LÖSUNG IM ÜBERBLICK
EU-DSGVO

DSGVO-Compliance: Wie können Sie sich auf die neue Verordnung einstellen?

ca technologies

Unternehmen halten schon seit über zwei Jahrzehnten Datenschutzrichtlinien und -verordnungen ein. Die Datenschutz-Grundverordnung (DSGVO), eine Neufassung vorhandener Datenschutzgesetze der Europäischen Kommission, dient dazu, diese Gesetze im Interesse der EU-Bürger zu verschärfen und zu vereinheitlichen. Die Hauptziele der DSGVO bestehen darin, Bürgern mehr Kontrolle über ihre personenbezogenen Daten zu ermöglichen und das regulatorische Umfeld für internationale Unternehmen zu vereinfachen. Was müssen Unternehmen, die bereits die Richtlinie 95/46/EG einhalten, in Bezug auf ihre Technologien unternehmen, um die DSGVO einzuhalten?

Abschnitt 1:

Einführung in die DSGVO

Ab dem 25. Mai 2018 muss jedes Unternehmen, das personenbezogene Daten von EU-Bürgern verarbeitet, die DSGVO einhalten. Diese Verordnung führt neue Anforderungen an den Datenschutz ein, die Auswirkungen auf die meisten Unternehmen in allen Branchen haben werden. Unternehmen, die die DSGVO nicht einhalten, riskieren Geldbußen von bis zu 20.000.000 € oder bis zu 4 % ihres weltweiten Umsatzes, je nachdem, welcher der Beträge höher ist.

Während die DSGVO die Datenschutzvorschriften verschärft, hat sie zugleich das Ziel, die Datenschutzgesetze innerhalb der Europäischen Union (EU) zu vereinheitlichen. Dies sollte Unternehmen in gewissem Maße helfen, stärker standardisierte Datenschutzrichtlinien und -prozesse einzuführen.

In der folgenden Tabelle sind die Anforderungen der DSGVO auf abstrakter Ebene kategorisiert:

Kategorie	Anforderungen
Rechte betroffener Personen	1. Betroffene Personen (Personen, um deren Daten es geht – siehe Definition 1) haben folgende Rechte: a. Auskunftsrecht zu ihren Daten b. Berichtigen, Löschen („Recht auf Vergessenwerden“) und Einschränken der Verarbeitung (siehe Definition 2) c. Datenübertragbarkeit d. Einlegen von Widerspruch gegen die Verwendung ihrer Daten
Rechenschaftspflicht	2. Diejenigen, die personenbezogene Daten verarbeiten, haben folgende Pflichten: a. Umsetzung geeigneter technischer und organisatorischer Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß der DSGVO erfolgt b. Einholen der Einwilligung der betroffenen Person für bestimmte Datenverarbeitungstätigkeiten c. Umsetzung geeigneter Datenschutzrichtlinien und -prozesse d. Führen eines Verzeichnisses aller Verarbeitungstätigkeiten e. Melden von Verletzungen des Schutzes personenbezogener Daten an Aufsichtsbehörden f. Benachrichtigen der betroffenen Person bei bestimmten Verletzungen des Schutzes personenbezogener Daten g. Gegebenenfalls Benennen eines Datenschutzbeauftragten
Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	3. Umsetzen geeigneter technischer und organisatorischer Maßnahmen, für die Folgendes gilt: a. Sie sind dafür ausgelegt, Datenschutzgrundsätze wie die Datenminimierung und die Pseudonymisierung wirksam umzusetzen und die notwendigen Garantien (Schutzmaßnahmen) in die Verarbeitung aufzunehmen. b. Personenbezogene Daten werden durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht.
Meldung von Verletzungen des Schutzes personenbezogener Daten	4. Im Fall einer Verletzung des Schutzes personenbezogener Daten (siehe Definition 7) gilt: a. Die Verantwortlichen müssen die Aufsichtsbehörde binnen höchstens 72 Stunden, nachdem ihnen die Verletzung bekannt wurde, unterrichten. b. Wenn dem Auftragsverarbeiter (8) eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich. c. Der Verantwortliche benachrichtigt die betroffene Person unverzüglich von der Verletzung (hiervon gelten einige Ausnahmen).

