CHANCEN DER DSGVO: KUNDENVERTRAUEN UND MARKENTREUE STÄRKEN

WIE CUSTOMER-IDENTITY- UND ACCESS-MANAGEMENT COMPLIANCE-PROBLEME LÖST UND DIE KUNDENBINDUNG FÖRDERT

WHITEPAPER

INHALTSÜBERSICHT

ZUSAMMENFASSUNG

Die Datenschutz-Grundverordnung (DSGVO) gehört zu den wichtigsten internationalen Datenschutzgesetzen der letzten 20 Jahre. Durch die Einführung strenger Kontrollen im Umgang mit personenbezogenen und sensiblen Daten sorgt sie für eine deutliche Verschärfung des Datenschutzes. Die EU-Verordnung stellt eine Reihe technischer und anderer Anforderungen an Organisationen, die Produkte oder Dienstleistungen an EU-Bürger verkaufen oder vermarkten, selbst wenn sie nicht in der EU ansässig sind. Obwohl schwerwiegende Konsequenzen bei Verstößen drohen, ist bereits jetzt abzusehen, dass viele Organisationen bis zum Inkrafttreten der DSGVO im Mai 2018 nicht ausreichend vorbereitet sein werden.

„Aktuellen Informationen des Datenspezialisten Alchemetrics zufolge könnten die von der britischen Datenschutzbehörde verhängten Geldstrafen als direkte Folge der DSGVO um beachtliche 4.500 % steigen."[1]

Führende Organisationen betrachten DSGVO-Compliance zu einem großen Teil als Erweiterung ihrer bestehenden Mitarbeitermanagement-, Kundenerfahrungs- oder Know Your Customer-Initiativen. Dieser Ansatz hat einen großen Vorteil: Neben der Umsetzung von Compliance-Vorgaben stärken Sie das Vertrauen und die Loyalität Ihres wertvollsten Gutes – Ihre Kunden – und bieten Ihren Mitarbeitern mehr Transparenz bei der Nutzung privater Mitarbeiterinformationen.

Ihre Organisation kann es sich nicht leisten, die Umsetzung der DSGVO-Bestimmungen aufzuschieben. Außerdem kann die Implementierung einer ganzheitlichen Identity- und Access-Management-Lösung sowohl für Ihre Mitarbeiter als auch für Ihre Kunden eine wichtige Rolle spielen.

Customer-Identity- und Access-Management(CIAM)-Lösungen bieten zentrale Funktionen, die Sie nicht nur bei der Umsetzung der DSGVO-Vorgaben unterstützen, sondern auch dazu beitragen, dass Sie Ihre Kunden aus einer völlig anderen Perspektive betrachten. Mit CIAM können Sie die Herausforderungen bei der DSGVO-Umsetzungen (z. B. Erfassen und Verwalten von Einwilligungen, Data-Access-Governance und Anwendungssicherheit) als Chance nutzen, um das Vertrauen Ihrer Kunden während Ihrer digitalen Transformation zu stärken.

[1] *Michael Hill, „GDPR: One Year and Counting" (DSGVO: Noch ein Jahr und die Uhr tickt), Infosecurity Magazine, 25. Mai 2017, https://www.infosecurity-magazine.com/news-features/gdpr-one-year-and-counting/*

EINLEITUNG

HINTERGRUND

Das EU-Parlament hat die DSGVO nach vier Jahren intensiver Auseinandersetzung, Diskussion und Vorbereitung verabschiedet. Ihr Vorgänger – die Datenschutzrichtlinie 95/46/EG – regelte die Verarbeitung personenbezogener Daten in der EU, galt aber weithin als nicht mehr ausreichend für den Schutz personenbezogener Daten in der heutigen digitalen Welt.

Mit der DSGVO sollen Datenschutzbestimmungen besser durchsetzbar und einheitlich gestaltet werden. Bestimmungen zu neuen Datenkategorien, erweiterten geografischen Geltungsbereichen sowie Datenzugriffs- und -löschrechten sind nur einige Bereiche, die nun verschärft wurden.

AUSWIRKUNGEN

Und was bedeutet das für Ihre Organisation?

Wenn Sie Ihre Produkte oder Dienstleistungen an EU-Bürger vermarkten oder verkaufen oder Daten von EU-Bürgern sammeln oder verarbeiten, muss Ihre Organisation – egal, wo sie niedergelassen ist – die Vorgaben der DSGVO erfüllen. Anderenfalls riskieren Sie empfindliche Geldstrafen bis zu 4 Prozent Ihres weltweit erzielten Jahresumsatzes oder 20 Millionen EUR, je nachdem, welcher Betrag höher ist.

Und vergessen Sie nicht, dass der Begriff der personenbezogenen Daten sehr breit gefasst ist. Wenn ein EU-Bürger beispielsweise Ihre Website besucht, werden seine Browsing-Daten schon als personenbezogene Daten eingestuft und erfordern daher eine Benutzereinwilligung.

