elastic

Einsatz von Elastic zur Unterstützung der Einhaltung globaler Datenschutzgesetze

Zusammenfassung

Um in der modernen digitalen Welt erfolgreich zu sein, konzentrieren sich Unternehmen auf Daten, insbesondere auf deren Rolle in der KI.
Als Reaktion darauf verändert eine Vielzahl neuer Datenschutzgesetze und -vorschriften die globale Geschäftswelt. Die Einhaltung dieser regulatorischen Entwicklungen dient nicht nur der Risikominderung und -begrenzung, sondern ist auch ein entscheidender und wichtiger Wettbewerbsvorteil. Die Einhaltung der sich schnell ändernden gesetzlichen und regulatorischen Datenschutzbestimmungen kann das Vertrauen der Kunden stärken, das finanzielle Wachstum fördern und die operative Widerstandsfähigkeit verbessern.

Dieses Whitepaper stellt grundlegende Konzepte des Datenschutzrechts vor und zeigt, wie Unternehmen die leistungsstarke Plattform von Elastic einsetzen können, um nicht nur die geltenden Anforderungen an den Schutz personenbezogener Daten zu erfüllen, sondern diese auch schnell, effizient und sicher umzusetzen. Wir werden die sechs grundlegenden Datenschutzprinzipien vorstellen, die weltweit für Datenschutzbestimmungen gelten, und diese auf die Plattformlösungen von Elastic anwenden.
So unterstützen wir Unternehmen dabei, Datenschutz von einer Compliance-Verpflichtung in einen Wettbewerbsvorteil zu verwandeln.

Bitte beachten Sie: Dieses Whitepaper dient ausschließlich Informationszwecken und stellt keine Rechtsberatung dar. Bitte konsultieren Sie Ihren eigenen Rechtsberater, um rechtlichen Rat einzuholen.

Hintergrund und Einführung in das globale Datenschutzrecht

Globale Datenschutzgesetze stellen Unternehmen, die personenbezogene Daten erfassen, vor zunehmend komplexe Herausforderungen. Da personenbezogene Daten weithin als eines der wertvollsten Güter der Welt angesehen werden, kann die Einhaltung von Datenschutzgesetzen ein wichtiger Geschäftsfaktor für Unternehmen sein, während Verstöße gegen diese Gesetze das Wachstum eines Unternehmens erheblich beeinträchtigen können.

Angesichts der zunehmenden Erfassung personenbezogener Daten durch Unternehmen wird es immer wichtiger, eine skalierbare Lösung für die Verwaltung und den Schutz dieser Daten zu finden, um Verantwortlichkeit zu demonstrieren und sich in einer zunehmend datenschutzbewussten Welt einen guten Ruf als vertrauenswürdiger Anbieter aufzubauen.

Obwohl es Unterschiede zwischen verschiedenen Datenschutzgesetzen gibt, teilen viele von ihnen bestimmte übergeordnete Prinzipien.

Zu den wichtigsten Datenschutzgesetzen gehören:

- Die Datenschutz-Grundverordnung („DSGVO“) der EU und ihr Pendant im Vereinigten Königreich
- Datenschutzgesetze der US-Bundesstaaten, wie der California Consumer Privacy Act („CCPA“)
- Das brasilianische Datenschutzgesetz („LGPD“)
- Das kanadische Gesetz zum Schutz personenbezogener Daten und elektronischer Dokumente („PIPEDA“)
- Japans Gesetz zum Schutz personenbezogener Daten („APPI“)

Die Flexibilität und Skalierbarkeit des Plattformangebots von Elastic ermöglichen es Unternehmen, die Einhaltung dieser verschiedenen und komplexen gesetzlichen Anforderungen zu steuern und zu verwalten.