Kategorie	Anforderungen
Anonymisierung und Pseudonymisierung	5. Techniken zur Anonymisierung und Pseudonymisierung müssen angewendet werden: a. als Teil der Grundsätze zum „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ bei der Verarbeitung personenbezogener Daten; b. auf Daten, die zu im öffentlichen Interesse liegenden Zwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken archiviert werden.
Grenzüberschreitende Datenübertragungen und verbindliche unternehmensinterne Datenschutzvorschriften	6. Die Übertragung personenbezogener Daten unterliegt Einschränkungen: a. in Länder außerhalb des Europäischen Wirtschaftsraums (EWR), b. die nicht als „angemessen“ aufgeführt sind. Verbindliche unternehmensinterne Vorschriften (Binding Corporate Rules, BCRs) (9) und Standardvertragsklauseln (oder Modellklauseln), die von der Europäischen Kommission ausgegeben wurden, bleiben gültige Instrumente, um die Einschränkungen der EU für die Datenübertragung einzuhalten (siehe Definition 10). c. Privacy Shield (siehe Definition 11).
Zertifizierungen, Verhaltenscodexe und Siegel	7. Unternehmen können Zertifizierungsverfahren nutzen, um nachzuweisen, dass sie bestimmte Garantien bieten und entsprechende Vorschriften einhalten.

Definitionen aus der DSGVO

1. **Betroffene Person:** als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt identifiziert werden kann, insbesondere durch Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Onlinekennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.
2. **Einschränkung der Verarbeitung:** die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.
3. **Verantwortlicher:** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
4. **Aufsichtsbehörde:** eine von einem Mitgliedsstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle.
5. **Datenschutzbeauftragter:** der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.
6. **Pseudonymisierung:** die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.
7. **Verletzung des Schutzes personenbezogener Daten:** eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

8. **Auftragsverarbeiter:** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
9. **Verbindliche unternehmensinterne Datenschutzvorschriften:** Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedsstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet, und zwar im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern.

Weitere für die DSGVO relevante Definitionen

10. **Angemessene Länder:** Personenbezogene Daten können aus den 28 EU-Ländern und drei EWR-Mitgliedsländern (Norwegen, Liechtenstein und Island) in ein Drittland übertragen werden, ohne dass weitere Garantien erforderlich sind.

    Die Kommission hat bisher **Andorra, Argentinien, Kanada** (kommerzielle Unternehmen), **die Färöer-Inseln, Guernsey, Israel, die Isle of Man, Jersey, Neuseeland, die Schweiz und Uruguay** als Orte anerkannt, die angemessenen Schutz bieten (siehe http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

11. Um personenbezogene Daten von der EU in die USA zu übertragen, stehen verschiedene Hilfsmittel zur Verfügung, wie Vertragsklauseln, verbindliche unternehmensinterne Datenschutzvorschriften und der Privacy Shield. Wenn der Privacy Shield verwendet wird, müssen Unternehmen in den USA sich zuerst beim U.S. Department of Commerce (Handelsministerium der USA) für dieses Framework anmelden. Die Verpflichtungen für Unternehmen, die den Privacy Shield nutzen, finden sich in den „Privacy Principles“ (Datenschutzgrundsätzen). Das Department of Commerce ist dafür verantwortlich, den Privacy Shield zu managen und zu verwalten sowie sicherzustellen, dass Unternehmen ihre Verpflichtungen einhalten. Um die Zertifizierung zu erhalten, müssen Unternehmen über eine Datenschutzrichtlinie verfügen, die den „Privacy Principles“ entspricht. Sie müssen ihre „Selbstzertifizierung“ für den Privacy Shield jährlich erneuern. Andernfalls können sie keine personenbezogenen Daten mehr aus der EU im Rahmen des Frameworks erhalten und verwenden. Eine Liste der Unternehmen, die eine Selbstzertifizierung für den Privacy Shield durchgeführt haben, finden Sie auf der Webseite des Department of Commerce (https://www.privacyshield.gov/welcome). Auch eine Liste der Unternehmen, die nicht mehr für den Privacy Shield zertifiziert sind, steht zur Verfügung.

