Uw AVG-traject (Algemene Verordening Gegevensbescherming) beginnen met Okta

okta

Inhoudsopgave

Disclaimer: Hoewel juridische begrippen aan de orde komen in dit artikel, vormt het geen juridisch advies. Raadpleeg een juridisch adviseur als u of uw organisatie juridisch advies wenst te ontvangen.

Inleiding

Organisaties die consumenten bedienen, beheren sinds lange tijd identiteitsdata van klanten. Ze bewaren gevoelige data variërend van klantnamen tot creditcardnummers en woonadressen. Vanwege een toenemend aantal datalekken, groeiende zorgen omtrent privacy en veelvuldig misbruik van data, hebben wetgevers besloten om strikte eisen te stellen aan het gebruik van data. In de Europese Unie was de Algemene Verordening Gegevensbescherming (AVG) de eerste stap om nieuwe normen te bepalen voor de bescherming van persoonsgegevens. Om te blijven voldoen aan de wetgeving voor gegevensbescherming moeten organisaties nu opnieuw bekijken hoe zij hun IT-infrastructuur toekomstbestendig maken en dit dient op directieniveau te gebeuren.

Deel I:

AVG en zakelijke gevolgen

Het centrale concept van de AVG is in algemene zin dat personen eigenaar zijn van hun eigen data. Dit concept kan op verschillende manieren tot uiting komen, bijvoorbeeld door personen in staat te stellen om te bekijken welke data ondernemingen over hen hebben verzameld of hen de mogelijkheid te bieden om persoonsgegevens te laten verwijderen. In deze tijd van strikte privacyvoorschriften en hoge boetes is binnen IT-infrastructuren een andere benadering van compliance vereist.

Vanwege de toename van grote datalekken, bijvoorbeeld bij Marriott en Panera Bread in 2018, is nieuwe regelgeving inzake gegevensbescherming zoals de AVG geïntroduceerd ter bescherming van persoonsgegevens. Steeds meer mensen zijn zich bewust van dergelijke lekken, wat het vertrouwen van de klant en het klantsentiment heeft geschaad, en tot omzetdalingen heeft geleid bij de betrokken organisaties. Volgens IBM heeft 46% van de organisaties reputatieschade en verlies van merkwaarde opgelopen als gevolg van vertrouwensbreuken. Daarnaast kunnen overtredingen van de AVG leiden tot boetes van € 20 miljoen of 4% of van de wereldwijde omzet. Vanaf nu moeten organisaties zorgvuldig nieuwe maatregelen en processen implementeren om op efficiënte wijze te voldoen aan deze regelgeving.

De Ierse Data Protection Commission en toekomstige handhaving

De Ierse Data Protection Commission (DPC), de nationale onafhankelijke instantie die verantwoordelijk is voor het beschermen van de fundamentele rechten van personen in de EU met betrekking tot hun persoonsgegevens, heeft zijn inspanningen voor het handhaven van de AVG vergroot. In oktober 2018 had de DPC 80 onderzoeken naar overtredingen van de AVG geopend, waaronder een statutair onderzoek naar de naleving van relevante bepalingen van de AVG door Facebook.

Deel II:

Zorg dragen voor compliance

Omdat de DPC en andere vergelijkbare toezichthouders voor gegevensbescherming de AVG strenger handhaven, moeten IT-managers zorgen dat zij klaar zijn om de regelgeving na te leven. Wanneer organisaties eenmaal aan de regels voldoen, kan het evenwel lastig zijn om deze te blijven naleven. De waarheid is dat naleving van de AVG een doorlopend traject is met verschillende compliancefasen.

Looptijd AVG

Afbeelding 1

Fase 1: organisaties die nog niet aan het compliancetraject zijn begonnen

Toen de AVG in mei 2018 van kracht werd, hebben de meeste organisaties getracht om de nieuwe regels zo snel mogelijk te implementeren. Er zijn evenwel veel organisaties die niet beseffen dat de AVG ook voor hen geldt. Deze organisaties bevinden zich in “fase 1”.

Volgens artikel 3 van de AVG moet een organisatie aan de AVG voldoen indien het:

- een verwerkingsverantwoordelijke of een verwerker in de EU is;
- goederen en diensten aanbiedt aan betrokkenen in de EU; of
- het gedrag van betrokkenen in de EU controleert.

De AVG geldt ook voor organisaties die mogelijk niet verwachten onder buitenlandse wetgeving te vallen, omdat artikel 3 van de AVG zodanig is verwoord dat de verordening van toepassing is op een grote verscheidenheid aan organisaties: organisaties die dienstverleners zijn, goederen of diensten aanbieden aan betrokkenen in de EU of het gedrag van betrokkenen in de EU "controleren". Bovendien is de definitie van persoonsgegevens in de AVG zo breed dat diverse datatypen eronder vallen, van socialmediaberichten tot creditcarddata die worden verkregen bij het boeken van een vlucht. Omdat deze definitie van persoonsgegevens zoveel data omvat, weten organisaties vaak niet zeker of hun gebruik van data er ook onder valt. Daardoor beseffen talloze organisaties niet dat de AVG ook voor hen geldt en dat zij aan deze wetgeving moeten voldoen.

Fase 2: organisaties die handmatige complianceprocessen gebruiken

Organisaties in deze fase van het compliancetraject zijn organisaties die weten dat de AVG voor hen geldt en zorg dragen voor compliance met handmatige processen. Afhankelijk van het type organisatie kan dit leiden tot een overmatige besteding van IT-, juridische, ondersteunings- en technische resources aan compliance en problemen met de handmatige configuratie van verschillende systemen. Volgens Forbes is in de VS en het VK $ 8 miljard uitgegeven aan compliance met de AVG. Dit bedrag is besteed aan het inhuren van juridische teams, consultants en functionarissen voor gegevensbescherming. Omdat organisaties worden overstelpt met verzoeken (zoals het recht om te worden vergeten), moeten IT-beheerders en helpdeskmedewerkers steeds meer tijd hieraan besteden in plaats van aan hun kerntaken.