Die DSGVO hat also weitreichende Auswirkungen auf sämtliche Unternehmensbereiche, nicht nur auf Geschäftsprozesse und die IT. In diesem Whitepaper beschäftigen wir uns mit einigen wichtigen technischen Anforderungen, den damit verbundenen Herausforderungen sowie mit Lösungen, wie Sie diese bewältigen können – während Sie gleichzeitig für eine nahtlose Kundenerfahrung sorgen.

[2] *„Comparison of General Data Protection Regulation and Data Protection Directive“ (Datenschutz-Grundverordnung und Datenschutzrichtlinie – ein Vergleich), The Centre for Internet & Society, letzter Abruf am 2. Februar 2018, https://cis-india.org/internet-governance/blog/comparison-of-general-data-protection-regulation-and-data-protection-directive*

WICHTIGE TECHNISCHE ANFORDERUNGEN DER DSGVO

Die Bestimmungen der DSGVO sind in den jeweiligen Gesetzesartikeln festgeschrieben und viele von ihnen regeln, wie Daten gesammelt, gespeichert, aufgerufen, geändert, transportiert, gesichert und gelöscht werden sollen. Diese Bestimmungen sind äußerst breit gefasst und müssen von Unternehmen im Rahmen prozessbezogener, organisatorischer und technischer Veränderungen umgesetzt werden. In diesem Whitepaper beschäftigen wir uns mit den technischen Anforderungen, die unseren Kunden am häufigsten Kopfzerbrechen bereiten.

EINWILLIGUNG

Die Artikel 7, 8 und 9 regeln, wie Einzelpersonen ihre Einwilligung geben und können daher zusammengefasst werden.
(HINWEIS: Bei allen hier aufgeführten Artikelbeschreibungen handelt es sich um Zusammenfassungen von Ping):

Der Verantwortliche muss die Einwilligung der betroffenen Person zur Erfassung, Speicherung und Verwendung personenbezogener Daten einholen und aufzeichnen. Organisationen müssen die unmissverständliche Einwilligung der betroffenen Person vor der Erfassung der Daten einholen. Dies beinhaltet die ungebündelte Einwilligung in Bezug auf Datenfelder sowie die Einwilligung in Bezug auf die Anwendungsfälle. Diese Einwilligung muss auf nachprüfbare, sichere Weise gespeichert werden. Darüber hinaus müssen Sie Ihren Kunden das Recht einräumen, ihre Einwilligung jederzeit zu widerrufen. Das hierfür eingesetzte Verfahren darf nicht komplizierter sein als das für die ursprüngliche Zustimmung verwendete Verfahren.

DATENZUGRIFF UND BERICHTIGUNG

In den Artikeln 15 und 16 geht es darum, dass Einzelpersonen auf Daten zugreifen und Ungenauigkeiten berichtigen können.

LÖSCHUNG

Im Artikel 17 geht es um die Löschung von Daten:

Die betroffene Person hat das Recht, den Verantwortlichen zu bitten, alle personenbezogenen Daten zu „vergessen" oder zu löschen. Jedoch können andere Bestimmungen, die eine Archivierung erfordern, Vorrang vor der Löschung haben.

DATENÜBERTRAGBARKEIT

Artikel 20 schreibt den Verantwortlichen vor, wie Daten strukturiert und übermittelt werden:

Die betroffene Person hat das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, zu erhalten. Die Daten müssen in einem gängigen, maschinenlesbaren Format strukturiert sein. Darüber hinaus kann die betroffene Person verlangen, dass die Daten direkt an einen Dritten übermittelt werden.

DATENSCHUTZ DURCH TECHNIKGESTALTUNG

Artikel 25 beschreibt, wie Datensysteme konzipiert sein sollten:

Der Verantwortliche muss Systeme entwickeln, um die Integrität personenbezogener Daten risikobasiert zu schützen. Dies umfasst eine Reihe an Datenschutztechniken, wie Speicherung, Backup, Wiederherstellung, Auslesen und Minimierung, wobei Unternehmen nur die erforderlichen Daten erheben dürfen.

DATENSICHERHEIT

In Artikel 32 sind Richtlinien zum Schutz personenbezogener Daten definiert.

Wichtige Definitionen im Rahmen der DSGVO*

Verantwortlicher: Die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Betroffene Person: Eine identifizierbare natürliche Person, die mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann.

Personenbezogene Daten: Alle Informationen, die sich auf die betroffene Person beziehen.

Einwilligung: Jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

*Auszug aus der *Datenschutz-Grundverordnung*

Der Verantwortliche muss Systeme zum Schutz personenbezogener Daten entwickeln und zu diesem Zweck angemessene technische und organisatorische Maßnahmen ergreifen. Mithilfe der sogenannten Pseudonymisierung sollten Daten in einem Format gespeichert bzw. abgelegt werden, das die personenbezogenen Informationen unkenntlich macht. Verschlüsselung ist eine der Techniken, um diese Bestimmung zu erfüllen. Organisationen sind zudem dafür verantwortlich, die Vertraulichkeit, Integrität und Verfügbarkeit ihrer Datenprozesse auf Dauer sicherzustellen. Anhand regelmäßiger Tests sollte geprüft werden, ob eine rasche Wiederherstellung der Verfügbarkeit und des Zugriffs auf die Daten bei einem Zwischenfall sichergestellt ist.

