okta

Ihr Einstieg in die Datenschutz-Grundverordnung (DSGVO) mit Okta

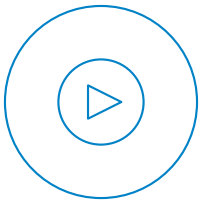
Okta Deutschland
Oskar-von-Miller-Ring 20
80333 München

info_germany@okta.com
+49 (89) 26203329

Haftungsausschluss

Obwohl sich dieser Artikel mit Rechtsfragen beschäftigt, stellt er keine Rechtsberatung dar. Wenn Sie oder Ihr Unternehmen Rechtsberatung benötigen, wenden Sie sich bitte an einen Anwalt oder die Rechtsabteilung Ihres Unternehmens.

Inhaltsverzeichnis



Einführung

Unternehmen, die in direktem Kontakt mit Verbrauchern stehen, verarbeiten seit Langem teils sensible personenbezogene Daten, vom Namen des Kunden bis hin zu Kreditkartennummern und Privatadressen. Aber aufgrund der ständig wachsenden Zahl an Datenschutzverstößen, Datenschutzbedenken und Fällen von Datenmissbrauch sah sich der Gesetzgeber veranlasst, das Datenschutzrecht zu verschärfen. In der Europäischen Union war die Datenschutz-Grundverordnung (DSGVO) der erste Schritt, um einen neuen Standard für den Datenschutz zu setzen. Im Zuge der laufenden Umsetzung der neuen Datenschutzvorgaben, die längst zur Chefsache geworden ist, müssen Unternehmen die Zukunftssicherheit ihrer IT-Infrastruktur genauer unter die Lupe nehmen.

Teil I: Die DSGVO und ihre wirtschaftlichen Auswirkungen

Grundsätzlich geht es bei der DSGVO um die Rechte von Personen als Eigentümer ihrer Daten. Dies kann sich praktisch in einer Vielzahl von Aspekten auswirken, etwa in dem Recht auf Auskunft darüber, welche Arten von personenbezogenen Daten von Unternehmen gesammelt werden, bis hin zum Recht auf Löschung dieser Daten. Im Zeitalter verschärfter Datenschutzbestimmungen und hoher Bußgelder müssen Unternehmen den Compliance-Ansatz ihrer IT-Infrastruktur überdenken.

Angesichts der Zunahme massiver Fälle von Datenschutzverletzungen wie bei Marriott und Panera Bread im Jahr 2018 werden neue Bestimmungen zum Schutz personenbezogener Daten wie die DSGVO durchgesetzt. Weil diese Verstöße heute stärker wahrgenommen werden, ist der Verlust des individuellen Vertrauens direkt mit der Kundenstimmung verbunden. Das wiederum wirkt sich auf den Umsatz aus: Laut IBM erlitten 46 % der Unternehmen durch Vertrauensbrüche einen Reputations- und Markenwertschaden. Darüber hinaus kann ein Verstoß gegen die DSGVO zu Geldbußen von bis zu 20 Mio. Euro oder 4 % des weltweiten Umsatzes führen. In Zukunft müssen Unternehmen sorgfältig neue Kontrollen und Prozesse implementieren, um diese Vorschriften einzuhalten.

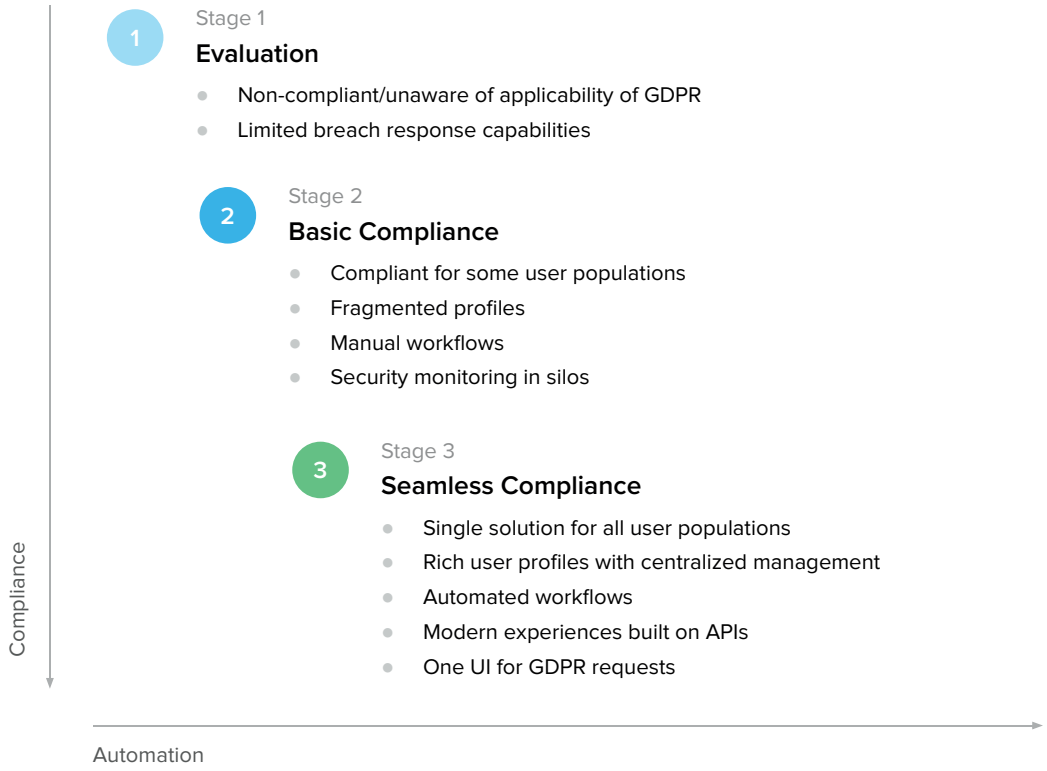
Die irische Datenschutzkommission und die künftige Durchsetzung der Vorschriften

Die irische Datenschutzkommission (Data Protection Commission of Ireland, DPC), die nationale unabhängige Behörde, die für die Wahrung des Grundrechts von Einzelpersonen in der EU auf Schutz ihrer personenbezogenen Daten zuständig ist, hat die Durchsetzung der DSGVO vorangetrieben. 80 Fälle von Verstößen gegen die DSGVO hatte die DPC bis Oktober 2018 eröffnet, darunter ein behördliches Ermittlungsverfahren, in dem die Einhaltung der einschlägigen Bestimmungen der DSGVO durch Facebook untersucht wurde.

Teil II: Der Weg zur Compliance

Da die DPC und andere ähnliche Datenschutzbehörden die Durchsetzung der DSGVO vorantreiben, sollten IT-Führungskräfte den Stand der Umsetzung in ihren Unternehmen prüfen. Abgesehen von der aktuellen Durchsetzung könnten aber auch Unternehmen, die die geltenden Vorschriften heute einhalten, in Zukunft Schwierigkeiten mit der laufenden Umsetzung haben. Die DSGVO-Umsetzung ist nämlich ein kontinuierlicher Prozess mit verschiedenen Compliance-Phasen.

GDPR Maturity Curve



Da die DPC und andere ähnliche Datenschutzbehörden die Durchsetzung der DSGVO vorantreiben, sollten IT-Führungskräfte den Stand der Umsetzung in ihren Unternehmen prüfen. Abgesehen von der aktuellen Durchsetzung könnten aber auch Unternehmen, die die geltenden Vorschriften heute einhalten, in Zukunft Schwierigkeiten mit der laufenden Umsetzung haben. Die DSGVO-Umsetzung ist nämlich ein kontinuierlicher Prozess mit verschiedenen Compliance-Phasen.

Stufe 1: Unternehmen, die ganz am Anfang des Weges zur Compliance stehen

Seit dem Inkrafttreten der DSGVO im Mai 2018 haben sich die meisten Unternehmen im Geltungsbereich der DSGVO um die Umsetzung der Vorschriften bemüht. Es gibt jedoch einen beträchtlichen Teil von Unternehmen, denen vielleicht nicht bewusst war, dass die DSGVO auf sie anwendbar ist. Nennen wir sie Unternehmen der „Stufe 1“.