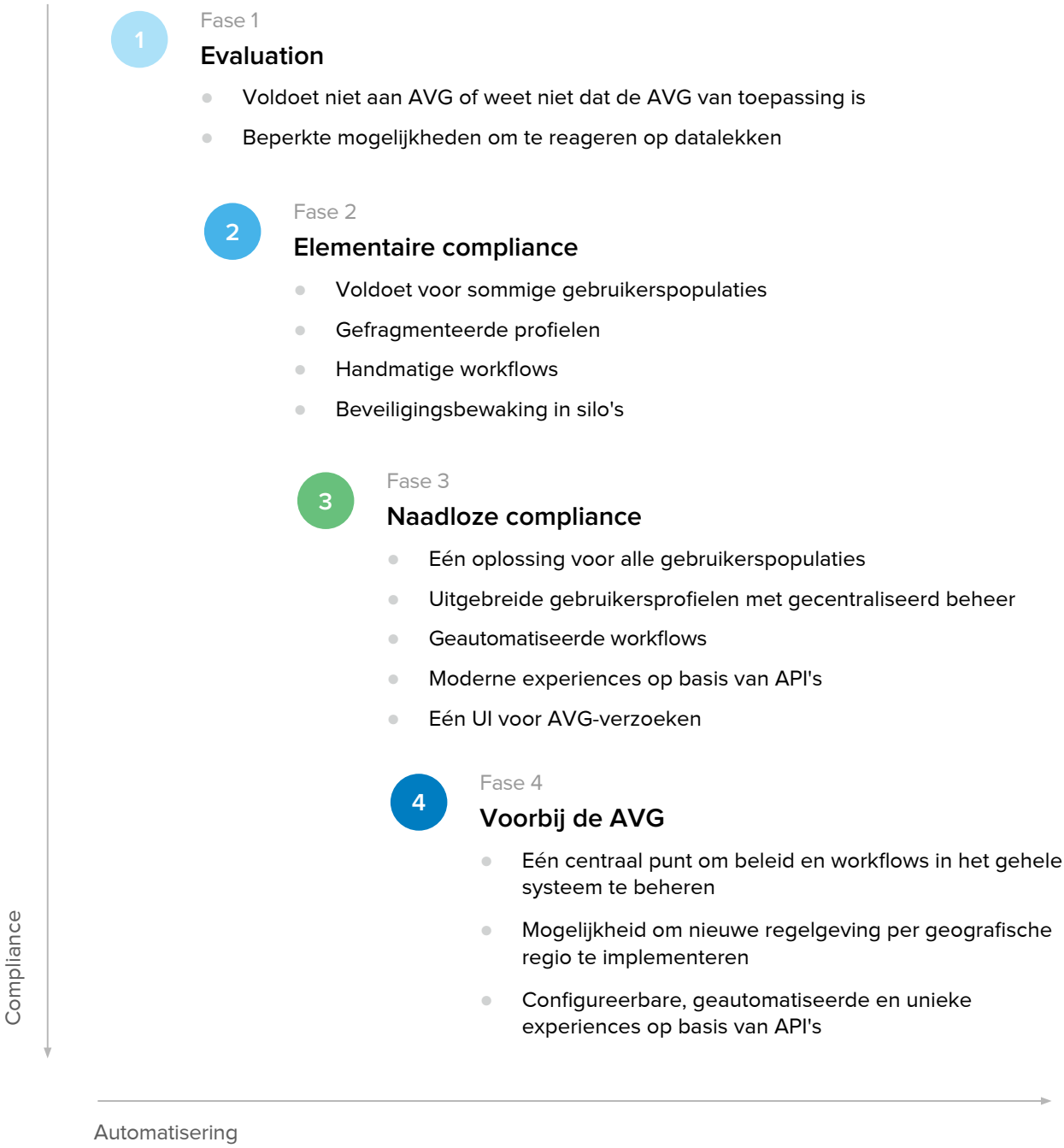
Bepaalde organisaties in deze fase hebben mogelijk alleen gezorgd voor compliance door hun eigen medewerkers, maar geen aandacht besteed aan de vereiste complianceprocessen voor hun klanten. Dit is een groeiend probleem met organisaties zoals Google die 2,4 miljoen verzoeken om te worden vergeten ontvangen en slechts 43% daarvan kunnen beantwoorden. Het feit dat 89% van deze verzoeken afkomstig was van privépersonen, wijst op toenemende zorgen over privacy onder consumenten.

Fase 3: organisaties die software gebruiken voor compliance met de AVG in overeenstemming met de digitale transformatie

Organisaties in deze fase gebruiken software voor compliance, zoals een moderne identity-oplossing, om repetitieve workflows te automatiseren. Door onderdelen van de AVG, zoals het recht om data te laten verwijderen of in te zien, te behandelen als provisioning- en deprovisioning-problemen, kunnen organisaties producten zoals Lifecycle Management inzetten om de werklast van IT-beheerders te verlichten. De functionaliteit kan verder worden uitgebreid door identity- en toegangsconcepten zoals beheer van downstream applicaties en beveiligingsbeleid te gebruiken voor compliance.

Fase 4: organisaties die een platform voor identity management invoeren dat dynamisch wordt aangepast aan wetten inzake gegevensbescherming

GDPR Maturity Curve



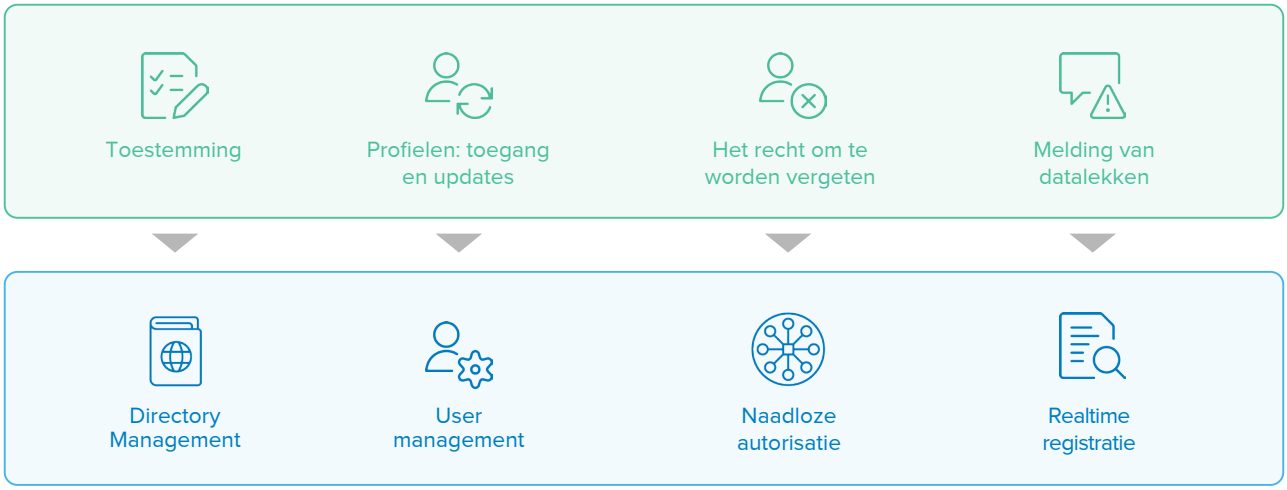
Er is een wereldwijde golf van regulering zichtbaar: van de AVG in de Europese Unie tot de Privacy Act in Australië en de CCPA in Californië. Privacy wordt een steeds belangrijker onderwerp voor IT-organisaties, die nu worstelen met de verplichting om te voldoen aan allerlei nieuwe privacyverordeningen. Grote organisaties, die in toenemende mate wereldwijd actief zijn, moeten een aanpasbare en flexibele identiteitsoplossing in overweging nemen, zodat zij kunnen blijven voldoen aan specifieke regelgeving in verschillende regio's. Zoals afbeelding 1 aangeeft zijn klanten in verschillende delen van de wereld onderworpen aan regelgeving op andere niveaus. Bovendien heeft elk land weer een eigen benadering van privacy.

De oplossing bestaat echter niet in het gebruik van verschillende tools om een moderne identity-oplossing samen te stellen; uiteindelijk is de overgang naar een identity-platform onvermijdelijk. De volgende stap bij compliancebeheer is de beschikking over één controlepunt om systeembrede beleidsregels en workflows te beheren.

Deel III:

Customer identity en compliance

Met een moderne identity-oplossing die automatisering biedt, kunnen organisaties hun complianceverplichtingen op grond van de AVG beter beheren, omdat de customer identity een centrale rol krijgt. Door de AVG te beschouwen als een op identity gebaseerd probleem, kunnen we een relevante reeks producten inzetten om de complianceproblemen op te lossen. Laten we de mogelijke tools en de bijbehorende vereisten naar aanleiding van de AVG bekijken.