HERAUSFORDERUNGEN DER DSGVO FÜR UNTERNEHMEN

Obwohl zahlreiche Organisationen bereits Systeme implementiert haben, die den Bestimmungen der DSGVO teilweise oder ganz entsprechen, bereitet die vollständige Umsetzung der DSGVO noch vielen Unternehmen Kopfzerbrechen.

HERAUSFORDERUNG NUMMER 1: UNZUREICHENDE EINWILLIGUNG

Die in der Vergangenheit geltenden Mindestvoraussetzungen in Bezug auf die Einwilligung reichen unter der DSGVO nicht mehr aus. Anstelle einer in manchen Fällen erlaubten impliziten oder Opt-out-Einwilligung, müssen Kunden jetzt ihre unmissverständliche Einwilligung in Form einer Erklärung oder klaren Handlung geben, beispielsweise durch Markieren eines Online-Kontrollkästchens oder Ausfüllen eines Online-Formulars. Als verantwortliche Stelle muss die Organisation nachweisen, dass die Einwilligungsanfrage auf klare und verständliche Weise präsentiert wurde.

Wenn Sie spezielle Datenkategorien erfassen, unterliegt die ausdrückliche Zustimmung einem noch höheren Standard. Darüber hinaus müssen Einwilligungen für mehr Szenarien als jemals zuvor eingeholt werden. Beispielsweise gelten Browserdaten von Anwendern als personenbezogene Daten und erfordern ein ausdrückliches Einverständnis zur Datenerfassung. Wenn Ihr Unternehmen dies nicht unterstützt, müssen Sie Ihre Umgebung auf den neuesten Stand bringen.

HERAUSFORDERUNG NUMMER 2: DATENSILOS

Nehmen wir an, ein Kunde kauft über Ihre Unternehmenswebsite ein. Möglicherweise speichert Ihr Unternehmen Browserdaten in einem Analysesystem, weitere Leaddaten in Ihrem E-Commerce-System, die Kaufhistorie in einem Auftragsabwicklungssystem und Anmeldedaten sowie weitere Identitätsdaten in einem anderen System. Isolierte Daten wie diese erschweren die Umsetzung der DSGVO-Bestimmungen in Bezug auf den Datenzugriff und die Übertragbarkeit. Außerdem ist es unwahrscheinlich, dass all diese heterogenen Systeme die Anforderungen an Datenschutz und Sicherheit durch Technikgestaltung erfüllen.

HERAUSFORDERUNG NUMMER 3: FEHLENDE GOVERNANCE

Den Zugriff von Anwendungen auf Kundenidentitäts- und -profildaten so weit wie möglich zu beschränken ist nicht nur eine gute Geschäftspraktik – auch die DSGVO schreibt bindend vor, dass Unternehmen spezielle Regeln erstellen müssen, um den Zugriff von Anwendungen auf nicht erforderliche Kundendaten einzuschränken. Ist dies noch nicht erfolgt, müssen Unternehmen anwendungsbezogene Datenzugriffsprozesse anhand zentralisierter Governance-Regeln für den Datenzugriff in Bezug auf die Einwilligung, Datenschutzeinstellungen und Unternehmensanforderungen anpassen und durchsetzen.

HERAUSFORDERUNG NUMMER 4: SCHWACHE ANWENDUNGSSICHERHEIT

Organisationen hatten schon lange vor der DSGVO mit großen Sicherheitsherausforderungen zu kämpfen. Jetzt allerdings wurden die Anforderungen noch einmal deutlich verschärft. Kundenbezogene Daten, die fragmentiert und ungeschützt auf der Datenebene vorliegen, sind anfällig für Sicherheitsverletzungen und schwächen das Sicherheitsprofil Ihrer Anwendungen. Zudem wird dadurch die Einhaltung der DSGVO-Bestimmung erschwert, wonach personenbezogene Daten mittels Technikgestaltung geschützt werden müssen.

HERAUSFORDERUNG NUMMER 5: EINGESCHRÄNKTER SELF-SERVICE-ZUGRIFF

Können Ihre Kunden selbstständig ihre Profile und Präferenzen verwalten? Werden diese Präferenzen konsequent über alle Geräte und Kanäle hinweg durchgesetzt? Ist Ihre Organisation in der Lage, unterschiedliche Arten strukturierter und unstrukturierter Präferenzdaten einfach zu speichern und auszulesen? Wenn Sie auch nur eine dieser Fragen mit „nein" beantworten, müssen Sie den Self-Service-Zugriff Ihrer Kunden dringend verbessern, da Sie sonst die Vorgaben der DSGVO nicht erfüllen.

WIE CIAM ZUR UMSETZUNG DER DSGVO BEITRÄGT

Diese Herausforderungen mögen vielleicht schwierig erscheinen, doch sie lassen sich bewältigen. Mit CIAM kann Ihre Organisation nicht nur viele mit der DSGVO verbundene Herausforderungen lösen, sondern darüber hinaus auch noch eine sichere, komfortable und personalisierte Kundenerfahrung über alle Kanäle und Geräte hinweg bereitstellen.