Abschnitt 2:

Anforderungen

Rechte betroffener Personen

Dies ist eines der wichtigsten Themen in dieser Verordnung. Die Bestimmungen wurden verschärft, und es wurden neue Rechte aufgenommen, die tiefgreifende Auswirkungen darauf haben werden, wie die IT personenbezogene Daten verarbeiten und die Kontrolle über sie ausüben muss. Es ist wichtig, zu verstehen, dass die DSGVO einen Ersatz für die **Datenschutzrichtlinie** (Richtlinie 95/46/EG) darstellt und dass ihr Ziel darin liegt, den Datenschutz für Personen in der EU zu verstärken und zu vereinheitlichen.

Während das herkömmliche Auskunftsrecht (Art. 15), Recht auf Berichtigung (Art. 16), Recht auf Löschung (Art. 17) und Widerspruchsrecht (Art. 21) im Wesentlichen unverändert bleiben, wurde ein neues Recht aufgenommen: das Recht auf Datenübertragbarkeit (Art. 20). Außerdem gibt es einige Änderungen am Recht auf Löschung: Aufgenommen wurden das Konzept des Rechts auf Vergessenwerden (Art. 17) und das Recht auf Einschränkung der Verarbeitung (Art. 18). Dies sind Grundrechte, die in der gesamten EU gelten, während mit der früheren Richtlinie jeder Mitgliedsstaat diese Rechte unterschiedlich interpretieren konnte, sodass es für die betroffenen Personen schwierig war, ihre Rechte einzufordern.

Für Unternehmen gelten mehrere Herausforderungen und einige der neuen Rechte, wie das Recht auf Datenübertragbarkeit. Dieses erlaubt es Personen, ihre personenbezogenen Daten zu ihren eigenen Zwecken zu beziehen und wiederzuverwenden, und ist möglicherweise eines der wichtigsten Rechte. Daher ist es notwendig, ein Modell einzuführen, das Unternehmen bei der Erfüllung aktueller und zukünftiger Anforderungen hilft.

Um aktuelle Anwendungen, die personenbezogene Daten umfassen, mit dieser neuen Verordnung kompatibel zu machen und zugleich die Kosten für die Veränderung vorhandener Anwendungen zu vermeiden, gibt es nur eine Möglichkeit: APIs.

Die Einführung eines API-basierten Modells für den Datenzugriff bildet die Grundlage für eine zukunftssichere Architektur, mit der das Unternehmen diese und zukünftige Verordnungen befolgen kann. Einer der Gründe hierfür ist, dass für APIs Security, Governance und Erweiterungen durch Implementierung geeigneter Softwarelösungen erreicht werden können.

Auch die Anforderung, die Einwilligung der betroffenen Person einzuholen, wurde verschärft, sodass Unternehmen ihre Beziehung mit dieser zukünftig anders handhaben müssen. Digitale Identitäten und das Management, die Governance und die Access Control für sie werden eine wichtige Rolle für alle Unternehmen spielen, die die Verordnung erfolgreich einhalten möchten.

Um die DSGVO einzuhalten, müssen Unternehmen neue Kommunikationskanäle mit betroffenen Personen einführen, um sicherzustellen, dass diesen ihre Grundrechte ordnungsgemäß zugestanden werden. Dies bedeutet, dass technische Maßnahmen angewendet werden müssen, damit Personen sicher und angemessen auf ihre Daten zugreifen können. Außerdem müssen neue Kanäle für die Datenübertragbarkeit eingerichtet werden, damit betroffene Personen vom Recht auf Datenübertragbarkeit Gebrauch machen können und veranlassen können, dass ihre Daten an den von ihnen benannten Dritten übertragen werden. Daher ist es unerlässlich, eine geeignete Security und eine robuste Access Control für diese neuen Daten-Gateways bereitzustellen.

Auch wenn dies möglicherweise ganz einfach aussieht: Personenbezogene Daten können über mehrere Dateisysteme und -server zugänglich sein. Daher muss eine ordnungsgemäße Erkennung, Analyse und Klassifizierung schon auf die IT-Infrastrukturen angewendet werden, bevor es um die Umsetzung von Datenschutzrichtlinien geht.