Afbeelding 2

In afbeelding 2 zien we vier producten die kunnen worden benut voor de AVG:

- Universal Directory – een gecentraliseerd archief van alle gebruikers, waarin profiel- en toestemmingsattributen kunnen worden opgeslagen.
- Lifecycle Management – downstream acties automatiseren wanneer een klant een handeling heeft uitgevoerd.
- API Access Management – toestemmingen en de reikwijdte beheren voor downstream applicaties.
- Realtime registratie – een audit trail voor compliance bieden met behulp van een systeemlogboek.

Deze tools kunnen worden benut voor de volgende belangrijke vereisten naar aanleiding van de AVG:

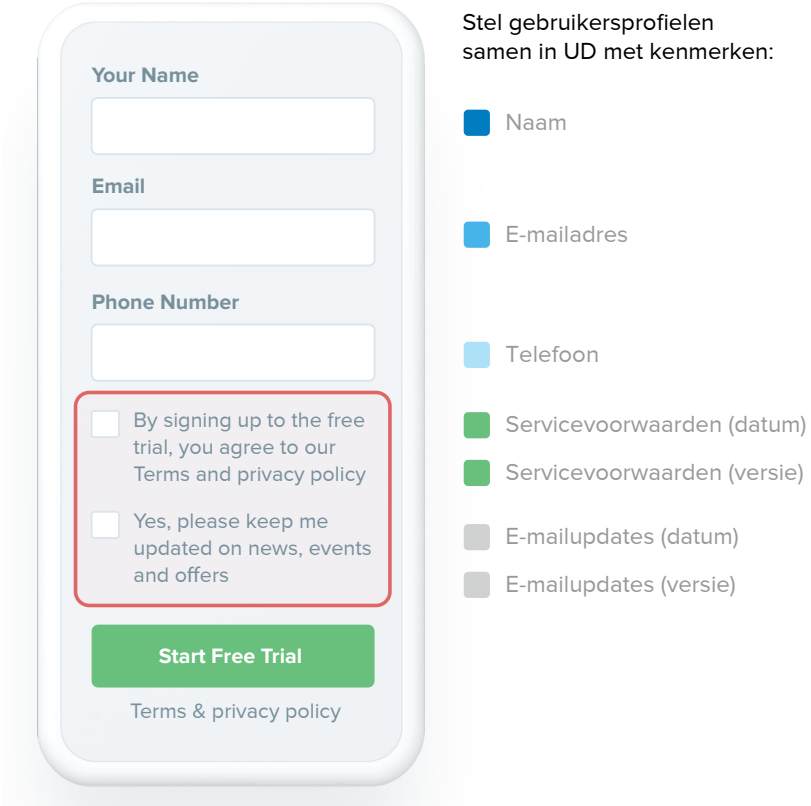
- Toestemming — Artikel 6 en 7 van de AVG
- Profieltoegang en -updates — Artikel 15, 20 en 40 van de AVG
- Recht om te worden vergeten — Artikel 17 van de AVG
- Melding van datalekken — Artikel 33 en 34 van de AVG

Door elke vereiste grondig te analyseren en productfunctionaliteiten te koppelen aan complianceverplichtingen, kunnen organisaties de eerste stappen zetten om in hun compliancebehoeften te voorzien met een identity-oplossing. In de volgende gedeelten gaan we dieper in op de verschillende artikelen van de AVG en beschrijven wij hoe u aan de compliancevereisten kunt voldoen met de Okta-productsuite.

Hoe Okta kan worden gebruikt voor het beheren van toestemmingen

Artikel 6 van de AVG biedt een uiteenzetting van de situaties waarin, of rechtsgronden op basis waarvan, organisaties persoonsgegevens mogen verwerken. Eén rechtsgrond voor het verwerken van persoonsgegevens is toestemming voor specifieke doeleinden. De specifieke voorwaarden voor geldige toestemming worden beschreven in artikel 7. Een veelvoorkomend scenario waarvoor organisaties toestemming moeten verkrijgen is de registratie van een mobiele agenda-applicatie. Bij Okta slaan we toestemmingsdata op als een attribuut in Universal Directory. In het volgende gedeelte behandelen we hoe een agenda-applicatie bijvoorbeeld wordt geregistreerd en tonen we hoe Okta helpt bij toestemmingsbeheer.

Agenda-appregistratie



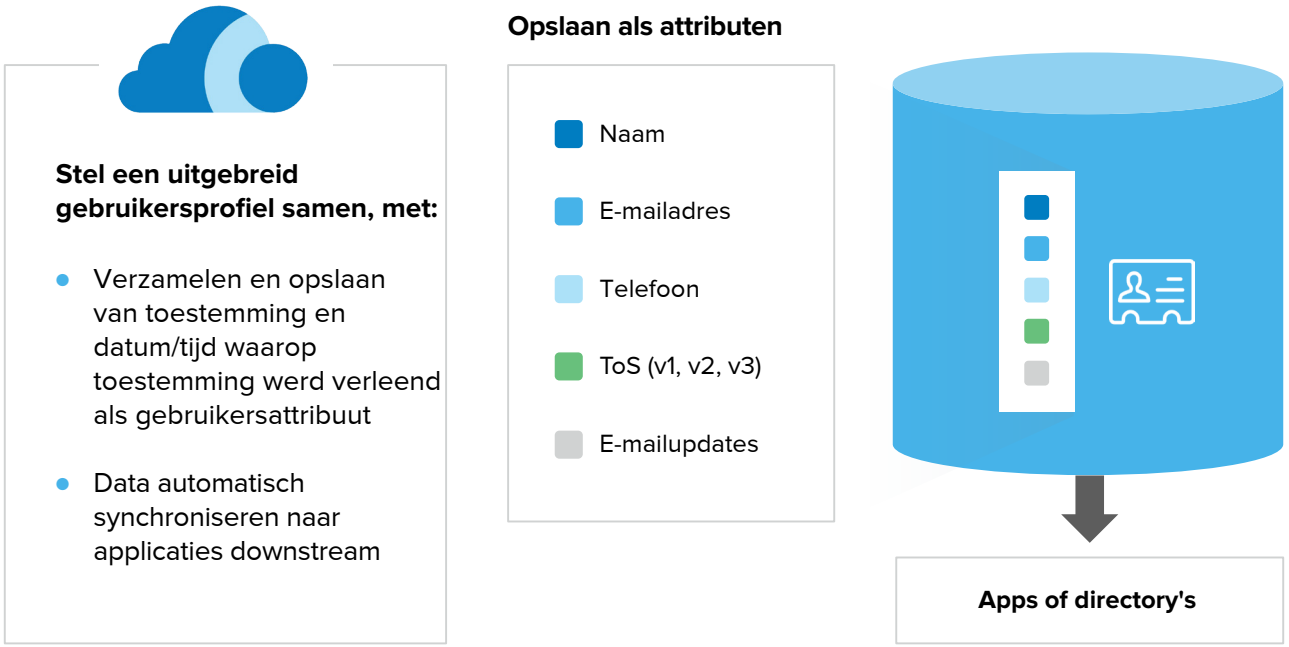
Registratie

In een registratieprocedure voor een agenda verzamelt een organisatie niet alleen attributen zoals naam, e-mailadres en telefoonnummer, maar ook zakelijke vereisten die worden doorgegeven aan IT-beheerders. Deze zakelijke vereisten kunnen bepalen welke toestemming voor het verzamelen van data moet worden verkregen voor de servicevoorwaarden en voor e-mailupdates, zoals links wordt weergegeven.

