für Datenexperten erstellt sowie sofortige Details zu personenbezogenen Daten, um Audit-Vorgaben hinsichtlich Datenschutz- und Datensicherheitsprogrammen zu verwalten und nachzuverfolgen.

Informatica

Worldwide Headquarters Ingersheimer Str. 10, 70499 Stuttgart Tel: +49 (0) 711 139 84-0 Gebührenfrei in den USA: 1.800.653.3871

IN08_0419_03601