Rechenschaftspflicht

Technische Anforderungen sind in die gesamte Verordnung eingestreut, aber im Endeffekt geht es um die „Rechenschaftspflicht“ des Verantwortlichen oder des Auftragsverarbeiters der Daten. Mit anderen Worten: Wenn Vorfälle auftreten, was fast unvermeidlich ist, fragt die Regulierungsbehörde nach dem Beweis, dass das untersuchte Unternehmen die richtigen organisatorischen und technischen Kontrollmechanismen eingerichtet hat, um personenbezogene Daten gemäß der Verordnung zu verarbeiten. Unternehmen müssen nachweisen, dass sie die in der Verordnung geforderten IT-Kontrollmechanismen und -Maßnahmen implementiert haben, und müssen alle durchgeführten Aktionen kontinuierlich überwachen und in Berichten dokumentieren. Ob das Unternehmen dies nachweisen kann, wird einen wesentlichen Einfluss auf die Höhe einer etwaigen Geldbuße haben. Dies wird aus Artikel 83 deutlich.

In der aktuellen hybriden IT-Welt ist es nicht immer leicht zu ermitteln, welche Daten in unseren Systemen wem gehören. Dies kann eine Herausforderung für Unternehmen darstellen, die personenbezogene Daten auf dem gesamten Spektrum vorhandener Plattformen scannen und erkennen müssen. Außerdem müssen Unternehmen Lösungen implementieren, die ihnen nicht nur helfen, die Informationen zu identifizieren, sondern auch, die Kontrolle über sie zu wahren und die Nutzung dieser personenbezogenen Daten während des gesamten Lebenszyklus zu verfolgen. Wenn das Unternehmen in diesen Bereichen keine technisch ausgereiften Kontrollmechanismen implementiert hat, wird es bei Vorfällen höchstwahrscheinlich von der Regulierungsbehörde nicht gerade freundlich behandelt.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Artikel 25 Absatz 2 schreibt Folgendes vor: „Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“ Außerdem schreibt Artikel 30 die Aufzeichnung der Verarbeitungstätigkeiten vor.

Des Weiteren fordert Artikel 32 „Sicherheit der Verarbeitung“ in Punkt (b) „die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen“. Punkt (d) fordert „ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung“.

Dies ist ein sehr umfangreiches Thema, das einen ganzheitlichen Ansatz erfordert, von Softwareentwicklungsprozessen über Testing, Qualitätssicherung und Releases neuer Versionen. Für alle diese IT-Disziplinen ist eine eingebettete Schicht von Security-Kontrollmechanismen erforderlich, um sicherzustellen, dass auf Daten nur die richtigen Personen zugreifen und nur zu den spezifischen Zwecken, zu denen die Daten erfasst wurden.

Meldung von Verletzungen des Schutzes personenbezogener Daten

Vom bereits erläuterten Prinzip der Rechenschaftspflicht wird abgeleitet, dass Datenverantwortliche oder -auftragsverarbeiter verpflichtet sind, bestimmte Verletzungen des Schutzes personenbezogener Daten zu melden. Die Arten von Verletzungen, die gemeldet werden müssen, sind in Artikel 33 und 34 beschrieben.

Artikel 33 beschreibt die Verpflichtung, Datenschutzverletzungen an die zuständige Aufsichtsbehörde zu melden, und Artikel 34 die Verpflichtung zur Meldung an die betroffene Person. Beachten Sie, dass Unternehmen laut Artikel 34 Absatz 3 von der Verpflichtung zur Benachrichtigung der betroffenen Person über den Vorfall befreit sind, wenn:

- der Verantwortliche **geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat** und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung;
- der Verantwortliche durch nachfolgende Maßnahmen sichergestellt hat, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht.

Die Meldung einer Datenschutzverletzung vom Auftragsverarbeiter an einen Verantwortlichen muss unverzüglich erfolgen, und vom Verantwortlichen an die Aufsichtsbehörde binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde. Der Bericht muss Informationen dazu enthalten, wer wann welche Aktionen durchgeführt hat und welche Maßnahmen ergriffen wurden, um jegliche möglichen nachteiligen Auswirkungen abzumildern.

Anonymisierung und Pseudonymisierung

In der DSGVO werden neue Konzepte im Hinblick auf die Grundsätze eingeführt, die angewendet werden sollen, wenn personenbezogene Daten vorliegen und verarbeitet werden. Personenbezogene Daten zu schützen und der betroffenen Person die Kontrolle über sie zu ermöglichen, ist das Hauptziel der Verordnung. Daher werden einige Techniken für den Schutz personenbezogener Daten erwähnt.