Gemäß Artikel 3 der DSGVO muss ein Unternehmen die Anforderungen erfüllen, wenn folgende Bedingungen zutreffen:

- **Es ist Datenverantwortlicher oder Auftragsverarbeiter in der EU,**
- **es bietet betroffenen Personen in der EU Waren und Dienstleistungen an oder**
- **es beobachtet das Verhalten betroffener Personen in der EU.**

Die Formulierung in Artikel 3 der DSGVO erweitert die Anwendbarkeit der DSGVO im weiteren Sinne auf Unternehmen, die die Anwendung ausländischen Rechts nicht erwarten würden, denn sie gilt auch für Unternehmen, die Dienstleister sind, Waren und Dienstleistungen für betroffene Personen in der EU anbieten oder das Verhalten von betroffenen Personen in der EU „beobachten“. Darüber hinaus ist die Definition von personenbezogenen Daten im Rahmen der DSGVO so weit gefasst, dass sie eine Vielzahl von Datentypen umfasst, von Beiträgen in sozialen Medien bis hin zu Kreditkartendaten, die bei der Buchung einer Fluggesellschaft erhoben werden. Da die Definition personenbezogener Daten eine so große Vielfalt von Daten umfasst, ist den Unternehmen oft nicht klar, ob die DSGVO für ihre Datenerhebung gilt. Dies führt dazu, dass viele Unternehmen nicht wissen, dass die DSGVO auf sie anwendbar ist und sie die rechtlichen Vorgaben einhalten müssen.

Stufe 2: Unternehmen, die manuelle Compliance-Prozesse einsetzen

Unternehmen auf dieser Stufe der Datenschutzumsetzung sind sich der Anwendbarkeit der DSGVO bewusst und haben die Umsetzung vielleicht durch manuelle Prozesse erreicht. Je nach Art des Unternehmens führt dies dazu, dass übermäßig viele IT-, Rechts-, Support- und Engineering-Ressourcen durch Compliance-Fragen und dem Aufwand der manuellen Konfiguration verschiedener Systeme gebunden sind. Laut Forbes haben die DSGVO-Kosten in den USA und Großbritannien 8 Milliarden Dollar erreicht, wobei diese Mittel für Rechtsanwälte, Berater und Datenschutzbeauftragte aufgewendet wurden. Da bei Unternehmen immer mehr Anfragen eingehen (zum Beispiel im Zusammenhang mit dem Recht auf Vergessenwerden), werden IT-Administratoren und Helpdesk-Mitarbeiter mehr Arbeitszeit für diese Randaufgabe benötigen, um die Konformität zu gewährleisten, statt ihren Kernaufgaben nachzukommen.

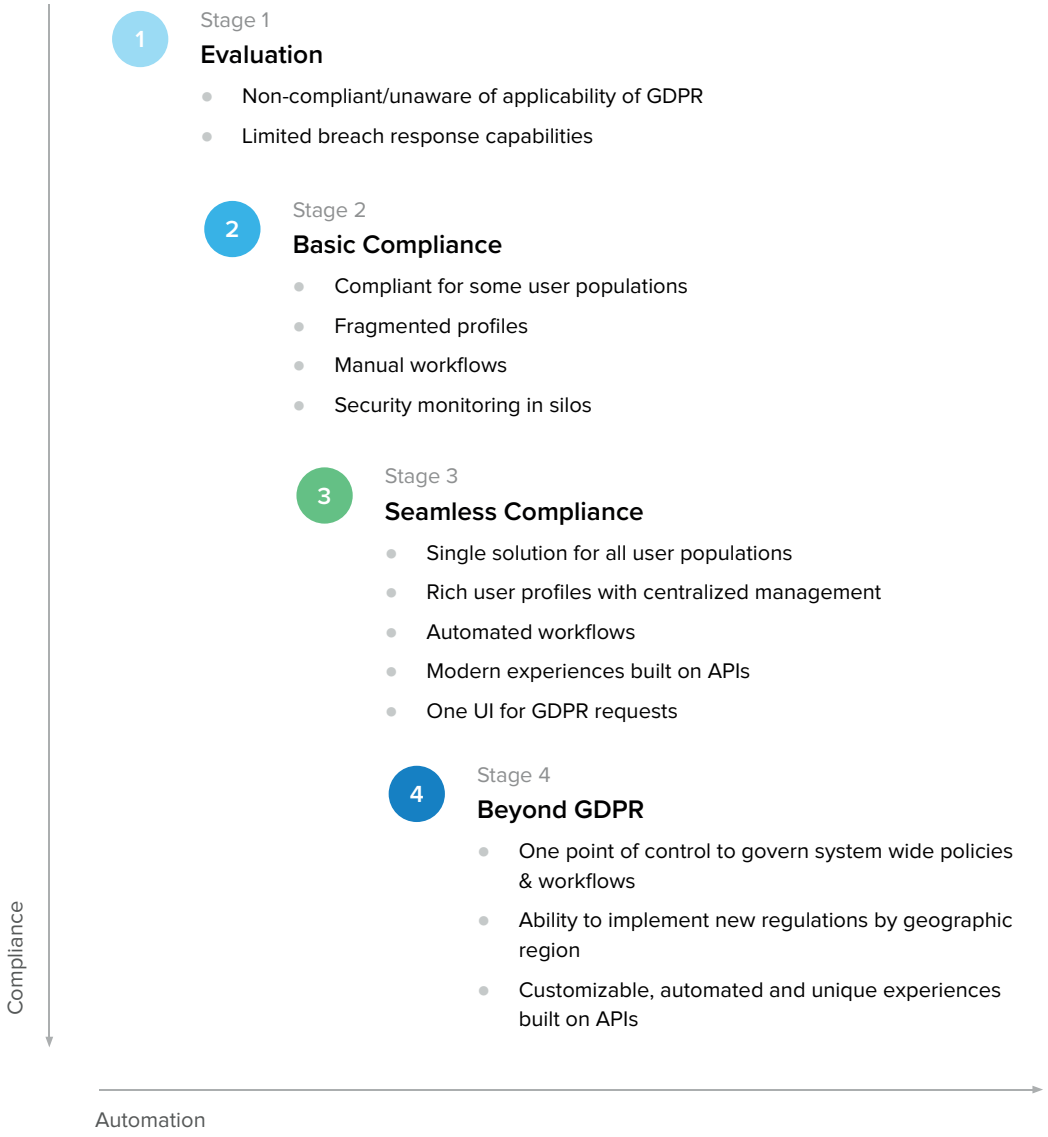
Einige Unternehmen auf dieser Stufe haben möglicherweise nur an die Compliance ihrer eigenen Mitarbeiter gedacht, nicht aber an Compliance-Prozesse, die für Verbraucher eingerichtet werden müssen. Dies ist ein wachsendes Problem, denn Unternehmen wie Google erhalten 2,4 Millionen Anfragen auf Vergessenwerden und können nur 43 % der Anfragen beantworten. 89 % dieser Anfragen kamen zudem von Privatpersonen, was auf ein wachsendes Interesse an Privatsphäre seitens der Verbraucher schließen lässt.

Stufe 3: Unternehmen, die Software zur Einhaltung der DSGVO im Rahmen der digitalen Transformation einsetzen

Unternehmen auf dieser Stufe setzen Software für Compliance ein, darunter eine moderne Identitätsmanagementlösung zur Automatisierung sich wiederholender Arbeitsabläufe. Indem die Umsetzung von Teilen der DSGVO wie das Recht auf Löschung und das Auskunftsrecht als Frage der Erteilung und des Entzugs von Zugangsrechten behandelt werden, können Unternehmen Lösungen wie ein Lifecycle Management nutzen, um die Arbeit der IT-Administratoren zu erleichtern. Die Funktionen werden durch die Verwendung von Identitätsmanagement- und Zugriffskonzepten wie nachgelagerte App-Steuerung und Sicherheitsrichtlinien zur Umsetzung der Compliance erweitert.