Als iemand zich aanmeldt voor e-mailupdates, wordt deze toestemming via het formulier geregistreerd als een attribuut van de persoon, dat aangeeft dat e-mailmarketing mogelijk is zonder de AVG te overtreden.

Toestemmingsdata opslaan als een attribuut

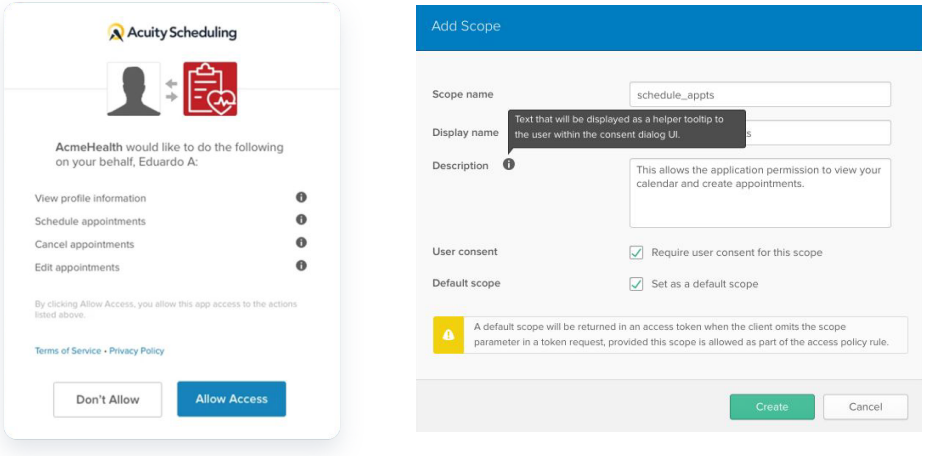
In de Universal Directory van Okta kan al deze data – waaronder het accepteren van de servicevoorwaarden – worden opgeslagen als attributen, zoals wordt weergegeven in afbeelding 3 (servicevoorwaarden).



Afbeelding 3

Optionele toestemming

Als een persoon geen marketing-e-mails wil ontvangen maar de applicatie wel wil gebruiken, kunt u dit ook opslaan als een attribuut. Via een kant-en-klare gebruikersinterface kan worden ingesteld wie marketingberichten ontvangt en wie niet, zoals wordt weergegeven in afbeelding 4. Dit vermindert de beheerlast aanzienlijk.



Afbeelding 4

Downstream apps

Een ander voorbeeld van toestemming voor het verzamelen van data is het scenario van downstream applicaties en toestemming om data te delen.

Als een gebruiker bijvoorbeeld Google Agenda wil synchroniseren met een aangepaste agenda-app, is toestemming voor het verzamelen van data vereist op grond van de AVG. In dit geval moet de gebruiker toestemming geven opdat de agenda-applicatie toegang krijgt tot Google Agenda. De vereiste reikwijdte bestaat bijvoorbeeld uit het profiel en de contactpersonen, en deze kunnen worden opgeslagen als attributen.

API access management biedt tevens een kant-en-klare gebruikersinterface voor toestemming voor het verzamelen van data. Ook kunt u uw eigen API's aanpassen, zoals wordt weergegeven in afbeelding 4. Hierdoor kunnen developers gemakkelijker een gebruiksvriendelijke interface presenteren aan eindgebruikers. Bij het verzenden van een aanvraag naar downstream applicaties kan Okta evenwel alleen ondersteuning bieden voor het automatiseren van de downstream aanvraag en is Okta niet in staat om de privacypraktijken of het datagebruik van de downstream applicatie te bepalen.

Toestemmingsdata op langere duur

Zoals eerder aangegeven, kan toestemming als een attribuut worden opgeslagen in Universal Directory en automatisch worden bijgewerkt als de gebruikssituaties voor de toestemming na verloop van tijd veranderen. Scenario's waarin dit gebeurt zijn bijvoorbeeld wijzigingen in de servicevoorwaarden, het privacybeleid of marketingvoorkeuren. Door een afzonderlijk gegevensattribuut op te slaan bij het toestemmingsattribuut kunnen IT-beheerders naleving van de toestemmingsvereisten gedurende een periode en andere toestemmingaspecten controleren.

Een algemeen voorbeeld voor verschillende toestemmingsvereisten zijn afwijkende privacybeleidsregels voor verschillende applicaties. Met bepaalde webapplicaties worden bijvoorbeeld alleen cookiedata verzameld, terwijl met andere apps persoonsgegevens zoals e-mailadressen worden verzameld. Vanwege deze afwijkende vereisten zijn unieke beleidsinstellingen en verschillende soorten toestemmingen nodig.

Hoe Okta profieltoegang en -updates beheert

De AVG biedt betrokkenen het recht van toegang (artikel 15) en rectificatie (artikel 16). Op grond van het recht van toegang moeten personen toegang kunnen krijgen tot de persoonsgegevens die over hen zijn verzameld. Op grond van het recht op overdraagbaarheid van data hebben personen het recht om de over hen verzamelde persoonsgegevens te verkrijgen in een machineleesbare vorm, zodat zij de data kunnen overdragen aan een andere organisatie. Organisaties kunnen aan deze twee rechten van personen voldoen met een platformgebaseerde oplossing van Okta (Universal Directory, API van het systeemlogboek), waarmee personen profieldata kunnen inzien en controleren.

Een geconsolideerd profiel creëren

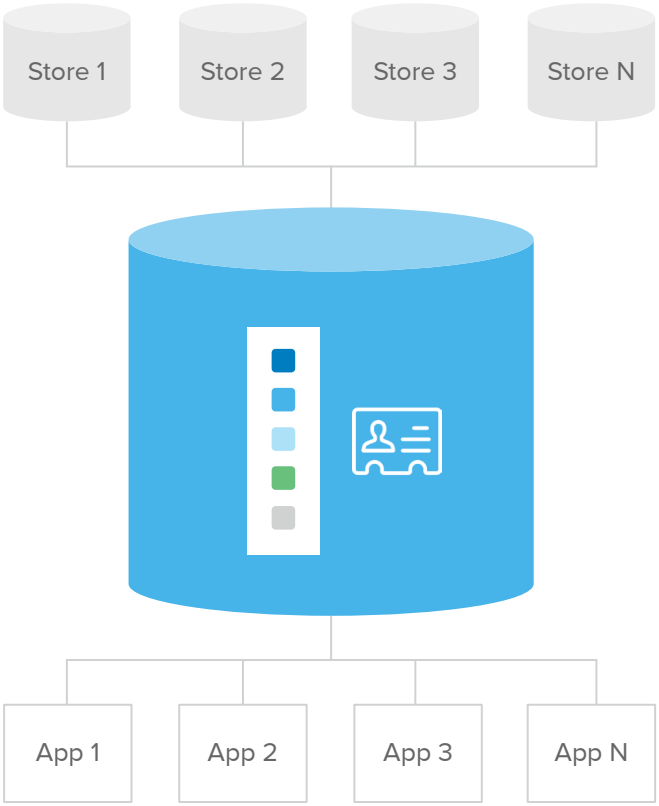
Zoals aangegeven voor toestemmingsbeheer speelt Universal Directory van Okta een centrale rol bij het ondersteunen van profieltoegang en -updates.