SICHERHEIT + COMPLIANCE + KUNDENERFAHRUNG = ERFOLG

Die meisten Organisationen sind davon überzeugt, dass ganzheitliche Kundenlösungen einen größeren Nutzen für Ihr Unternehmen haben und sich eher langfristig bewähren. Wenn Sie mit einem umfassenden Blick auf Ihre Customer Journey beginnen und diese Erkenntnisse in ein Compliance-Rahmenwerk einfließen lassen, führt dies zu einer besseren Compliance-Lösung mit einem erheblich höheren Nutzen für Ihre Organisation.

Werfen wir dazu einen kurzen Blick auf die wichtigsten Phasen einer typischen Kundenreise und schauen wir uns an, inwiefern in den jeweiligen Phasen DSGVO-Bestimmungen zu erfüllen sind.

Website-Besuch
In dieser Phase ist ein Kunde möglicherweise nur ein anonymer Interessent, aber sobald Sie mit Cookies personenbezogene Browsingdaten erfassen – und sich bei der Datenverarbeitung nicht auf eine andere Rechtsgrundlage berufen können – ist eine Einwilligung erforderlich. Sobald Daten auf eine IP-Adresse zurückzuführen sind oder andere personenbezogene Daten erhoben werden, müssen Sie eine Einwilligung einholen.

Kauf
Da sowohl Gäste als auch registrierte Benutzer Einkäufe tätigen können, ist die Einwilligung zur Nutzung personenbezogener Daten erforderlich. Je nachdem, wie die Daten genutzt werden, ist es in dieser Phase entscheidend, dass die Daten geschützt werden und registrierte Kunden Funktionen zur Accountverwaltung nutzen können. Zudem muss der Prozess zum Einholen der Kundeneinwilligung und zur schrittweisen Vervollständigung eines Kundenprofils einfach und nahtlos gestaltet sein. Hierzu gibt es Bestimmungen, nach denen die Einwilligungsanfrage klar und verständlich formuliert sein und sich klar von anderen Inhalten der Kommunikation abheben muss.

Registrierung
Eine weitere Phase, in der personenenbezogene Daten erhoben werden, ist die Registrierung eines anonymen Benutzers als Kunde. Hier kann eine Einwilligung erforderlich sein. Außerdem müssen die entsprechenden Daten sicher und geschützt sein. Die Weitergaben solcher Profildaten an Dritte, wie z. B. Datenimporteuren, ist ebenfalls in der DSGVO geregelt.

Account-Management
Registrierte Benutzer benötigen Zugriff, damit sie ihre Profildaten verwalten und aktualisieren können. Dazu sind Funktionen erforderlich, die Datenzugriff und Berichtigung unterstützen. In dieser Phase müssen Benutzer normalerweise auch eine Kopie ihrer Daten (Datenübertragbarkeit) und gegebenenfalls die Löschung ihrer Account- und personenbezogenen Daten (Recht auf Löschung bzw. auf Vergessenwerden) verlangen können.

Die oben genannten Phasen müssen möglichst einfach gestaltet sein, da schlecht implementierte DSGVO-Funktionen die Kundenreise beeinträchtigen können.

CIAM-Lösungen verbessern nicht nur die Sicherheit und den Datenschutz, sie ermöglichen Organisationen auch eine effektive Interaktion mit ihren Kunden. Mit der CIAM-Lösung von Ping Identity können Sie DSGVO-Compliance als Chance für Ihr Unternehmen nutzen, sich vom Wettbewerb abzuheben, das Vertrauen Ihrer Kunden zu stärken und Ihren Markenwert zu steigern.

SYNCHRONISIERTE UND KONSOLIDIERTE KUNDENDATEN

Wenn Sie einheitliche Kundenprofile schaffen möchten, müssen Sie in der Lage sein, Ihre Kundendaten zu synchronisieren und zu konsolidieren. Setzen Sie jedoch – wie viele Unternehmen – auf Identitätssilos, trägt dies zu einer komplexen IT-Landschaft bei, die unter der DSGVO schwer zu verwalten ist. Doch zum Glück gibt es im Rahmen von CIAM eine Antwort auf diese Herausforderung.

Eine umfassende CIAM-Lösung konsolidiert Identitässilos mit Tools wie bidirektionale Synchronisierung in Echtzeit oder mit Zeitplan, Mappen von Datenschemas, Unterstützung für mehrere Verbindungsmethoden/-protokolle und integrierte Redundanz, Failover-Funktion und Lastverteilung. Das Synchronisieren und Konsolidieren von Kundendaten ist nicht nur eine gute Strategie, um die Vorgaben der DSGVO zu erfüllen, Ihre Organisation kann so auch die Kundenerfahrung verbessern.