Personenbezogene Daten

Vorbei sind die Zeiten, in denen der Begriff „personenbezogene Daten“ auf offensichtliche Identifikatoren, wie vollständige Namen, E-Mail-Adressen, staatliche Kennungen und Telefonnummern, beschränkt war. Heutzutage definieren Datenschutzgesetze weltweit personenbezogene Daten weit gefasst, um alle Informationen zu erfassen, die mit einem bestimmten Gerät oder einer bestimmten Person in Verbindung gebracht werden können.

Eine sinnvolle Faustregel wäre, davon auszugehen, dass Datenschutzgesetze wahrscheinlich gelten, wenn Informationen mit einer eindeutigen Kennung einer Person verknüpft werden können. Durch die Allgegenwart von Smartphones, IoT-Geräten und anderen Computergeräten im Alltag hat die Erfassung personenbezogener Daten in Unternehmen aller Branchen erheblich zugenommen. Dadurch besteht ein dringender und unbestreitbarer Bedarf an Produkten und Dienstleistungen, die es Unternehmen ermöglichen, die Verarbeitung solcher Daten zuverlässig zu verwalten.

Verantwortliche und Auftragsverarbeiter

Datenschutzgesetze weltweit erlegen Unternehmen in der Regel unterschiedliche – jedoch häufig sich überschneidende – Verpflichtungen auf, je nachdem, ob sie als „Verantwortlicher“ oder als „Auftragsverarbeiter“ personenbezogener Daten agieren.

- **Controller** (auch als „Unternehmen“ im Sinne des CCPA bezeichnet) bestimmen Zweck und Mittel der Verarbeitung personenbezogener Daten. Sie sind die Stellen, die unabhängige Entscheidungen darüber treffen, welche personenbezogenen Daten sie erheben und wie sie diese verarbeiten.
- **Prozessoren** (im CCPA auch als „Dienstleister“ bezeichnet) erbringen Dienstleistungen für einen vorgelagerten Verantwortlichen (oder manchmal auch für einen anderen Verarbeiter) und dürfen personenbezogene Daten ausschließlich in strikter Übereinstimmung mit den Anweisungen des Verantwortlichen zum Zwecke der Erbringung von Dienstleistungen für den Verantwortlichen verarbeiten.

Obwohl für Verantwortliche und Auftragsverarbeiter unterschiedliche Verpflichtungen gelten, erfordert die Einhaltung der Vorschriften in jeder Rolle ein Verständnis der Arten von personenbezogenen Daten, die verarbeitet werden, sowie die Fähigkeit, personenbezogene Daten gezielt, skalierbar und effizient zu lokalisieren.

Die meisten Datenschutzgesetze weltweit ermächtigen Personen auch, bestimmte Rechte in Bezug auf ihre Daten auszuüben, wie etwa Zugriff, Löschung und Berichtigung. Angesichts relativ kurzer Reaktionszeiten trägt die Verwendung einer Plattform wie Elastic zum effizienten Durchsuchen unstrukturierter und strukturierter Datensätze nicht nur zur Optimierung der Compliance bei, sondern verringert auch das Risiko behördlicher Untersuchungen und zivilrechtlicher Verfahren.

Grundlegende Datenschutzprinzipien

Globale Datenschutzgesetze basieren oft auf grundlegenden Datenschutzprinzipien. Auf hoher Ebene sind das:

1

Hinweis

Datenschutzgesetze schreiben vor, dass Unternehmen genaue und aktuelle Informationen über ihre Datenschutzpraktiken bereitstellen müssen.

2

Datenschutz durch Design

Die Datenschutzgesetze verlangen von Unternehmen, dass sie sich Gedanken darüber machen, wie sich ihre Praktiken auf die Datenschutzrechte und die Interessen von Einzelpersonen auswirken können, und dass sie ihre Produkte so gestalten, dass sie diesen Gesetzen entsprechen.

3

Rechte

Datenschutzgesetze gewähren Einzelpersonen bestimmte Rechte in Bezug auf ihre personenbezogenen Daten, darunter das Recht auf Auskunft, Löschung und Berichtigung ihrer Daten.