Stufe 4: Unternehmen mir einer Identitätsmanagementplattform, die sich dynamisch an Datenschutzgesetze anpasst

GDPR Maturity Curve



Von der DSGVO in der Europäischen Union über den Privacy Act in Australien bis hin zum CCPA in Kalifornien ist eine globale Regulierungswelle zu beobachten: Der Datenschutz wird für IT-Organisationen weltweit immer mehr zu einer expliziten Aufgabe, weil sie mit der Frage konfrontiert sind, wie sich ein konstanter Strom von Datenschutzbestimmungen bewältigen lässt. Darüber hinaus sollten größere Unternehmen im Zuge der Globalisierung eine anpassungsfähige und flexible Identitätsmanagementlösung für die laufende Einhaltung der jeweiligen Vorschriften in verschiedenen Ländern in Betracht ziehen. Abbildung 1 zeigt, dass für Kunden weltweit unterschiedliche Datenschutzstandards gelten, wobei jedes Land seinen eigenen Ansatz verfolgt.

Aber wichtiger als der Einsatz verschiedener Tools zur Realisierung eines modernen Identitätsmanagements ist der unvermeidliche Übergang zu einer Identitätsmanagementplattform. Der nächste Schritt des Compliance-Managements besteht darin, einen zentralen Kontrollpunkt zur Steuerung systemweiter Richtlinien und Workflows einzurichten.

Teil III: Kundenidentität und Compliance

Durch die Automatisierung in Form einer modernen Identitätsmanagementlösung können Unternehmen ihren Pflichten im Rahmen der DSGVO besser nachkommen, da die Kundenidentität im Mittelpunkt steht. Wenn wir die DSGVO als identitätsbezogene Aufgabe betrachten, können wir entsprechende Produkte einsetzen, um Compliance-Probleme zu lösen. Betrachten wir nun die Werkzeuge, die wir einsetzen können, und die entsprechenden Anforderungen der DSGVO.

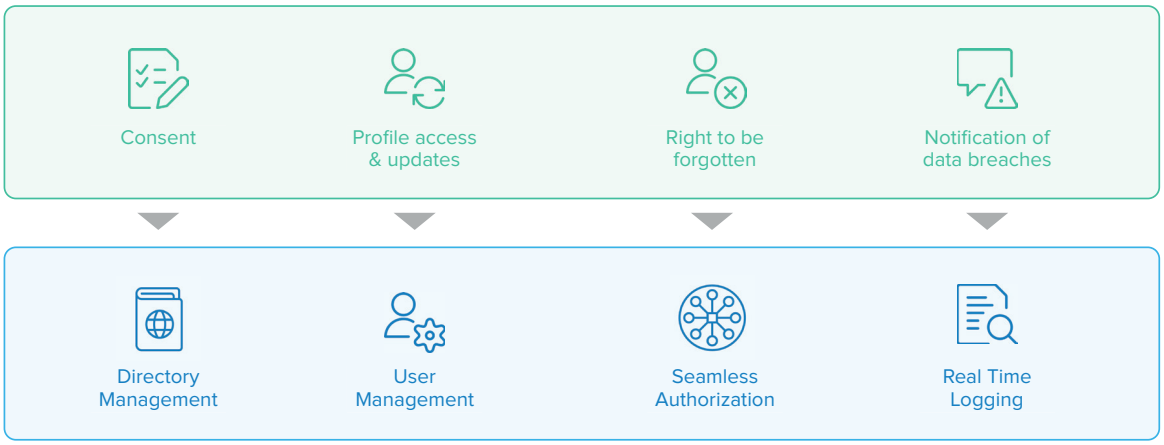


Abbildung 2

Aus Abbildung 2 ist ersichtlich, dass vier Produkte einen DSGVO-Bezug haben:

- **Universal Directory – ein zentralisierter Speicher für alle Benutzer; kann Profil- und Einwilligungsattribute speichern.**
- **Lifecycle Management – Automatisieren der nachgelagerten Maßnahmen, sobald ein Kunde tätig wird.**
- **API Access Management – Verwaltung von Genehmigungen und Geltungsbereichen für nachgelagerte Anwendungen.**
- **Echzeit-Logging – Verwenden eines Syslog, um einen Audit-Trail für die Einhaltung der Vorschriften zu erstellen.**

Dem lassen sich vier wichtigen DSGVO-Anforderungen zuordnen:

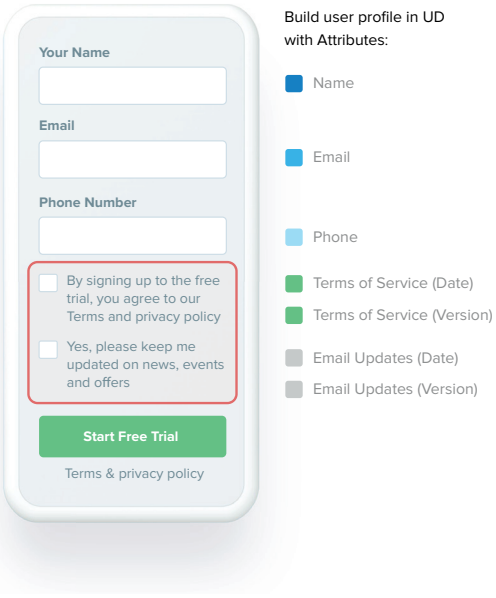
- Einwilligung — Artikel 6 und 7 der DSGVO
- Datenzugriffsrechte und Berichtigungsrecht — Artikel 15, 20 und 40 der DSGVO
- Recht auf Vergessenwerden — Artikel 17 der DSGVO
- Meldung von Datenschutzverstößen — Artikel 33 und 34 der DSGVO

Durch die Analyse jeder Anforderung und die Zuordnung der Produktfunktionalitäten zu den Datenschutzverpflichtungen können Unternehmen die ersten Schritte unternehmen, um eine Identitätsmanagementlösung zur Erfüllung ihrer Pflichten zu nutzen. In den folgenden Abschnitten werden wir einen tieferen Einblick in einzelne Artikel der DSGVO geben und beschreiben, wie Sie Okta nutzen können, um die Anforderungen zu erfüllen.

So lässt sich Okta für die Verwaltung von Einwilligungen nutzen

Artikel 6 der DSGVO legt die Bedingungen bzw. Rechtsgrundlagen fest, die es Unternehmen gestatten, personenbezogene Daten zu verarbeiten. Eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten ist die Einwilligung in die Datenverarbeitung für bestimmte Zwecke. Die spezifischen Bedingungen für eine gültige Einwilligung sind in Artikel 7 beschrieben: Ein gängiger Fall, in dem ein Unternehmen eine Einwilligung einholen muss, ist die Registrierung einer mobilen Kalenderanwendung. Bei Okta speichern wir die Einwilligung als Attribut im Universal Directory. Im nächsten Abschnitt betrachten wir eine Musterregistrierung für eine Kalenderanwendung an, um zu zeigen, wie Okta beim Einwilligungsmanagement hilft.

Registrierung für Kalender-App



Registrierung

In einem Ablauf zur Kalenderregistrierung sammelt ein Unternehmen nicht nur Attribute wie Name, E-Mail und Telefonnummer, sondern auch Geschäftsanforderungen, die an IT-Administratoren weitergeleitet werden. Diese Geschäftsanforderungen können die Einholung der Einwilligung zu Nutzungsbedingungen und dem Empfang von E-Mails definieren, wie auf der linken Seite dargestellt.

Wenn eine Person in den Empfang von E-Mails einwilligt, erfasst das Formular die erteilte Einwilligung als Attribut der Person, um das E-Mail-Marketing zu ermöglichen und dabei die Datenschutzbestimmungen einzuhalten.