In Kapitel II („Grundsätze“) sehen wir die Absicht, die Verarbeitungsverfahren für personenbezogene Daten zu stärken („Datenminimierung“) und dafür zu sorgen, dass diese Daten nicht länger als notwendig in einer Form gespeichert werden, die die Identifizierung der betroffenen Person ermöglicht. Außerdem müssen die personenbezogenen Daten in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Grenzüberschreitende Datenübertragungen und verbindliche unternehmensinterne Datenschutzvorschriften

Wie in der früheren Richtlinie werden in Artikel 45 der Verordnung Einschränkungen für internationale Übertragungen personenbezogener Daten an „nicht angemessene“ Länder außerhalb der EU aufgestellt. In Artikel 46 Absatz 2, sind die geeigneten Garantien beschrieben, die vorhanden sein müssen, damit Datenübertragungen ohne eine besondere Genehmigung einer Aufsichtsbehörde durchgeführt werden können.

Verbindliche unternehmensinterne Vorschriften (Art. 47) und Standardvertragsklauseln (oder Modellklauseln), die von der Europäischen Kommission ausgegeben wurden, bleiben gültige Instrumente, um die Einschränkungen der EU für die Datenübertragung einzuhalten. Die Verwendung dieser Übertragungsmechanismen für gruppeninterne Zwecke sollte leichter werden, da bestimmte vorhandene Genehmigungsanforderungen aufgehoben wurden. Zu Auswirkungen auf den US Privacy Shield siehe Definitionen 10 und 11.

Die Kontrolle darüber zu haben, wer Zugriff auf Daten erhält, ist eine grundlegende Voraussetzung für die Erfüllung dieser Anforderung. Unternehmen müssen regelmäßige Zugriffszertifizierungskampagnen durchführen, um sich zu vergewissern, dass die Zugriffsrechte für ihre Anwender jederzeit richtig sind. Der benannte Datenschutzbeauftragte (Data Protection Officer, DPO) benötigt fortschrittliche Reporting-Funktionen für unterschiedliche Bereiche der IT-Security, um die Einhaltung von Vorschriften sicherzustellen.

Außerdem sind Funktionen erforderlich, mit denen das Versenden von Dokumenten, die personenbezogene Daten enthalten, an Empfänger außerhalb des Unternehmens eingeschränkt wird. So kann sichergestellt werden, dass niemand versehentlich Dateien, die als DSGVO-relevant gekennzeichnet sind, an unbefugte Dritte sendet.

Zertifizierungen, Verhaltenscodexe und Siegel

Unternehmen können Zertifizierungsverfahren nutzen, um nachzuweisen, dass sie bestimmte Garantien bieten. Artikel 42 enthält eine entsprechende Handlungsaufforderung an die Mitgliedsstaaten, Aufsichtsbehörden und sonstigen EU-Institutionen: Gefordert wird die Einführung von datenschutzspezifischen Zertifizierungsverfahren sowie von Datenschutzsiegeln und -prüfzeichen, mit denen die Einhaltung der Verordnung nachgewiesen wird. Außerdem erwähnt Artikel 42 auch ein zukünftiges Framework für eine gemeinsame Zertifizierung, das „Europäische Datenschutzsiegel“, mit dem ein EU-weiter gemeinsamer Zertifizierungsstandard sichergestellt werden soll, um die Konsistenz und die Transparenz für die Bürger zu erhöhen.

Abschnitt 3:

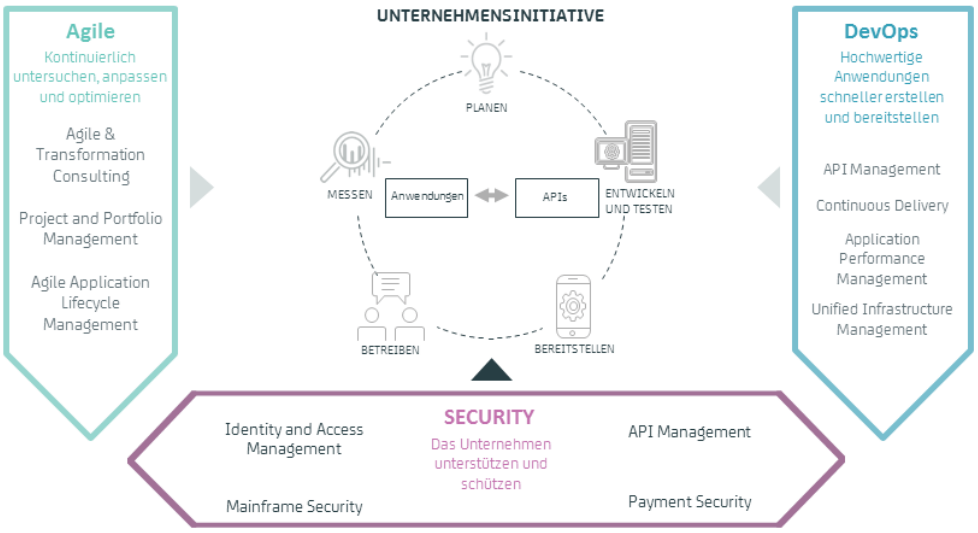
CA Technologies unterstützt Sie

Um die Verordnung einzuhalten, benötigen Sie eine sorgfältige Herangehensweise sowie Unterstützung durch Ihre Rechts- und IT-Abteilung, in einigen Fällen auch durch Beratungsfirmen. Nur so können Sie detaillierte Bewertungen und Überprüfungen im Hinblick auf die Verordnung durchführen und Ihre organisatorischen Prozesse überarbeiten. Als innovatives Softwareunternehmen und Vordenker der Application Economy führt CA Technologies Unternehmen durch den Prozess der digitalen Transformation und kann ein breites Spektrum an Softwarelösungen bereitstellen, um sie auf ihrem Weg zur Compliance zu unterstützen.

CA Technologies bietet die Technologien, die Unternehmen brauchen, um DSGVO-Compliance zu erreichen und um die vorgeschriebenen Kontrollmechanismen bereitzustellen, die dem Grundgedanken „Sicherheit durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“ der Verordnung entsprechen.

Was CA Technologies von Anbietern spezifischer Einzellösungen unterscheidet, ist, dass unsere Produktlösungen fast jeden Aspekt des Datenlebenszyklus im Unternehmen einbeziehen. Unternehmen können Lösungen von CA Technologies kombinieren, die den Datenzugriff schützen, den Anwenderzugriff managen und steuern sowie unbefugte Zugriffe auf personenbezogene Daten durch Externe und Interne verhindern. So können sie sicherstellen, dass sie die neue Verordnung einhalten, indem sie die Rechte der betroffenen Personen an ihren Daten schützen. CA Technologies bietet die Tools und das notwendige Expertenwissen, um Unternehmen durch den gesamten Prozess zu führen.

CA Technologies bietet eine umfassende, sichere DevOps-Strategie. Sie beschleunigt nicht nur die Entwicklung und Bereitstellung von Anwendungen, sondern sorgt auch für die Sicherheit der Anwendungen und des gesamten Lebenszyklus der Softwarebereitstellung. Zu unseren umfassenden Security-Lösungen gehören das API Management, die Mainframe Security und mehrere Komponenten unserer umfangreichen IAM-Security-Suite. Weitere Informationen zu unseren IAM-Security-Lösungen finden Sie unter ca.com/iam.



CA Technologies für die Klassifizierung und Ortung von Daten

Auch wenn im Unternehmen die Ansicht besteht, dass bekannt ist, wo personenbezogene Daten gespeichert sind, und dass sie unter Kontrolle sind, ist die Realität eine andere: Personenbezogene Daten sind im gesamten Unternehmen verteilt und werden an vielen Orten genutzt und transformiert, wobei verschiedene Personen auf unterschiedliche Weisen auf sie zugreifen. Daher reichen anwendungsbasierte Kontrollmechanismen nicht aus, um die Verordnung einzuhalten.

Außerdem lag der Schwerpunkt der früheren Richtlinie eher auf dem Schutz der Dateien mit den personenbezogenen Daten und auf der Speicherung der Informationen, während die neue Verordnung auf die Verarbeitung der Daten abzielt. Dies ist das Ergebnis des neuen digitalen Zeitalters, in dem Daten sehr schnell transformiert, hinzugefügt, erweitert und verarbeitet werden. Mit modernen Big-Data-Analysen können scheinbar voneinander unabhängige Daten zu personenbezogenen Daten kombiniert werden, die der Verordnung unterliegen.

Deshalb ist es äußerst wichtig, eine mehrschichtige Verteidigung einzuführen, um personenbezogene Daten zu schützen und die Kontrolle über sie zu wahren.