4

Datenminimierung

Datenschutzgesetze verlangen von Unternehmen, dass sie Datenminimierung praktizieren (d. h. nur die personenbezogenen Daten erheben und verarbeiten, die für die geschäftlichen Zwecke, für die sie erhoben wurden, erforderlich sind) und Aufbewahrungsfristen und Löschrichtlinien festlegen, um sicherzustellen, dass Unternehmen keine Daten aufbewahren, die sie nicht benötigen.

5

Sicherheit

Datenschutzgesetze schreiben bestimmte Sicherheitsstandards zum Schutz personenbezogener Daten vor.

6

Benachrichtigung über eine Datensicherheitsverletzung

Datenschutz- und Sicherheitsgesetze verpflichten Unternehmen, die von einem Sicherheitsvorfall oder einer Datenverletzung betroffen sind, die sich auf personenbezogene Daten auswirkt, zur Erfüllung einer Reihe von Verpflichtungen.

Die Kosten der Nichteinhaltung

Die Nichteinhaltung von Datenschutzgesetzen kann zu hohen Strafen, Anwaltskosten und Reputationsschäden führen. Regulatorische Strafen im Rahmen von Vorschriften wie der DSGVO und dem CCPA können erheblich sein und sich erheblich auf das Geschäftsergebnis eines Unternehmens auswirken. Darüber hinaus können Zivilkläger Ansprüche wegen Datenschutzverletzungen geltend machen, einschließlich Sammelklagen nach Datenschutzverletzungen.

Laut einem Bericht von IBM Security und dem Ponemon Institute betrugen die durchschnittlichen Kosten einer Datenschutzverletzung im Jahr 2024 4,88 Millionen US-Dollar, was einem Anstieg von 10 % gegenüber dem Vorjahr entspricht.
Der Bericht von AON ergab, dass 56 stark beachtete Cyber-Ereignisse im Jahr 2024 durchschnittlich zu Kursverlusten von 27 % für die betroffenen Unternehmen führten. Es ist offensichtlich, dass eine solche Schädigung des Rufs ebenfalls irreversible Auswirkungen auf den Wettbewerbsvorteil eines Unternehmens haben kann. In diesem Umfeld ist Compliance nicht nur ein Kostenfaktor, sondern eine strategische Investition.

Einsatz von Elastic für Ihre Anforderungen hinsichtlich der datenschutzrechtlichen Compliance

Elastic unterstützt Unternehmen dabei, mit offenen und flexiblen Unternehmenslösungen relevante Antworten in beispielloser Geschwindigkeit zu finden. Die Einhaltung der Datenschutzgesetze weltweit erfordert ein umfassendes Verständnis Ihres gesamten Datenökosystems: wo sich personenbezogene Daten befinden, wie sie übertragen werden und wie diese Daten anderweitig verarbeitet werden. Hier zeichnet sich die Elasticsearch-Plattform aus, indem sie diese Prozesse vereinfacht und automatisiert und so eine nahtlose Compliance gewährleistet.
Im Folgenden erläutern wir den Nutzen von Elastic im Hinblick auf die sechs oben erläuterten grundlegenden Datenschutzprinzipien.

Hinweis

Die Datenmapping-Funktionen von Elastic ermöglichen es Unternehmen, den Umfang und die Arten von personenbezogenen Daten auf allen Unternehmensservern und darüber hinaus zu erfassen.

Die Benachrichtigung ist ein grundlegendes Prinzip der Datenschutzgesetze. Einzelpersonen haben das Recht, zu erfahren, welche Arten von personenbezogenen Daten ein Unternehmen über sie sammelt, zu welchen Zwecken diese Daten erfasst werden und unter welchen Umständen ihre Daten an Dritte weitergegeben werden. Datenschutzgesetze verlangen von Unternehmen häufig, dass sie umfassende Datenschutzrichtlinien bereitstellen, wie beispielsweise die Datenschutzerklärung von Elastic selbst, in der diese Konzepte erläutert werden, wie dies im Elastic Trust Center der Fall ist.