EINFACHES ERFASSEN UND VERWALTEN DER KUNDENEINWILLIGUNG

Ein umfassendes CIAM-System bietet naturgemäß eine maßgeschneiderte Lösung zur nahtlosen Einwilligungserfassung und -verwaltung. CIAM vereinfacht die Einwilligungserfassung über mehrere Kanäle hinweg, sodass Sie sich auf die Erfassung für bestimmte Attribute konzentrieren können. So haben Sie die Möglichkeit, Einwilligungsentscheidungen auf der Grundlage zentraler Regeln durchzusetzen, die auf lokalen Bestimmungen wie der DSGVO, Unternehmensrichtlinien, branchenspezifischen Vorgaben und Kundeneinwilligungen zur Datenweitergabe an interne Teams, externe Partner oder andere Gruppen basieren können.

Darüber hinaus ermöglichen viele CIAM-Systeme eine Transaktionseinwilligung und -genehmigung – beides wichtige Anwendungsfälle bei der Multifaktor-Authentifizierung (MFA). Und nicht zuletzt erlauben CIAM-Systeme dem Kunden, seine Einwilligung jederzeit zu widerrufen und erfüllen so eine zentrale Vorgabe der DSGVO.

SELBSTVERWALTETE KUNDENPROFILE

Im Rahmen der DSGVO sollten Ihre Kunden in der Lage sein, drei Arten von personenbezogenen Profilinformationen einzusehen und zu verwalten: Profildaten, persönliche Präferenzen und Einwilligungen. Dies ist ein weiterer Bereich, in dem robuste CIAM-Systeme punkten können, da sie mit ihren vorgefertigten Benutzeroberflächen und APIs Benutzern die selbstständige Verwaltung ihrer Profile erlauben.

Mit CIAM können Kunden ihre Daten abrufen und ändern bzw. verlangen, dass Änderungen durchgeführt werden. CIAM ermöglicht Endbenutzern außerdem, persönliche Präferenzen einzusehen und setzt diese konsequent über die unterschiedlichen Kanäle hinweg durch. Kunden können auch ihre Einwilligungsdaten einsehen und nachverfolgen, von wann ihre Einwilligung datiert, worauf sich diese genau bezieht und an wen ihre Daten weitergegeben werden dürfen, etc.

DATA-ACCESS-GOVERNANCE

Data-Access-Governance gehört seit langem zu den zentralen Komponenten einer soliden CIAM-Strategie. Wenn Anwendungen unbeschränkten Zugriff auf Kundendaten haben, ist großer Schaden vorprogrammiert, da das Risiko für Sicherheitsverletzungen und Vertrauensverluste steigt. Setzen Sie stattdessen auf CIAM und holen Sie das Maximum aus Ihren Daten heraus.

CIAM ermöglicht zentralisierte Governance-Regeln für den Datenzugriff mit einer fein abgestimmten Kontrolle auf der Ebene einzelner Attribute, sodass interne und externe Anwendungen nur auf die Identitätsattribute zugreifen können, die auch wirklich benötigt werden. Mit CIAM können Sie den Zugriff auf Kundendaten über ein zentrales System kontrollieren und prüfen. Auf diese Weise erfüllen Sie die DSGVO sowie andere Vorgaben, wie z. B. gesetzliche Bestimmungen, oder branchenspezifische Richtlinien.

KONTROLLE DES GLOBALEN NAMENSRAUMS

CIAM-Systeme verfügen über zahlreiche Funktionen zur Verwaltung eines globalen Namensraums. Erstens können Sie „Data Residency“ erreichen, indem Sie Daten mit einem Proxyserver an den richtigen Ort leiten. Zweitens können Sie partielle Datensynchronisierungen einrichten und gegebenenfalls partielle Kopien Ihrer Daten anlegen. Und drittens können Sie – wie bereits erwähnt – festlegen, auf welche Daten Anwendungen attributbezogen auf der Grundlage geografischer, unternehmensweiter, branchenspezifischer oder anderer Richtlinien zugreifen können. Dies unterstützt

Sie bei der Umsetzung der DSGVO-Vorgaben in Bezug auf die Datenübertragbarkeit sowie weiterer Vorgaben zu Datensicherheit und Datenschutz durch Technikgestaltung.

SICHERE KUNDENDATEN

Natürlich bietet ein verwalteter globaler Namensraum keine absolute Sicherheitsgarantie. Daher ist es extrem wichtig, beim Schutz von Kundenidentitäten auf der Datenebene anzusetzen. Statt einer Fragmentierung, bei der einige Bereiche weniger geschützt sind, gewährleistet dieser zentralisierte Ansatz einen hohen Schutz über alle Anwendungen hinweg.

Ein solides CIAM-System bietet zahlreiche zentralisierte Sicherheitsfeatures auf der Datenebene wie Datenverschlüsselung in jedem Zustand (im ruhenden Zustand, während der Übertragung und Verwendung), Limit beim Zugriff auf Datensätze, manipulationssichere Anmeldung, aktive und passive Warnmeldungen, Integration mit Überwachungstools von Drittanbietern, etc. Diese zentralisierte, sichere Umgebung unterstützt Sie dabei, die Datensicherheitsvorgaben der DSGVO zu erfüllen.