Einwilligung als Attribut speichern

Das Universal Directory von Okta kann alle Antworten als Attribute speichern, einschließlich der Zustimmung zu den Nutzungsbedingungen, wie in Abbildung 3 (TOS) dargestellt.

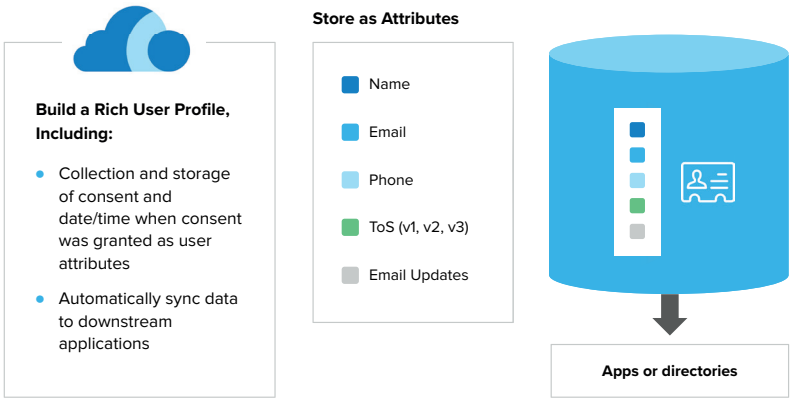


Abbildung 3

Optionale Einwilligung

Wenn eine Person keine Marketing-E-Mails erhalten, aber trotzdem die Anwendung nutzen möchte, lässt sich auch das als Attribut speichern. Durch Eingrenzung des Empfängerkreises für Marketing-Nachrichten wird der Aufwand für den IT-Administrator reduziert, indem eine vorgefertigte Oberfläche angezeigt wird, wie in Abbildung 4 dargestellt.

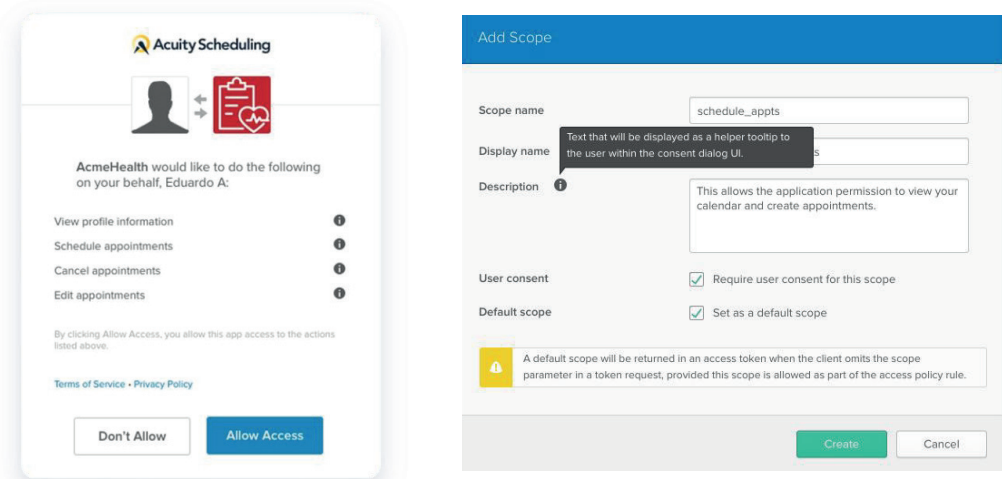


Abbildung 4

Nachgelagerte Anwendungen

Ein weiteres Beispiel für die Einholung der Einwilligung ist das Szenario der nachgelagerten Anwendungen und die Einholung der Einwilligung zum Austausch von Daten.

Wenn ein Nutzer beispielsweise seinen Google-Kalender mit seiner anderen Kalender-App synchronisieren möchte, ist die Einholung einer Einwilligung erforderlich, um die DSGVO einzuhalten. In diesem Fall wird die Zustimmung des Benutzers benötigt, damit die Kalenderanwendung auf Google Calendar zugreifen kann. Erforderliche Bereiche sind das Benutzerprofil und Kontakte, die als Attribute gespeichert werden könnten.

Eine Funktion, die das API-Zugriffsmanagement bietet, ist eine vorgefertigte Oberfläche zum Einholen der Einwilligung und die Möglichkeit, die eigene Benutzeroberfläche über die in Abbildung 4 dargestellten APIs anzupassen. Dies erleichtert Entwicklern ihre Arbeit, da damit eine benutzerfreundliche Oberfläche zur Verfügung steht, die dem Endbenutzer angezeigt wird. Dabei ist allerdings immer zu bedenken, dass Okta beim Senden einer Anfrage an nachgelagerte Anwendungen nur bei der Automatisierung der Anfrage helfen, aber die Datenschutzpraktiken oder die Datenverwendung durch eine nachgelagerte Anwendung nicht kontrollieren kann.

Einwilligung im Zeitverlauf

Wie bereits erwähnt kann die Einwilligung als Attribut im Universal Directory gespeichert und automatisch aktualisiert werden, wenn sich die Anwendungsfälle für die Einwilligung im Lauf der Zeit ändern. Einige Beispielszenarien hierfür wären die Aktualisierung einer Servicebedingung, einer Datenschutzerklärung oder der Marketingpräferenzen. Durch die Speicherung eines separaten Datumsattributs in Verbindung mit dem Einwilligungsattribut können IT-Administratoren die Einhaltung der Einwilligung über einen bestimmten Zeitraum und unterschiedliche Einwilligungsanforderungen überprüfen.

Ein häufiges Beispiel für unterschiedliche Einwilligungsanforderungen könnten unterschiedliche Datenschutzrichtlinien für verschiedene Anwendungen sein. Beispielsweise könnten einige Webanwendungen Cookies verwenden, während andere Anwendungen personenbezogene Daten wie E-Mails erfassen. Diese verschiedenen Anforderungen erfordern angepasste Richtlinieneinstellungen und unterschiedliche Arten der Einwilligung.

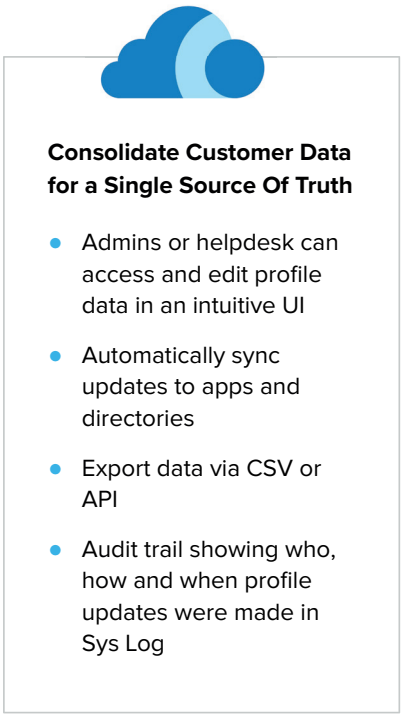
So lassen sich mit Okta Datenzugriffsrechte und das Berichtigungsrecht umsetzen

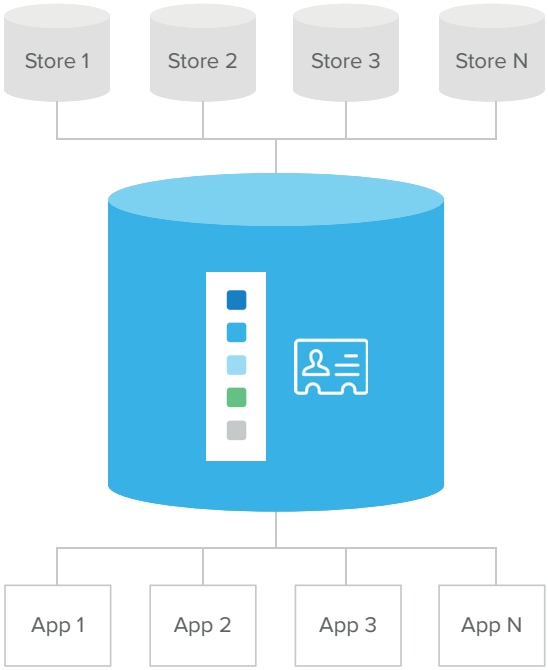
Die DSGVO umfasst ein Auskunftsrecht der betroffenen Personen (Artikel 15) und das Recht auf Berichtigung (Artikel 16). Das Auskunftsrecht garantiert den betroffenen Personen den Zugang zu den über sie erhobenen personenbezogenen Daten. Durch das Recht auf Datenübertragbarkeit können Betroffene Unternehmen dazu auffordern, die über sie gesammelten personenbezogenen Daten in einem maschinenlesbaren Format bereitzustellen, damit sie an andere Unternehmen übermitteln werden können. Unternehmen können diese Rechte mit einer Plattformlösung von Okta (Universal Directory, Syslog-API) umsetzen, die Benutzern den Zugang zu und die Prüfung von Profildaten ermöglicht.