Um diesem Grundsatz der Benachrichtigung nachzukommen, muss ein Unternehmen den Umfang der von ihm erhobenen personenbezogenen Daten verstehen.
Dies erfordert ein robustes Daten-Mapping, also einen systematischen Prozess, der alle personenbezogenen Datenflüsse innerhalb eines Unternehmens identifiziert und dokumentiert.

Ohne eine skalierbare Lösung sind Unternehmen häufig auf eine Vielzahl veralteter Tabellenkalkulationen, Antworten auf Dateninventarumfragen und zufällige Befragungen verschiedener Geschäftsbereiche angewiesen, um zu ermitteln, welche personenbezogenen Daten erfasst werden und wie diese innerhalb und außerhalb des Unternehmens weitergegeben werden.

Im besten Fall sind Aufzeichnungen zu einem bestimmten Zeitpunkt korrekt, leiden jedoch unter den Anforderungen der Datenerfassung und -verarbeitung in einer datengesteuerten Wirtschaft.

Elastic kann Unternehmen dabei unterstützen, wichtige Erkenntnisse zu gewinnen, um ihre Datenmapping-Prozesse zu verbessern. Ohne Kenntnis darüber, welche Arten von personenbezogenen Daten erhoben werden, wo diese Daten gespeichert sind und an wen sie weitergegeben werden, kann ein Unternehmen die Einhaltung der Datenschutzgesetze nicht gewährleisten. Durch die Indizierung von Informationen über Ihre Datenflüsse in Elastic ermöglichen die leistungsstarken Volltextsuchfunktionen eine schnelle Identifizierung von Anwendungen, Tabellen, Abfragen oder Berichten, die auf personenbezogenen Daten basieren.

Die Verwendung von Elastic zur Optimierung des Datenmappings hilft Unternehmen auch dabei, vertragliche Verpflichtungen aus Datenschutzgesetzen zu erfüllen, da identifizierte Datenflüsse bestimmen, mit welchen anderen Parteien ein Unternehmen einen Datenschutzzusatz, Datenübertragungsmechanismen oder andere Vereinbarungen zum Schutz personenbezogener Daten abschließen sollte. Ebenso können sich die heutigen Lieferketten auf Hunderte oder Tausende von Anbietern und Unterauftragsverarbeitern erstrecken. Die Möglichkeit, Tausende von Vereinbarungen im Handumdrehen zu indexieren und eine Volltextsuche durchzuführen, kann auch die Erstellung von Lieferantenstatusberichten erleichtern und, was noch wichtiger ist, proaktive Lieferantenmanagementprogramme ermöglichen.

Datenschutz durch Design

Unternehmen können Elastic nutzen, um den Datenschutz durch Technikgestaltung zu verbessern, einschließlich der Implementierung von Prinzipien zur Datenminimierung.

Wenn ein Unternehmen erwägt, Elastic als Datenspeicher für personenbezogene Daten zu verwenden, können die Funktionen von Elastic Cloud Enterprise („ECE“), der zentralen Orchestrierungssoftware von Elastic, das Unternehmen von Anfang an auf den richtigen Weg bringen. Das Prinzip des eingebauten Datenschutzes besteht darin, personenbezogene Daten wie ein wertvolles Gut zu behandeln, indem der Zugriff darauf beschränkt, die Richtigkeit gewährleistet, angemessene Datensicherheitskontrollen durchgeführt und die Aufbewahrungsfristen begrenzt werden.

Im Gegensatz zu herkömmlichen Datenarchitekturen mit einem einzigen massiven Datenspeicher und einer Vielzahl komplexer, sich überschneidender Datenzugriffskontrollen (die erforderlich sind, um verschiedenen Projekten nur Zugriff auf bestimmte Daten zu gewähren) ermöglicht Elastic den Benutzern, für jedes Projekt neue Elasticsearch-Cluster zu instanziieren und nur die für dieses Projekt relevanten Daten in den Cluster aufzunehmen.