Persoonsgegevens zijn vaak verspreid over verschillende losse identity stores, zodat er niet één source of truth bestaat en het in geval van een verzoek van een betrokkene onmogelijk is om de verzamelde persoonsgegevens nauwkeurig weer te geven. Dit probleem wordt opgelost met directoryintegraties. Hierbij maakt Okta verbinding met verschillende identity stores en wordt al de data over een persoon op één plaats getoond. Legacy directory's zoals AD en LDAP kunnen ook worden geïntegreerd via een on-prem provisioning-agent die via HTTPS beschikbaar is in Okta.

Laat gebruikers hun eigen persoonsgegevens beheren

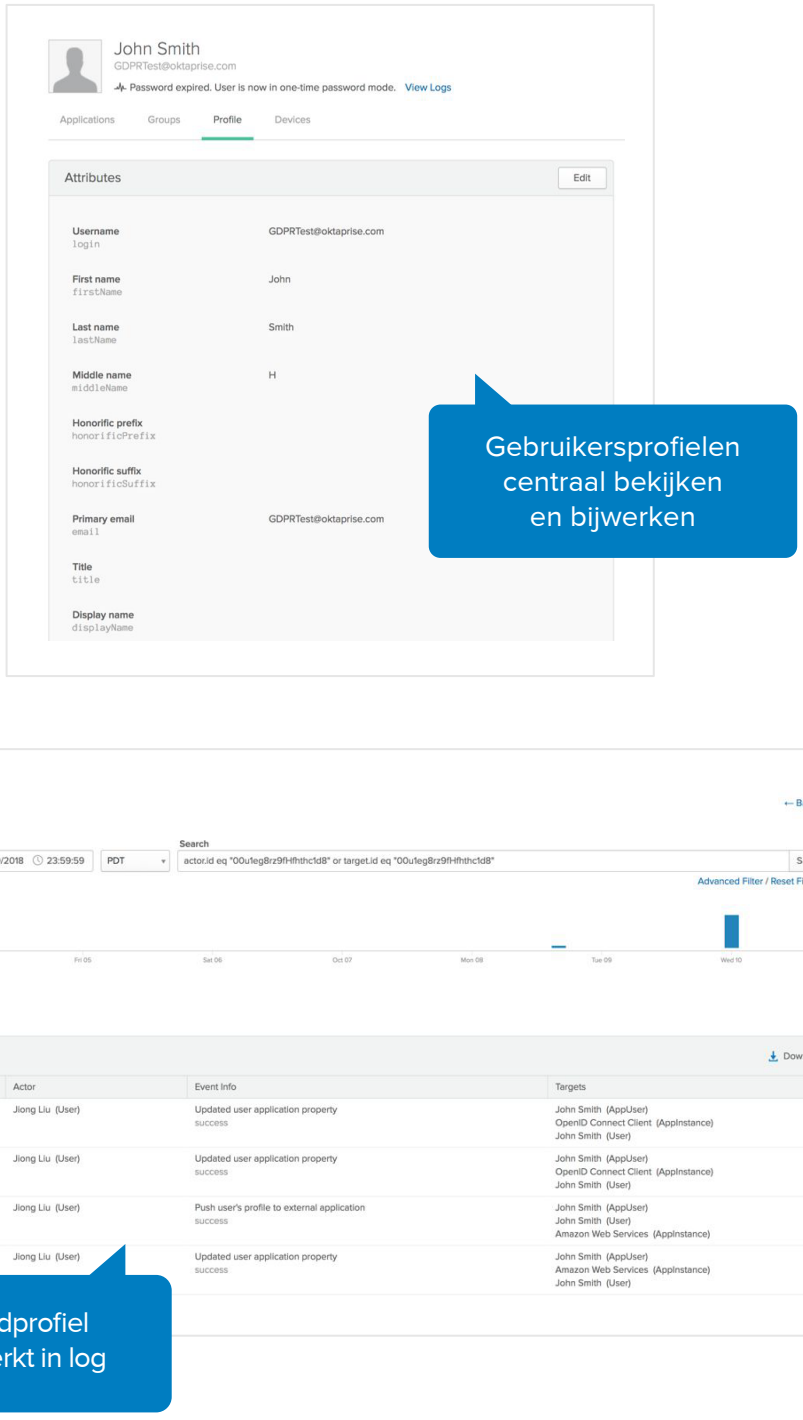
Consolideer klantgegevens voor één source of truth

- Beheerders of de helpdesk kunnen profieldata bewerken in een intuïtieve UI
- Synchroniseer updates automatisch voor apps en directory's
- Exporteer data via CSV of API
- Audit trail die laat zien door wie, hoe en wanneer profielupdates in System Log werden gemaakt



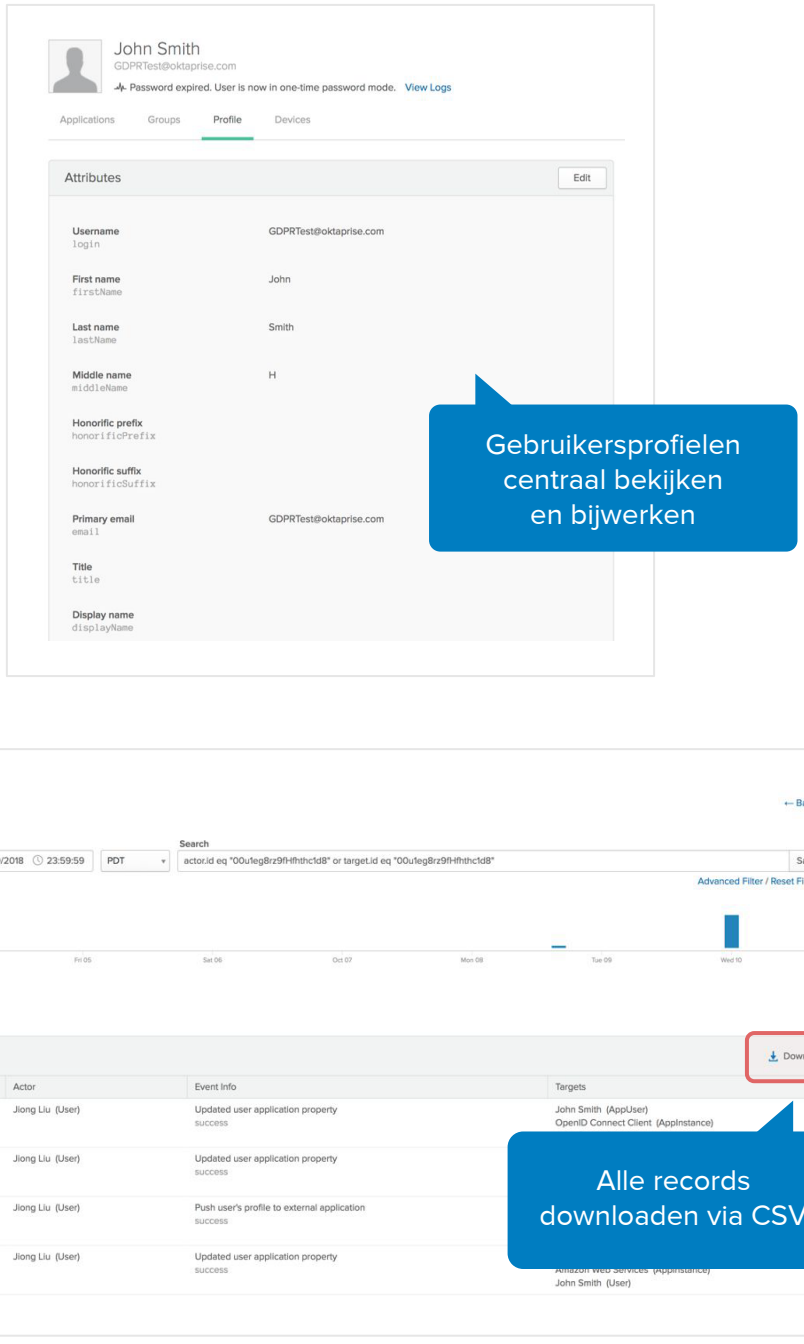
Wanneer alle afzonderlijke data is geïmporteerd biedt Okta beheer- en helpdeskprofielen met specifieke bevoegdheden. Als een persoon zijn of haar recht van toegang, overdraagbaarheid van data of rectificatie op grond van de AVG wil uitoefenen, kan de beheerder op basis van diens specifieke bevoegdheden de data exporteren of de profieldata wijzigen op verzoek van de persoon. Als deze functionaliteit samen met de ondersteuning voor realtime registratie van Okta wordt gebruikt, kunnen organisaties een audit trail bijhouden van datatoegang, -wijzigingen en -exports door de beheerder. Zij kunnen deze data vervolgens verstrekken wanneer een regulerende instantie om compliancedocumenten vraagt.