CIAM-Funktion	Relevante DSGVO-Artikel
Synchronisierte und konsolidierte Kundendaten	Artikel 15, 16, 17, 20 und 25
Einfache Einwilligungserfassung und -verwaltung	Artikel 7, 8 und 9
Selbstverwaltete Kundenprofile	Artikel 15 und 16
Data-Access-Governance	Artikel 32
Kontrolle des globalen Namensraums	Artikel 25
Sichere Kundendaten	Artikel 32

ANSÄTZE ZUR CIAM-IMPLEMENTIERUNG UNTER DER DSGVO

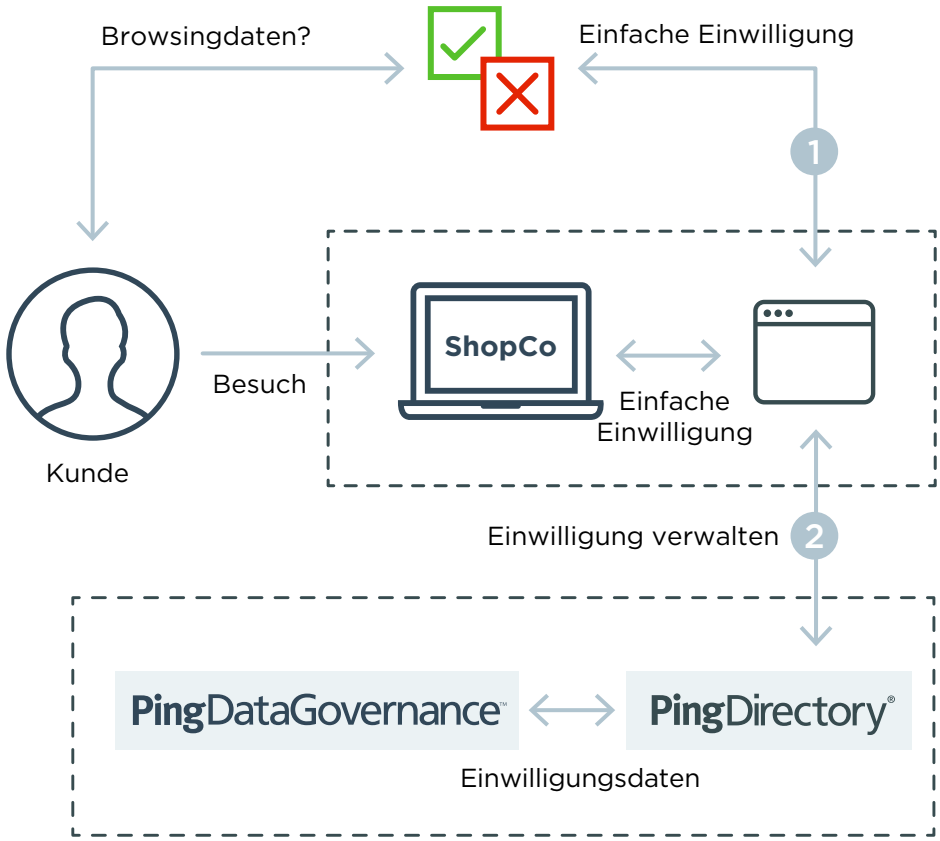
CIAM ALS WICHTIGES FUNDAMENT

Viele CIAM-Komponenten bieten wesentliche Bausteine für eine DSGVO-Lösung, die über Compliance hinausgeht. Zudem zeichnen sich Lösungen, die mit Blick auf die digitale Transformation konzipiert wurden, langfristig durch einen größeren Nutzen und eine höhere Kapitalrendite aus als Maßnahmen, die nur auf Compliance abzielen. Denken Sie zum Beispiel daran, was passiert, wenn neue Verordnungen verabschiedet oder bestehende überarbeitet werden. Rein auf Compliance ausgerichtete Lösungen unterstützen Veränderungen dieser Art in der Regel nicht. Eine umfassendere Businesslösung wie CIAM kann und sollte dagegen die Flexibilität und Erweiterbarkeit bieten, um neue oder veränderte Anforderungen zu erfüllen.

Sehen wir uns also etwas genauer an, wie sich einige gängige DSGVO-Anwendungsfälle mithilfe zentraler CIAM-Komponenten bewältigen lassen.