Diese verteilte Architektur ermöglicht die Minimierung personenbezogener Daten – ein weiteres zentrales Datenschutzprinzip. Beispielsweise können Kunden Elastic verwenden, um Daten in Speicherebenen zu kategorisieren, wobei Zugriffsprotokollinformationen von Elastic Unternehmen dabei unterstützen können, ungenutzte Daten zu identifizieren, um Richtlinien und Praktiken zur Datenaufbewahrung zu optimieren.

Elastic ermöglicht es Unternehmen außerdem, zu verstehen, wann und wie Datenschutz-Folgenabschätzungen („DPIAs“) durchgeführt werden sollten. Gemäß der DSGVO und ähnlichen Datenschutzbestimmungen ist eine Datenschutz-Folgenabschätzung eine teilweise obligatorische Bewertung, mit der sichergestellt wird, dass Sie personenbezogene Daten verantwortungsbewusst verarbeiten und mögliche Schäden für Einzelpersonen minimieren. Das Wissen darüber, wo sich Daten befinden, wie sie verarbeitet werden und wohin sie fließen, vereinfacht die Durchführung von Datenschutz-Folgenabschätzungen, die traditionell multifunktionale Unterstützung über Geschäftsbereiche hinweg erfordern können, um die Verwendung personenbezogener Daten zu verstehen. Datenschutz-Folgenabschätzungen (DPIAs) demonstrieren grundlegende Compliance und ermöglichen es Unternehmen gleichzeitig, die Verarbeitung personenbezogener Daten auf das zu beschränken, was gemäß den globalen Datenschutzgesetzen zulässig ist.

Rechte der betroffenen Personen

Unternehmen können Elastic nutzen, um relevante personenbezogene Daten zu identifizieren, die Anwendbarkeit von Rechten zu bewerten und Anfragen zu erfüllen.

Globale Datenschutzgesetze geben Einzelpersonen bestimmte Wahlmöglichkeiten hinsichtlich der Verarbeitung ihrer personenbezogenen Daten. Dazu gehören in der Regel das Recht auf Zugang, Löschung und Berichtigung personenbezogener Daten sowie das Recht auf Widerspruch gegen bestimmte Arten der Verarbeitung personenbezogener Daten. Die Elastic Datenmapping-Funktionen bilden das Kernfundament, mit dem Unternehmen Anfragen von betroffenen Personen bearbeiten können.

- **Zugriff:** Mit Elasticsearch können Unternehmen Datenspeicher durchsuchen, um personenbezogene Daten im gesamten Unternehmen zu identifizieren, einschließlich der Tabellen, Abfragen, Berichte oder Anwendungen, die auf personenbezogenen Daten basieren. Unternehmen können Elastic auch zur Unterstützung von Suchfunktionen für Endbenutzer einsetzen, sodass diese nach ihren eigenen Benutzerdaten suchen können. Durch die Bereitstellung leistungsstarker Suchfunktionen für Endbenutzer wird der Bedarf an Kundensupport reduziert, da Endbenutzer ihre Daten mit Self-Service-Tools identifizieren und exportieren können. Wenn Self-Service-Tools nicht ausreichen, ermöglicht Elastic Unternehmen die schnelle Suche in ihren eigenen Datenspeichern, um Auskunftsersuchen von betroffenen Personen nachzukommen.