Erstellen eines konsolidierten Profils

Wie vorstehend für die Verwaltung von Einwilligungen beschrieben, bildet das Universal Dictionary von Okta das Kernelement der Verwaltung von Profilzugriff und -aktualisierungen. Häufig werden die Daten von Einzelpersonen in isolierten Identitätsspeichern aufbewahrt. Damit wird es schwierig, eine zentrale verlässliche Informationsquelle zu definieren und genau darzustellen, welche personenbezogenen Daten im Falle einer Zugriffsanfrage einer betroffenen Person gesammelt werden. Dieses Problem wird durch Verzeichnisintegrationen gelöst, die es Okta ermöglichen, sich mit verschiedenen Identitätsspeichern zu verbinden und ein zentrales Modul mit den personenbezogenen Daten zu präsentieren. Ältere Verzeichnislösungen wie AD und LDAP können auch über einen lokalen Bereitstellungsagenten integriert werden, der über HTTPS an Okta angebunden wird.

Give users control over personal data





Wenn alle personenbezogenen Daten importiert sind, bietet Okta Admin- und Helpdesk-Rollen mit speziellen Zugriffsrechten. Werden die Rechte auf Auskunft, Datenübertragbarkeit oder Berichtigung im Rahmen der DSGVO von Betroffenen ausgeübt, ermöglichen die entsprechend zugeschnittenen Rollen Administratoren den Zugriff auf und Export dieser Daten für die betroffene Person sowie die Änderung der Profildaten auf deren Wunsch. Kombiniert man diese Funktion mit der Unterstützung von Echtzeit-Protokollierung in Okta, können Unternehmen einen Audit-Trail über den Datenzugriff, die Änderungen und den Export durch den Administrator erstellen, der als Nachweis dient, falls eine Regulierungsbehörde Compliance-Protokolle anfordert.

Betrachten wir nun ein Beispiel für Profiländerungen von nachgelagerten Anwendungen. Wie wird in diesem Fall sichergestellt, dass diese Änderungen über die Okta-Oberfläche vorgenommen werden? Wie aus Abbildung 2 ersichtlich werden die Änderungen an die externe Anwendung übertragen, um die Änderung zu übernehmen, sobald ein Profilattribut (beispielsweise der Vorname) im Profilabschnitt geändert wird. Damit Unternehmen die Anforderungen an die Datenübertragbarkeit bzw. das Recht erfüllen können, personenbezogene Daten in einem maschinenlesbarem Format zu erhalten, bietet die Benutzeroberfläche von Okta auch eine Funktion zum Herunterladen einer CSV-Datei, die dann an die betroffene Person übermittelt werden kann. Entwickler können auch eine eigene Benutzeroberfläche erstellen, indem sie die APIs von Okta nutzen und die Daten automatisiert im Rahmen einer einheitlichen Benutzererfahrung bereitstellen.