ARCHITEKTUR FÜR EINWILLIGUNGEN ANONYMER NUTZER UNTER DER DSGVO

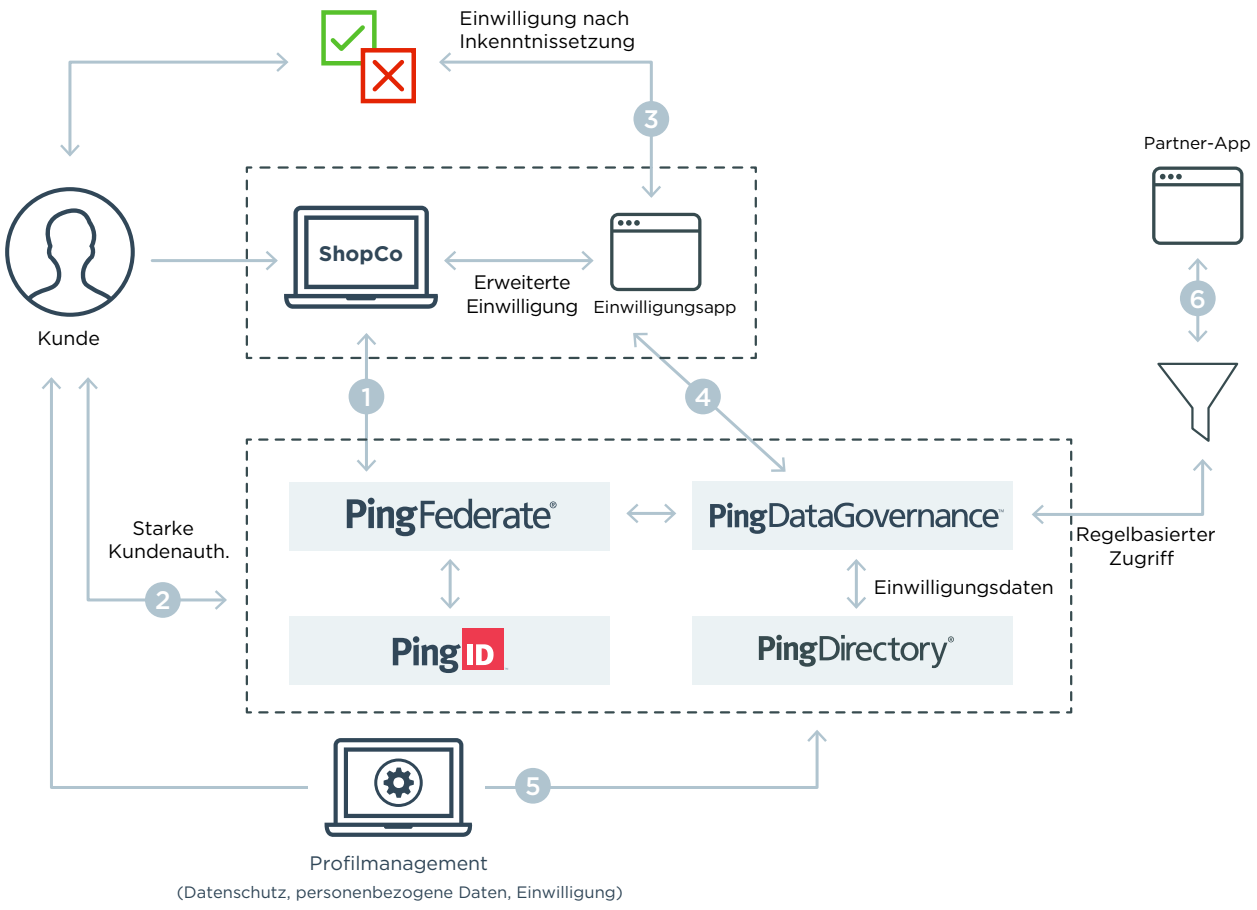
Die Einwilligungserfassung beginnt mit anonymen Nutzern, die Ihre Website besuchen. Wenn Sie IP-Adressen und andere persönliche Informationen erheben und diese Daten in Cookies speichern, müssen Sie diese Einwilligungen verwalten. Die Grafik unten zeigt eine grundlegende Lösungsarchitektur, um die Einwilligung anonymer Nutzer zu erfassen.