- **Löschung:** Nachdem ein Unternehmen mit Elastic die über eine Person gespeicherten personenbezogenen Daten identifiziert hat, kann es Elastic weiter nutzen, um diese Daten zu transformieren, einschließlich der Kennzeichnung von Daten zur Aufbewahrung unter einer Löschungsausnahme, der dauerhaften Löschung von Daten und der Verwendung anderer Löschtechniken, die nach den Datenschutzgesetzen zulässig sind, einschließlich der Anonymisierung und bestimmter Arten der Pseudonymisierung personenbezogener Daten. Durch die Verwendung von Elastic zur schnellen und kostengünstigen Umwandlung personenbezogener Daten können Unternehmen die Einhaltung von Vorschriften gewährleisten, behördliche Kontrollen vermeiden und die Nutzbarkeit von Daten im Rahmen der globalen Datenschutzgesetze aufrechterhalten.
- **Korrektur:** Ebenso erlauben Datenschutzgesetze oft Einzelpersonen, eine Korrektur ihrer persönlichen Daten zu beantragen. Elastic kann personenbezogene Daten über eine Person isolieren, damit das Unternehmen sich auf die Bearbeitung der Anfrage konzentrieren kann – nicht darauf, die Daten zu finden.
- **Beschränkungen:** Einige Datenschutzgesetze wie die DSGVO und ihr britisches Pendant enthalten auch ein Widerspruchsrecht oder ein Recht auf Einschränkung der Verarbeitung personenbezogener Daten. Unternehmen können die Datenzuordnungs- und Datenkategorisierungsfunktionen von Elastic nutzen, um schnell zu ermitteln, wie sie auf solche Anfragen reagieren und die Zugriffs- und Nutzungsberechtigungen entsprechend einschränken können. Dadurch sparen sie wertvolle Zeit, sodass Compliance-Teams innerhalb der durch diese Gesetze vorgegebenen kurzen Fristen reagieren können.

Datenminimierung

Wie bereits im Abschnitt *Datenschutz durch Technikgestaltung* erwähnt, unterstützt Elastic Unternehmen bei der Umsetzung von Datenminimierungsfunktionen. Die Grundsätze der Datenminimierung verlangen, dass Unternehmen personenbezogene Daten nur in dem Umfang erheben, verarbeiten und speichern, wie es für die Erreichung der autorisierten Verarbeitungszwecke des Unternehmens erforderlich ist.

Eine Möglichkeit, die Verarbeitung personenbezogener Daten zu minimieren, um dieser Verpflichtung nachzukommen, ist beispielsweise die **Pseudonymisierung** (d. h. das Ersetzen personenbezogener Identifikatoren in Daten durch Platzhalterwerte) oder die **Anonymisierung** (d. h. das vollständige Entfernen personenbezogener Identifikatoren aus Daten, sodass eine Person nicht mehr identifiziert werden kann). Erfahren Sie, wie eine führende europäische Fluggesellschaft die Elastic Ingest Pipeline nutzt, um sensible Daten vor der Speicherung zu verschleiern. Solche Ergebnisse können mit Logstash erzielt werden, einer verfügbaren Integration in Elastic, die Daten aus einer Vielzahl von Quellen aufnimmt, um die Umwandlung solcher Daten – einschließlich Anonymisierung und Pseudonymisierung – zu erleichtern und so die Ziele der Datenminimierung voranzutreiben und Datensicherheitsrisiken zu verringern.

Durch den Einsatz von Elastic für das Datenmapping und die Datenprüfung können Unternehmen außerdem ihre tatsächliche Nutzung gespeicherter personenbezogener Daten genauer analysieren und so die Aufbewahrungsfristen und -richtlinien für Daten effektiver anpassen.

Sicherheit und Benachrichtigung bei Verstößen

Weitere Informationen darüber, wie Elastic Unternehmen dabei helfen kann, ihre personenbezogenen Daten zu schützen und im Falle einer Datenschutzverletzung schnell zu reagieren, finden Sie in unserem Security White Paper.

Fazit

Der Datenschutz ist nicht nur eine gesetzliche Vorschrift, sondern eine geschäftliche Notwendigkeit. Angesichts hoher Geldstrafen, Betriebsunterbrechungen, Reputationsschäden und des drohenden Vertrauensverlusts der Kunden benötigen Unternehmen eine zuverlässige und skalierbare Methode, um ihre Daten zu erfassen, zu kategorisieren, zu verwalten, zu transformieren, zu analysieren und zu löschen. Elastic optimiert jeden Schritt dieses Prozesses und bietet die Skalierbarkeit und Leistung, die Ihr Unternehmen für Compliance und Kundenvertrauen benötigt.