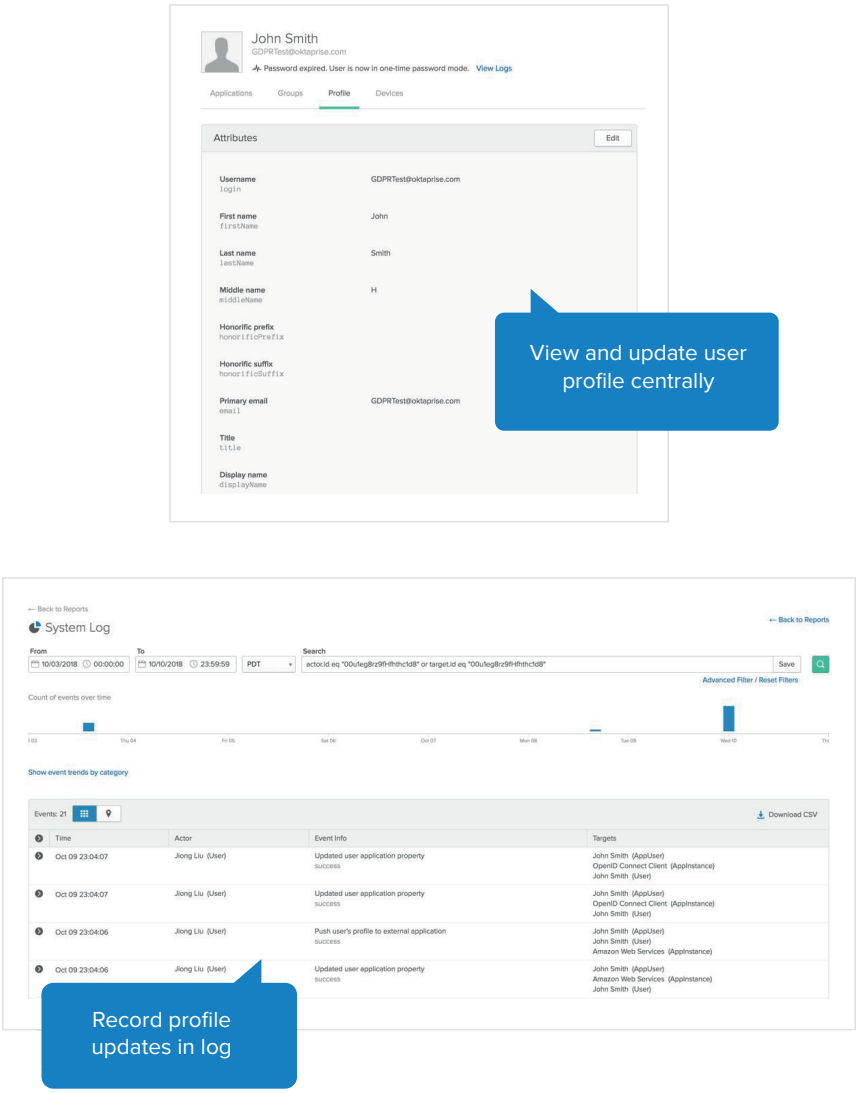


Abbildung 5

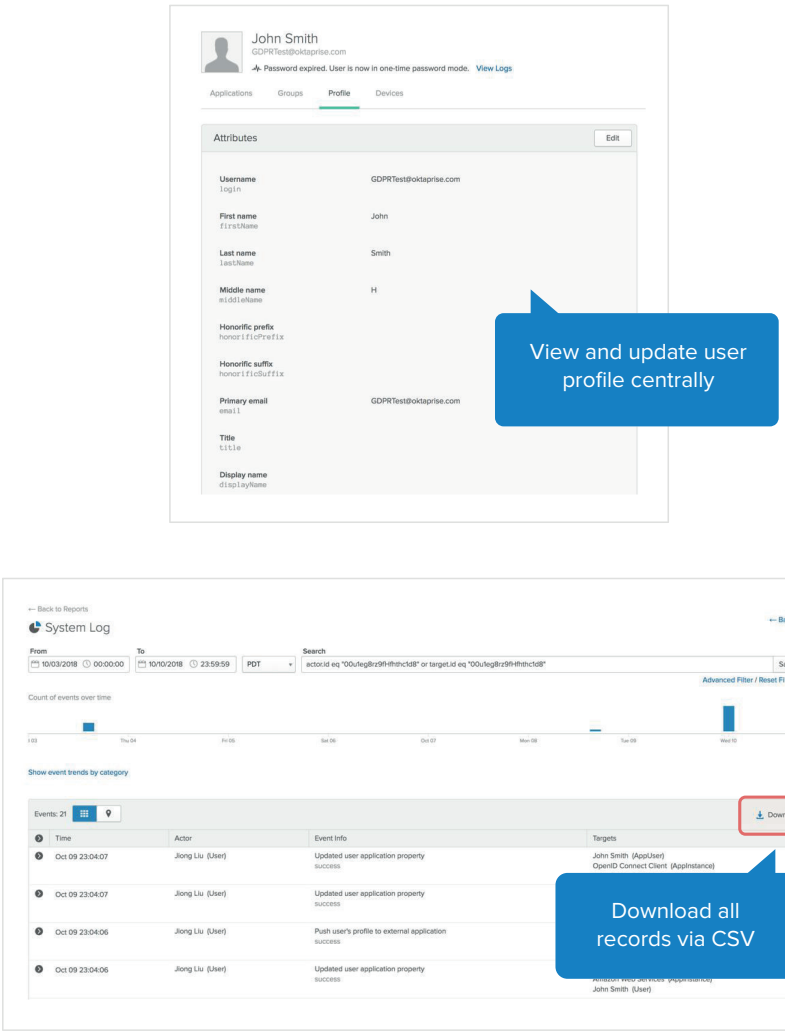
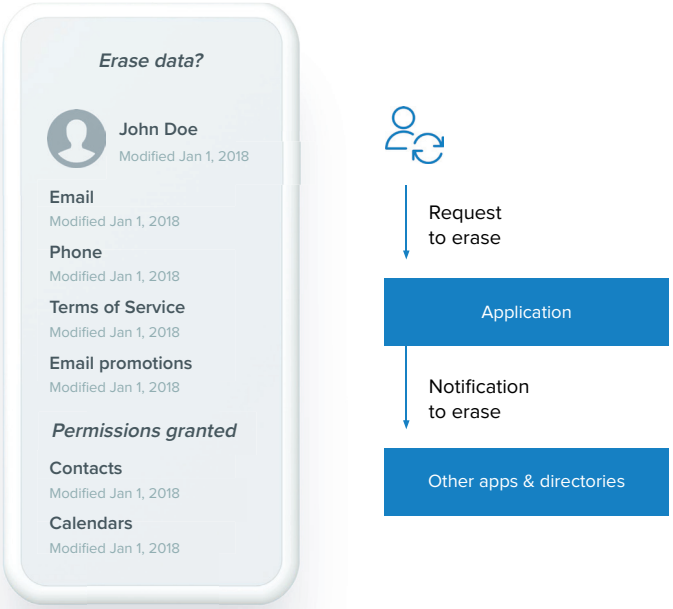


Abbildung 6

So lässt sich mit Okta das Recht auf Vergessenwerden umsetzen

Artikel 17 der DSGVO legt das Recht einer betroffenen Person auf Löschung personenbezogener Daten fest. Das bedeutet, dass moderne Unternehmen verpflichtet sind, personenbezogene Daten unverzüglich nach Erhalt einer entsprechenden Anfrage zu löschen.



Für IT-Administratoren bedeutet dies eine Verpflichtung zur Löschung der gesammelten personenbezogenen Daten einer betroffenen Person, die Einwilligungseinstellungen, E-Mail-Marketingeinstellungen sowie Profildaten umfassen können, und die Verpflichtung sicherzustellen, dass alle nachgelagerten Anwendungen und Datenspeicher, die personenbezogene Daten der anfragenden Person enthalten, diese im Rahmen der Anfrage ebenfalls löschen.

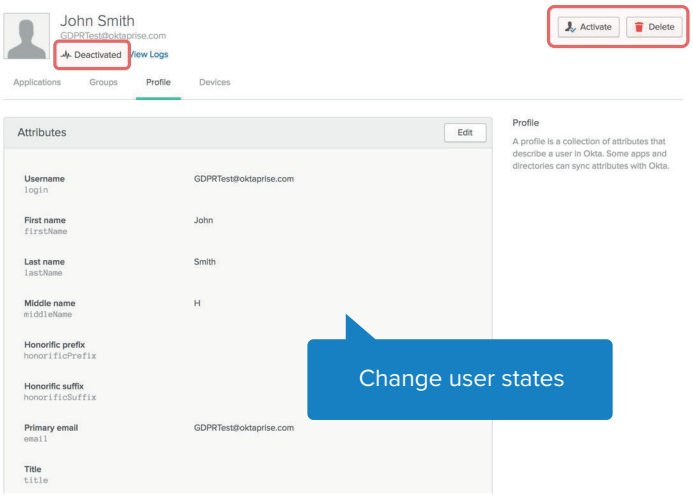
Das Produkt, das diesen Prozess vereinfacht, ist das Lifecycle-Management-Tool, das die Bereitstellung und den Entzug von Benutzerkonten von Okta verwaltet. Das LCM unterscheidet drei Zustände im Lebenszyklus eines Benutzerkontos: Suspendieren, Deaktivieren/Aktivieren und Löschen.

Ihre volle Leistungsfähigkeit entfaltet diese Funktion, wenn das Tool über ein API angesprochen wird, um einen automatisierten Prozess zur Verwaltung von Personen zu implementieren, die ihr Recht auf Vergessenwerden ausüben. Die Löschanfrage kann an nachgelagerte Anwendungen weitergeleitet werden, damit IT-Administratoren leichter gewährleisten können, dass keine Identitätsspeicherinstanz die personenbezogenen Daten des betreffenden Benutzers vorhält. Dies wird durch das Systemprotokoll dokumentiert, sodass Unternehmen einen Audit-Trail der Umsetzung der rechtlichen Vorgaben erstellen können.

Automated deletion from a central location

Manage Requests With A Centralized Identity

- Suspent, deactivate/reactivate, and delete user states
- Automated worlows and self service capabilities available through API
- Auditable record trail



So unterstützt Okta die Meldung von Datenschutzverstößen

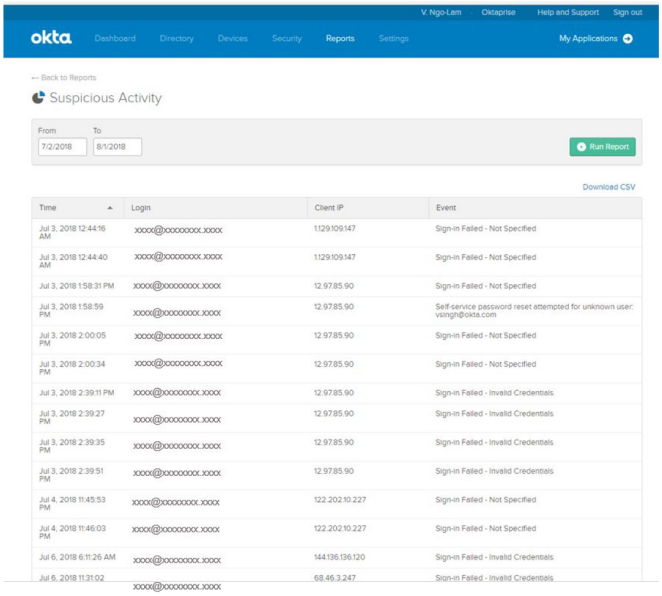
Artikel 33 und 34 der DSGVO schreiben vor, dass Unternehmen, die Datenverantwortliche in Sinne der DSGVO sind, einer Aufsichtsbehörde unverzüglich und nach Möglichkeit spätestens 72 Stunden nach Bekanntwerden einer Verletzung des Schutzes personenbezogener Daten Folgendes mitteilen müssen:

- **Art der Verletzung des Schutzes personenbezogener Daten**
- **Folgen der Verletzung des Schutzes personenbezogener Daten**
- **Maßnahmen zur Schadensbegrenzung**
- **Kontaktdaten des Datenschutzbeauftragten**

Breach report

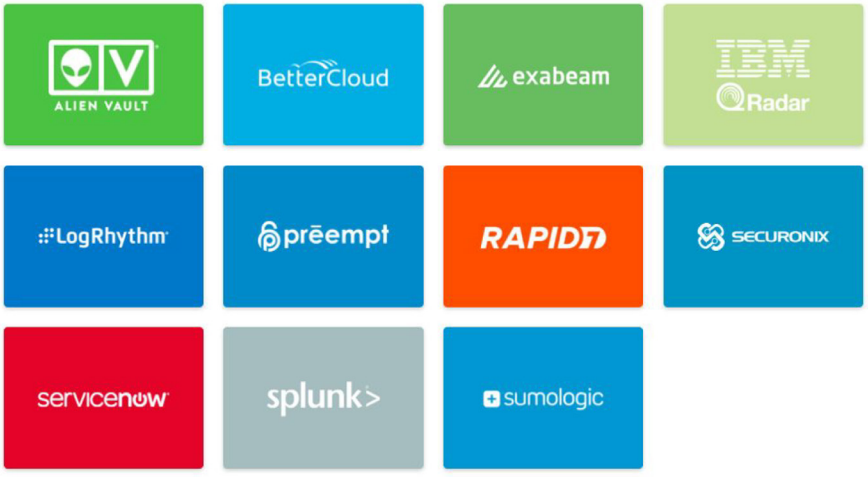
- Identify what was breached
- Investigate causes
- Contain further damage

Okta kann Incident-Response-Teams bei datenschutzrechtlichen Verpflichtungen unterstützen. Über die Auswertung des Systemprotokolls können Incident-Response-Teams ein detailliertes Protokoll aller Anmeldeaktivitäten einsehen. Darüber hinaus bietet das Syslog-API Entwicklern fertige Benutzeroberflächen/ Berichte aus allen Anwendungen (Cloud, Mobil usw.), die wiederum von Unternehmen im Rahmen einer Untersuchung des Datenschutzverstoßes verwendet werden können, um einige der notwendigen Angaben zu liefern, die von der DSGVO gefordert werden, was manuelle Prozesse minimiert und IT-Administratoren entlastet.



Wenn Okta mit allen eingesetzten Anwendungen verbunden ist, kann das Syslog auch zeigen, wer Zugriff auf die Anwendungen hat, und die Anmeldeversuche bei diesen Anwendungen mithilfe von vorfertigen Berichten nachweisen. Ein Beispiel wäre ein Bericht über verdächtige Aktivitäten, der die Anmeldung, die IP-Adresse und den Zeitpunkt der Aktivität eines verdächtigen Benutzers ausweist. Solche Berichte geben einen Einblick in unbefugte Benutzer, die möglicherweise versuchen, die IT-Infrastruktur zu infiltrieren.

Für komplexere Anwendungsfälle und eine ganzheitlichere Sicht auf die Umgebung der Kontoaktivitäten verfügt Okta über Integrationen für die größten SIEM-Anbieter. Dienste wie Splunk und Rapid 7 können Sicherheitsanalysen auf einer tieferen Ebene anbieten.

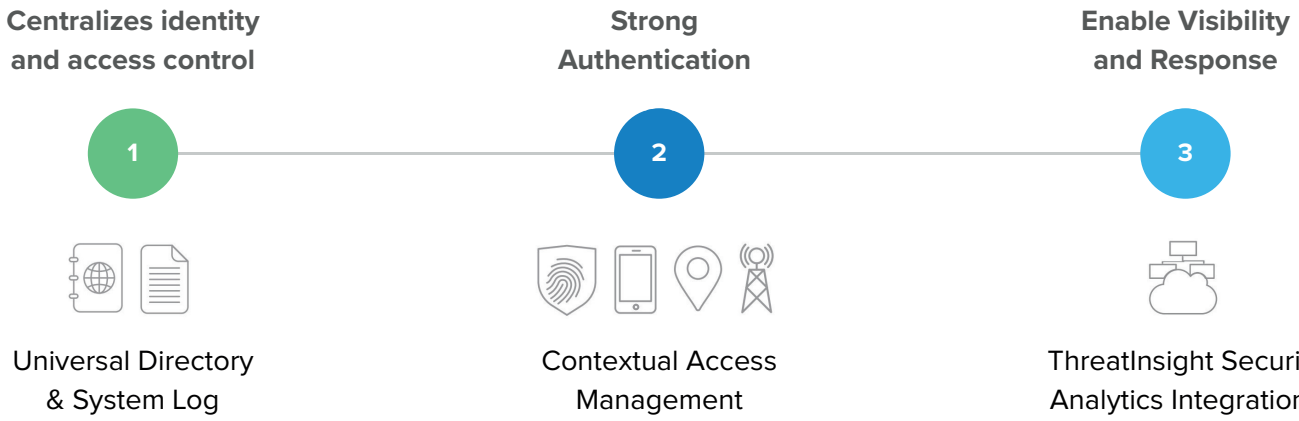


Integrations

Teil IV: Proaktive Vermeidung von Datenschutzverstößen

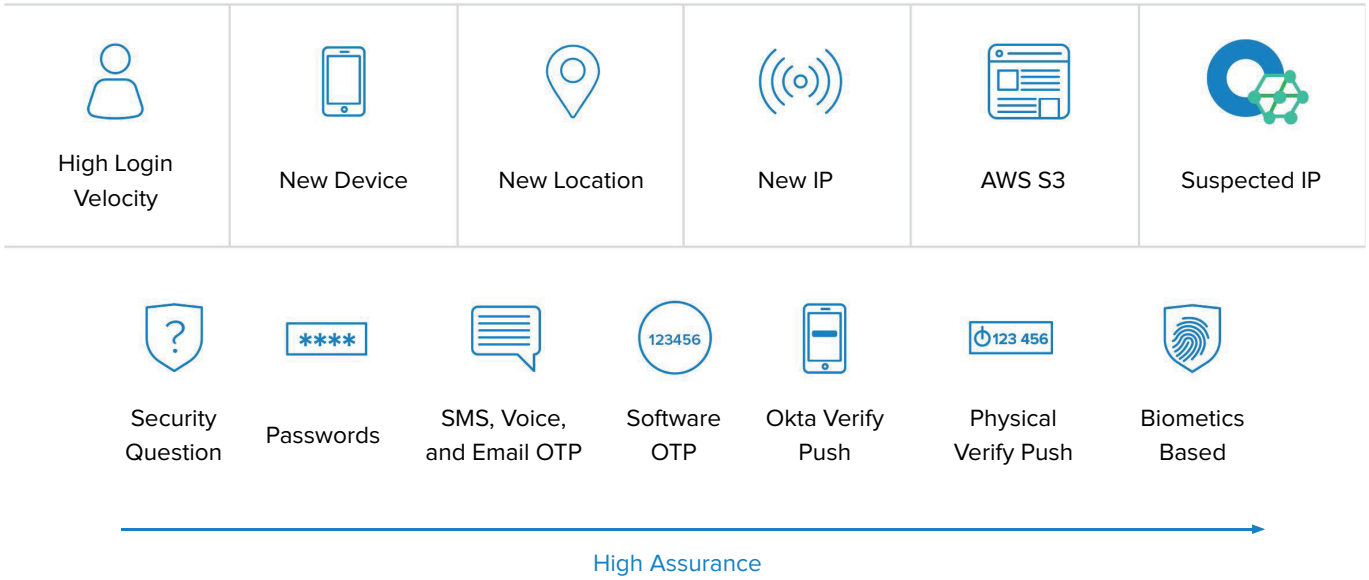
Wir bei Okta unterstützen Kunden bei Ihrer Verpflichtung, im Falle eines Datenschutzverstoßes die richtigen Stellen zu informieren. Am besten wäre es allerdings, wenn es gar nicht erst zu einem Datenschutzverstoß käme. Hier kommt das breitere Produktangebot von Okta ins Spiel und dabei ist es sinnvoll, Sicherheit als Frage des Identitätsmanagements zu betrachten. Mit der Verbreitung von IoT-Geräten hat sich die Angriffsfläche von Unternehmen auf Bereiche jenseits der Außengrenze ihres Netzwerks erweitert.