ARCHITEKTUR FÜR KUNDENEINWILLIGUNGEN UND DATENZUGRIFF UNTER DER DSGVO

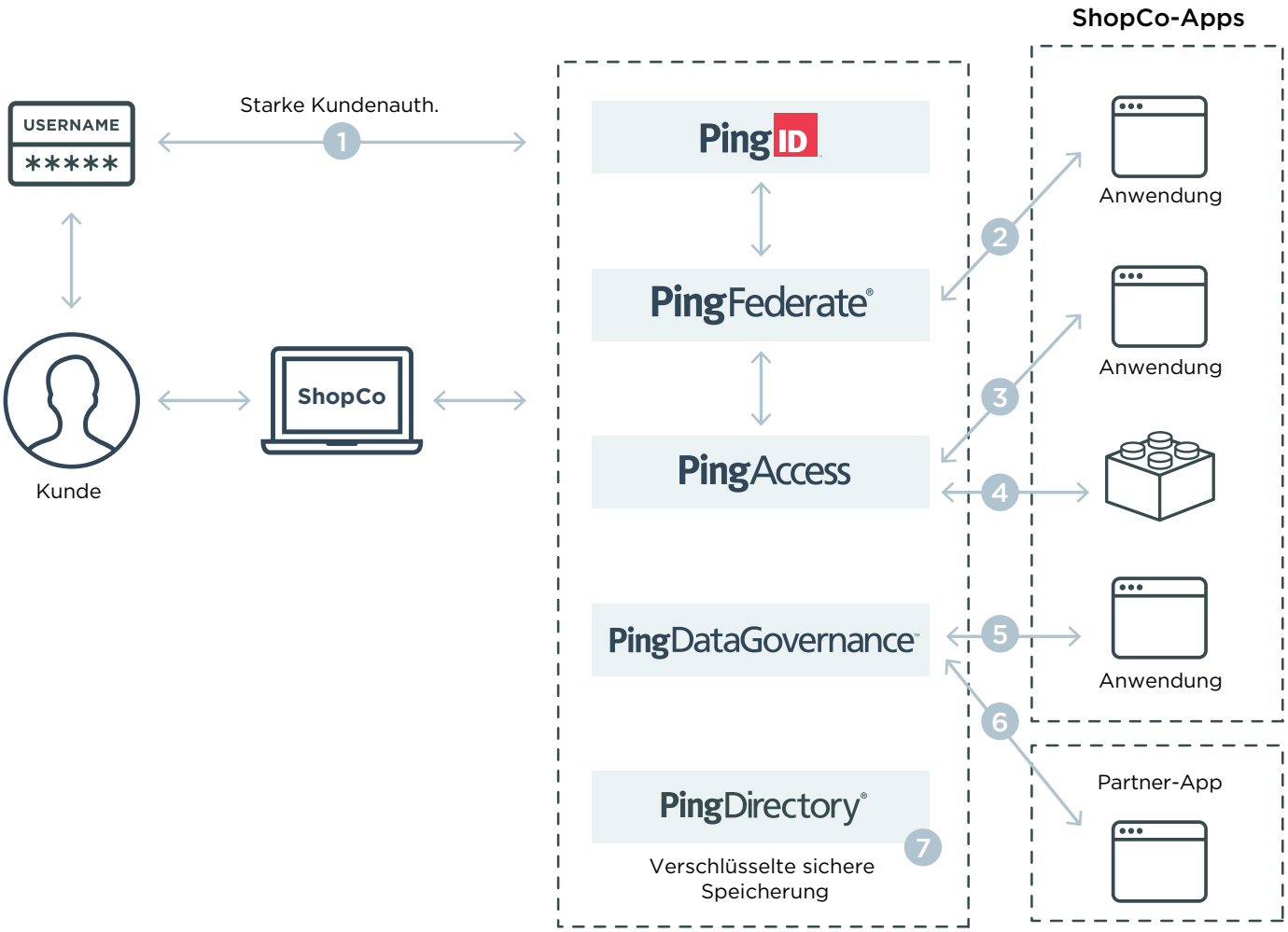
Für registrierte Nutzer muss Ihre Lösung andere Funktionen bereitstellen. Eine starke Kundenauthentifizierung, wie sie im Finanzsektor vorgeschrieben und in anderen Branchen ebenfalls sinnvoll ist, muss sicherstellen, dass nur die richtigen Kunden auf ihre eigenen Accounts zugreifen können und eine sichere Benutzererfahrung gewährleisten.

Darüber hinaus müssen Einwilligungen laufend verwaltet werden. Über die Profilverwaltungsoberfläche sollten Kunden vollen Datenzugriff erhalten, damit sie je nach Belieben ihre personenbezogenen Daten verwalten und aktualisieren können. Und schließlich ist auch ein kontrollierter Datenzugriff für andere Anwendungen und Partner wichtig.



ARCHITEKTUR FÜR DATENSCHUTZ UND -SICHERHEIT UNTER DER DSGVO

Es ist enorm wichtig, sich über alle Funktionen bewusst zu sein, die dem Schutz personenbezogener Daten dienen. Dies fängt bei der Authentifizierung an, schließt aber auch Datenzugriffskontrollen für Anwendungen und APIs sowie eine sichere Datenspeicherung ein.



FAZIT

Robuste CIAM-Lösungen bieten wichtige Funktionen wie Datenkonsolidierung, Einwilligungserfassung und -verwaltung, Data-Access-Governance und End-to-End-Sicherheit, um Ihr Unternehmen bei der Umsetzung der DSGVO-Vorgaben zu unterstützen. Darüber hinaus tragen CIAM-Best Practices mittels Datenkonsolidierung und einer verbesserten Kontrolle und Governance Ihrer Daten zu einer effizienten und kosteneffektiven Umsetzung der DSGVO-Vorgaben bei. Gleichzeitig verbessern sie die Sicherheit und optimieren die Benutzererfahrung.

Am meisten profitieren Organisationen, die mehr als nur Compliance im Blick haben. Mit CIAM können sie eine sichere, nahtlose Erfahrung über alle Kanäle und Geräte hinweg bereitstellen und so Kundenvertrauen und Markentreue verbessern.

Die Ping Identity-Plattform stellt standardmäßig wichtige Funktionen bereit, um technische DSGVO-Anforderungen zu erfüllen. Mit unserer führenden CIAM-Lösung können Sie DSGVO-Compliance als Chance nutzen, um Ihre Kunden enger an sich zu binden, Ihr Vertrauen zu stärken und Ihr Engagement zu steigern.

Unter www.pingidentity.com/GDPR erfahren Sie, wie die CIAM-Lösungen von Ping Identity Ihre Organisation unterstützen können.

#3257 | 02.18 | v00b