Laten we een voorbeeld bekijken van profielupdates voor downstream applicaties, waarbij de wijzigingen moeten worden aangebracht via de Okta-gebruikersinterface. Afbeelding 2 toont dat een wijziging aan een profielattribuut (voornaam) in het profielgedeelte direct wordt doorgestuurd naar een externe applicatie.



Afbeelding 5

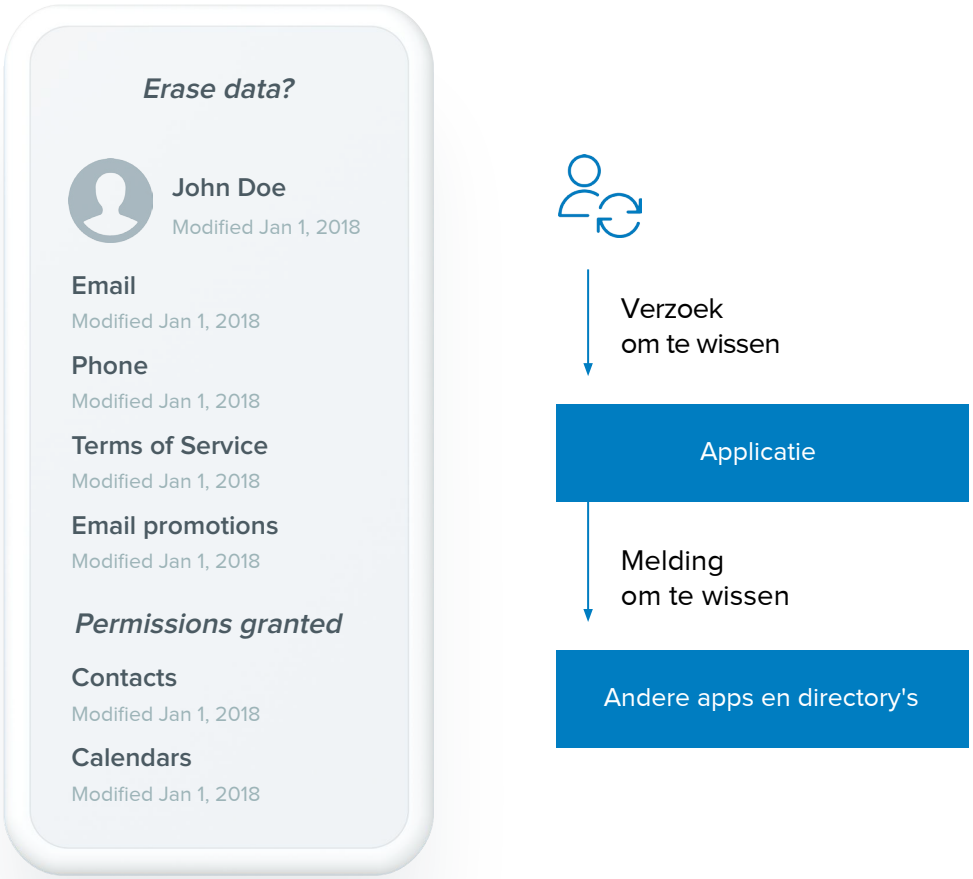
Om organisaties in staat te stellen te voldoen aan de vereisten voor overdraagbaarheid van data of het recht om verzamelde data te verkrijgen in een machineleesbare vorm, biedt de Okta-gebruikersinterface ook een functie om een CSV-bestand te downloaden dat vervolgens kan worden verstrekt aan de aanvrager. Developers kunnen ook een gebruikersinterface met een eigen merkidentiteit creëren door de API's van Okta te benutten en de data automatisch te leveren, zonder dat dit ten koste gaat van de customer experience.



Afbeelding 6

Hoe Okta het recht om te worden vergeten (wissen) beheert

Artikel 17 van de AVG bepaalt dat een betrokkene het recht heeft om data te laten wissen. Dit houdt in dat moderne organisaties de verantwoordelijkheid hebben om persoonsgegevens onverwijld te wissen na ontvangst van een verzoek daartoe.



Voor IT-beheerders betekent dit dat zij de persoonsgegevens moeten verwijderen die over iemand zijn verzameld. Hiertoe kunnen toestemmingsvoorkeuren, e-mailmarketingvoorkeuren en profieldata behoren. Bovendien moet ervoor worden gezorgd dat de persoonsgegevens van de aanvrager ook worden verwijderd uit eventuele downstream applicaties en data stores.

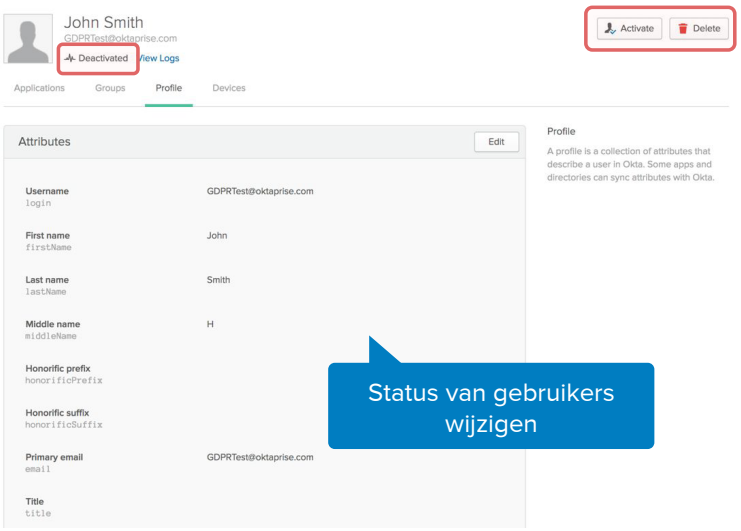
Het product waarmee het proces in dit geval kan worden vereenvoudigd, is Lifecycle Management. Hiermee wordt de provisioning en deprovisioning van gebruikersaccounts bij Okta beheerd. LCM biedt drie gebruikersstatuswaarden binnen de levenscyclus: Opschorten, Deactiveren/activeren en Verwijderen.