Die Okta-Plattform für identitätsbasierte Sicherheit hat drei Hauptaspekte:

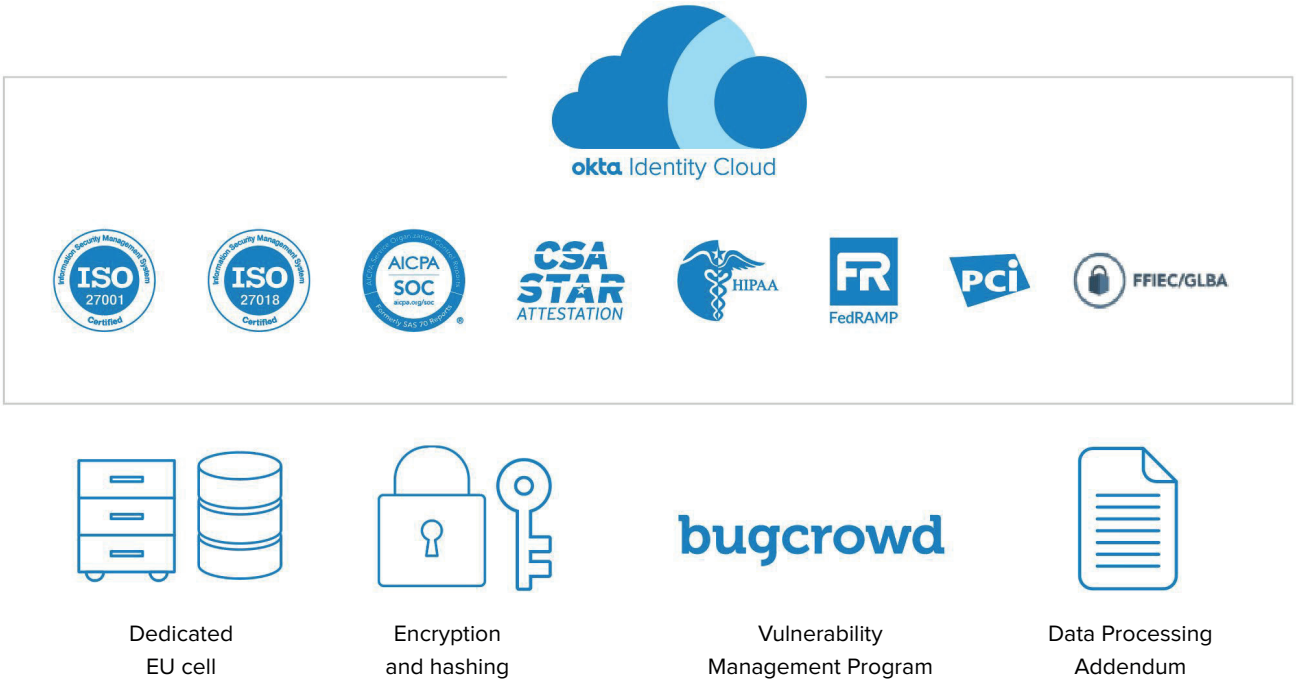


Zentralisieren der Identitäts- und Zugriffskontrolle – Durch die Einrichtung einer verlässlichen zentralen Informationsquelle und eines Fensters zum Backend der Kontoaktivitäten mit Universal Directory und Syslog können Identität und Zugriff über eine vorgefertigte Benutzeroberfläche gesteuert oder über das Okta-API individuell angepasst werden, wie unter Datenzugriffsrechte und Berichtigungsrecht erläutert.

Stärkung der Authentifizierung – SFA und 2FA sind überholt. Moderne Sicherheit erfordert den Einsatz von kontextbezogenem Zugriffsmanagement: Beim kontextabhängigen Zugriff können diese Szenarien mit anpassbaren Sicherheitsrichtlinien gesteuert werden, die IT-Administratoren einfach über die Okta-Oberfläche implementieren können. Durch die Analyse von Elementen wie Netzwerkeigenschaften, Gerätetyp, Standort und biometrische Daten ist unser adaptives MFA-Produkt (AMFA) der Goldstandard, um eine höhere Unternehmenssicherheit zu erreichen, die mit der Benutzerfreundlichkeit vereinbar ist.



Transparenz und Reaktionsfähigkeit – Als führender Anbieter von Identitätsmanagementlösungen bieten wir unseren Kunden identitätsbasierte Sicherheit der nächsten Generation, da sie ausgewählte Informationen von SIEM-Anbietern aus dem Okta Integration Network integrieren können. Okta bietet mit seinen 4.300 Kunden und 5.000 Partnern ein einzigartiges Leistungsversprechen durch eine Reihe von Best Practices für verdächtige Zugriffsanfragen. Wenn eine Anfrage im Sicherheitscheck mit weniger als 100 % eingestuft wird, leitet Okta die Authentifizierungsanfrage an einen Risiko-Scoring-Mechanismus weiter, der zur Festlegung der Zugriffsrichtlinien des Kunden verwendet werden kann. Okta kann durch eine entsprechende Konfiguration auch Netzwerkzonen und die Zugangshäufigkeit berücksichtigen, um gegebenenfalls eine Step-up-MFA auszulösen.



Teil V: Privatsphäre als Grundkonzept

Die Okta Identity Cloud wurde in der Cloud und unter Berücksichtigung von Sicherheit und Datenschutz entwickelt. Mit zahlreichen Zertifizierungen in einer Vielzahl von Branchen und mehreren externen Bestätigungen hat sich Okta als der führende Identitätsmanagementanbieter erwiesen.

- **Okta bietet noch weitere Funktionen an:**
- **Eigene EU-Zelle für DSGVO**
- **Verschlüsselung und Hashing**
- **Programm zum Management von Schwachstellen**
- **Nachtrag zur Datenverarbeitung**

Grundsätzlich geht Okta beim Datenschutz davon aus, dass Kunden die Eigentümer ihrer Daten sind. Wir verwenden Daten nur zur Erbringung unserer Dienstleistungen. Wir verkaufen keine Kundendaten oder Daten aus der Okta Identity Cloud. Wir ergreifen die in unserer Vertrauens- und Sicherheitsdokumentation beschriebenen Maßnahmen, damit die Daten unserer Kunden sicher und geschützt sind.

Über Okta

Okta ist der führende unabhängige Anbieter von Identitätslösungen für Unternehmen. Die Okta Identity Cloud verbindet und schützt Mitarbeiter vieler der weltweit größten Unternehmen. Zudem verbindet sie Unternehmen auf sichere Weise mit ihren Partnern, Lieferanten und Kunden. Durch nahtlose Einbindung in über 5.000 Anwendungen ermöglicht die Okta Identity Cloud den einfachen und sicheren Zugriff von jedem Gerät aus.

Tausende von Kunden, darunter 20th Century Fox, Adobe, Dish Networks, Experian, Flex, LinkedIn und News Corp, verlassen sich auf Okta, um schneller zu arbeiten, ihren Umsatz zu steigern und ihre Sicherheit zu wahren. Mit Okta kommen Kunden schneller ans Ziel, denn Okta macht den Zugang zu Technologien, die Kunden für ihre Arbeit unbedingt benötigen, sicher und benutzerfreundlich.

Weitere Informationen dazu finden Sie unter www.okta.com