Door deze tool via een API te koppelen is het ook mogelijk om een krachtige automatische workflow te creëren voor personen die het recht om te worden vergeten willen uitoefenen. Het verwijderverzoek kan worden verzonden naar downstream applicaties, zodat IT-beheerders kunnen zorgen dat de desbetreffende persoonsgegevens worden verwijderd uit alle identity stores. Deze verzoeken worden gedocumenteerd via het systeemlogboek, zodat organisaties een audit trail van de getroffen maatregelen kunnen bijhouden met het oog op de compliance.

Geautomatiseerd verwijderen vanaf een centrale locatie

Verzoeken beheren met een gecentraliseerde identity

- Gebruikersstatus opschorten, deactiveren/reactiveren en verwijderen
- Geautomatiseerde workflows en selfservice beschikbaar via API
- Audit trail voor records



Hoe Okta helpt bij het melden van datalekken

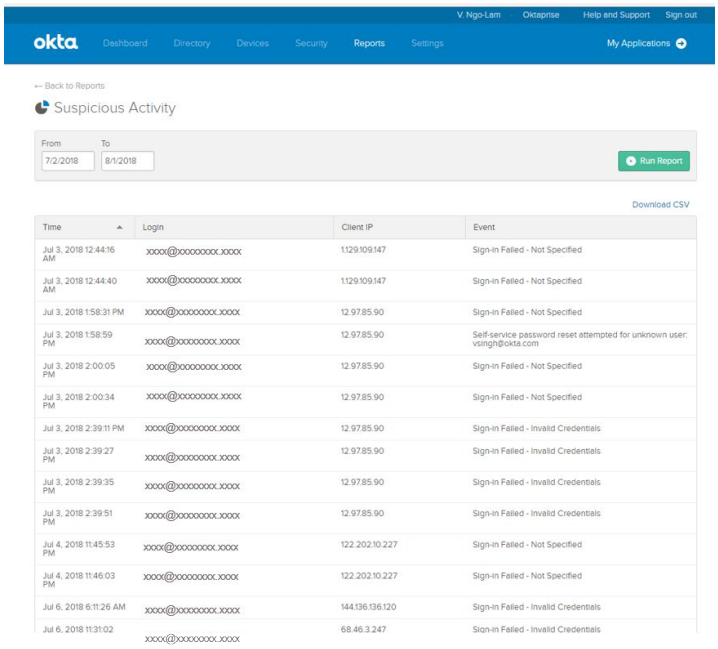
Op grond van artikel 33 en 34 van de AVG zijn organisaties die optreden als verwerkingsverantwoordelijke verplicht om een datalek in verband met persoonsgegevens zonder onredelijke vertraging en, zo mogelijk, uiterlijk 72 uur nadat zij er kennis van hebben genomen te melden aan de toezichthoudende autoriteit. Deze melding moet de volgende informatie bevatten:

- de aard van het datalek in verband met persoonsgegevens;
- de gevolgen van het datalek in verband met persoonsgegevens;
- de voorgestelde maatregelen ter beperking van de gevolgen;
- de contactgegevens van de functionaris voor gegevensbescherming.

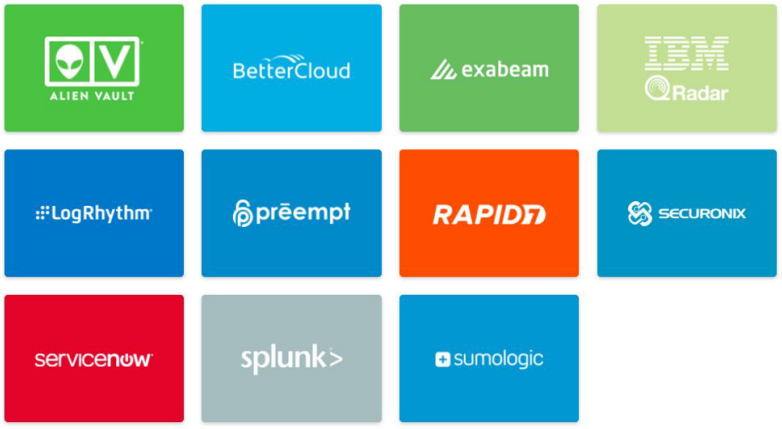
Rapport over datalekken

- Vaststellen wat er is gelekt
- Oorzaken onderzoeken
- Verdere schade beperken

Okta kan calamiteitenteams helpen bij hun verplichtingen met betrekking tot het datalek. Het systeemlogboek biedt calamiteitenteams een gedetailleerd overzicht van alle logins-activiteiten. Developers verkrijgen via de API van het systeemlogboek bovendien kant-en-klare gebruikersinterfaces/rapporten op basis van alle apps (cloud, mobiel, enzovoort). Hiermee kunnen organisaties vervolgens het datalek onderzoeken en bepaalde data leveren die vereist zijn op grond van de AVG, zodat er nauwelijks handmatige processen nodig zijn en de IT-beheerlast wordt verlicht.



Als Okta is verbonden met al uw apps, bieden standaardrapporten van het systeemlogboek ook informatie over toegangsrechten voor applicaties en de bijbehorende loginspogingen. Een voorbeeld van een dergelijk rapport is het rapport over verdachte activiteiten waarin de gebruikersnaam, het IP-adres en het tijdstip van de activiteit worden vastgelegd. Rapporten zoals deze verschaffen informatie over kwaadwillenden die mogelijk uw IT-infrastructuur proberen te infiltreren. Om te voldoen aan geavanceerdere use cases en een holistisch beeld van accountactiviteiten te bieden, beschikt over Okta tevens over integratieopties voor de belangrijkste SIEM-providers. Services zoals Splunk en Rapid 7 kunnen beveiligingsanalyses op een dieper niveau leveren.



Integraties

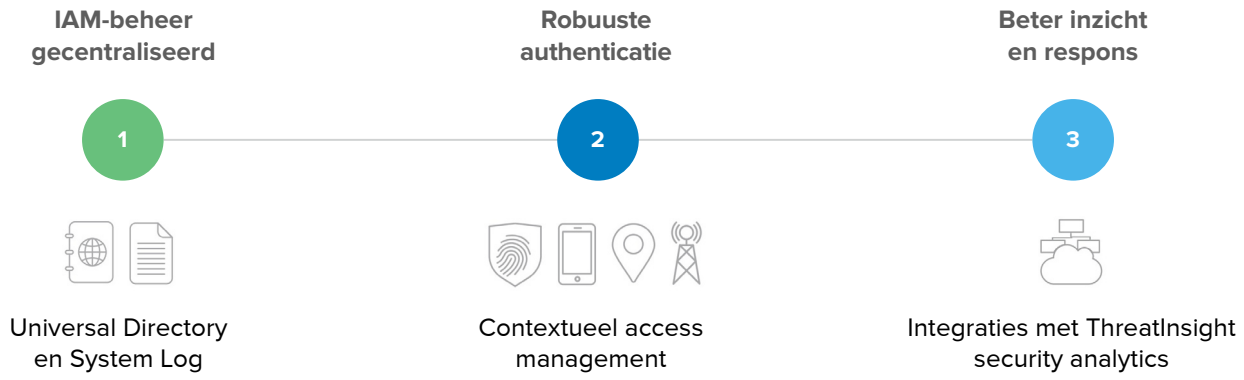
Deel IV:

Datalekken proactief voorkomen

Okta begrijpt dat klanten in geval van een datalek verplicht zijn om dit te melden aan de juiste instanties, maar het is nog beter om datalekken geheel te voorkomen. Daarom is het verstandig om ook andere producten uit de Okta-suite in overweging te nemen en beveiliging te beschouwen als een identity-gerelateerd probleem.

Door de opkomst van IoT-apparaten zijn organisaties tegenwoordig ook buiten de firewall kwetsbaar.

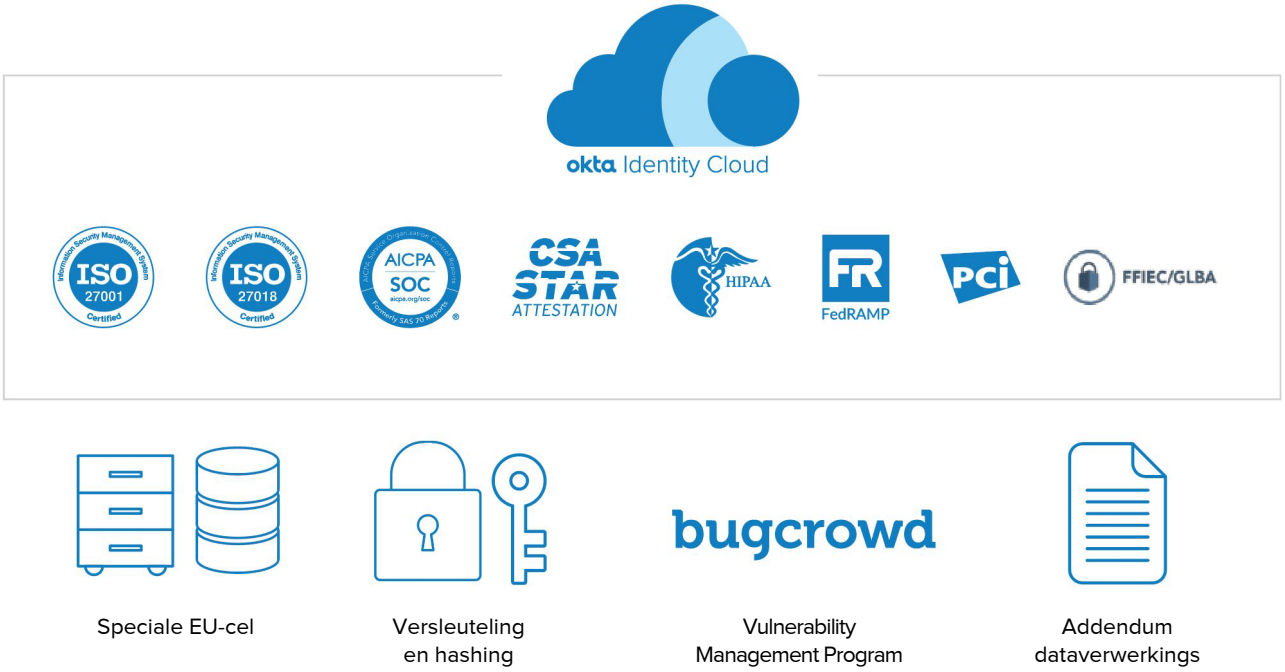
Okta's platform voor security op basis van identity werkt op 3 manieren:



Centralisering van identity en access management – Door één source of truth en inzicht in de back-end van accountactiviteit te bieden met Universal Directory en het systeemlogboek, kunnen identity's en toegang worden beheerd via een standaardgebruikersinterface of een aangepaste interface die wordt gemaakt met de API van Okta. Dit wordt beschreven onder Profieltoegang en -updates.

Robuustere authenticatie – SFA en 2FA zijn alweer verouderd. Voor moderne beveiliging moet contextafhankelijk access management worden gebruikt. Met contextafhankelijke toegang kunnen deze scenario's worden beheerd met aanpasbaar beveiligingsbeleid dat IT-beheerders eenvoudig kunnen implementeren via de gebruikersinterface van Okta. Ons aanpasbare MFA-product (AMFA) analyseert zaken zoals netwerkkenmerken, type apparaat, locatie en biometrische data en biedt daardoor een optimale combinatie van superieure enterprisebeveiliging en bruikbaarheid.

Inzicht bieden en respons ondersteunen - Klanten die in zee gaan met de toonaangevende identity provider kunnen identity-gebaseerde beveiliging naar een hoger niveau brengen door beheerde data van SIEM-providers uit het Okta Integration Network te benutten. Met meer dan 4300 klanten en 5000 partners is Okta als geen ander in staat om een verzameling best practices met betrekking tot verdachte toegangsverzoeken te bieden. Als bij een verzoek de identiteit van de gebruiker niet 100% zeker wordt geacht, wordt het authenticatieverzoek geanalyseerd met een risicobepalingsmechanisme, waarmee vervolgens het toegangsbeleid voor de klant kan worden vastgesteld. Okta biedt daarnaast instellingen om de oplossing aan te passen aan netwerkzones en te bepalen hoe vaak aanvullende MFA wordt gebruikt.



Deel V:

Ontwikkeld met privacy in gedachten

Okta Identity Cloud bevindt zich in de cloud en is ontworpen met beveiliging en privacy in gedachten. Okta beschikt over talrijke certificeringen in allerlei sectoren en tevens over diverse getuigschriften van derden. Daarmee maakt Okta zijn reputatie als toonaangevende identity provider meer dan waar.

Okta kan ook de volgende services bieden:

- Speciale EU-afdeling voor de AVG
- Versleuteling en hashing
- Programma voor het beheren van kwetsbaarheden
- Addendum over dataverwerking

Samenvattend is de benadering van Okta ter bescherming van persoonsgegevens gebaseerd op het concept dat klanten eigenaar zijn van hun data. Wij gebruiken alleen data om onze diensten te leveren. Bovendien verkopen wij geen klantdata en treffen wij de maatregelen die worden beschreven in onze Trust and Security Documentation om de data van onze klanten te beschermen en te beveiligen.

Over Okta

Okta is een toonaangevende, onafhankelijke identity provider voor enterprises. De Okta Identity Cloud stelt organisaties in staat om de juiste mensen op het juiste moment veilig te verbinden met de juiste technologieën. Met meer dan 6000 vooraf gedefinieerde integraties met applicaties en infrastructuurleveranciers, kunnen klanten van Okta gemakkelijk en veilig de beste technologieën gebruiken voor hun organisatie. Meer dan 6100 organisaties, waaronder 20th Century Fox, JetBlue, Nordstrom, Slack, Teach for America en Twilio, vertrouwen op Okta voor de bescherming van de identiteiten van hun personeel en klanten.

www.okta.com