Beginnen wir mit der Identifizierung und Klassifizierung der Daten sowie der Ermittlung der Speicherorte personenbezogener Daten in unserer Infrastruktur. Wenn sich personenbezogene Daten außerhalb der dafür vorgesehenen Kanäle und Abläufe befinden, muss dies bekannt sein, und die entsprechenden Risiken müssen eingeschätzt werden.

Zu wissen, wo sich personenbezogene Daten befinden und wer im Unternehmen auf sie zugreifen kann, ist einer der Grundgedanken der DSGVO.

CA Data Content Discovery

In der Application Economy ist der Mainframe zunehmend mit dem Rest des Rechenzentrums vernetzt, ist auch für gelegentliche Anwender eher verfügbar und unterliegt der Datenschutzverordnung. Daten werden aus der Produktion kopiert, um sie in der Entwicklung oder im Testing zu nutzen, und werden dann einfach zurückgelassen; andere sind verwaist, weil die Verantwortlichen das Unternehmen verlassen haben. Außerdem können Anwender über UNIX® System Services unstrukturierte Daten einbringen. Dies hat möglicherweise dazu geführt, dass umfangreiche Daten auf dem Mainframe verborgen sind, die Vorschriften unterliegen oder vertraulich sind. Wenn das Unternehmen die Kontrolle über diese Daten verliert, können finanzielle Schäden und Rufschädigungen die Folge sein.

Auch heute befinden sich über 70 % der unternehmenskritischen Daten auf dem Mainframe. Wenn Sie beispielsweise heute Ihre EC-Karte verwendet, einen Flug gebucht oder telefoniert haben, haben Sie wahrscheinlich mit einem Mainframe zu tun gehabt. Die Application Economy hat jedoch neue Risiken für den Mainframe mit sich gebracht: Er wird bei fast allen Anwendungen einbezogen, und Datenschutzverletzungen sind häufig in den Nachrichten. Es wäre für das Unternehmen verheerend, wenn der Mainframe und die darauf befindlichen Vorschriften unterliegenden oder vertraulichen Daten kompromittiert würden.

In der aktuellen hybriden IT-Welt ist es nicht immer leicht zu ermitteln, welche Daten in unseren Systemen zu der Gruppe gehören, auf die sich die Verordnung bezieht. Um dies ordnungsgemäß und systematisch herauszufinden, findet, klassifiziert und schützt **CA Data Content Discovery** vertrauliche Mainframe-Daten, um das gesamte Spektrum vorhandener Plattformen abzudecken. Die Lösung umfasst vordefinierte Richtlinien für personenbezogene Daten. Diese helfen nicht nur, die Informationen zu identifizieren, sondern auch, ihre Nutzung durch die Anwender zu steuern und zu verfolgen, wie in mehreren Artikeln vorgeschrieben. Der Scanvorgang erfolgt zu 100 % auf der Mainframe-Plattform. Ihre Daten werden also zur Analyse nicht an einen anderen Speicherort dupliziert. So können Unternehmen Daten schnell identifizieren und schützen, damit sie nicht kompromittiert werden können.

CA Identity Suite

Artikel 25 Absatz 2 schreibt Folgendes vor: „Der Verantwortliche trifft geeignete technische und organisatorische Maßnahmen, die sicherstellen, dass durch Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.“ Außerdem schreibt Artikel 30 die Aufzeichnung der Verarbeitungstätigkeiten vor. Dies bedeutet, dass Sie eine Lösung implementieren müssen, die den geeigneten Zugriff von Mitarbeitern auf personenbezogene Daten verwaltet und steuert, damit die Daten nicht unnötig offengelegt werden.

Mit **CA Identity Suite** können Sie den Anwenderzugriff auf Unternehmensanwendungen und auf die zugrunde liegenden Daten verwalten und steuern. Die Lösung unterstützt die vollständige Erfüllung dieser Anforderung. Sie stellt Berichte dazu bereit, wer auf was zugreifen kann. Außerdem kann sie Zugriffszertifizierungskampagnen durchführen und verwalten, damit das Unternehmen die Verordnung dauerhaft einhalten kann.

Eine gängige Methode für die Einhaltung von Vorschriften ist eine regelmäßige Überprüfung, ob die Anwender über angemessenen Zugriff auf Unternehmensressourcen verfügen. Während der Zugriffszertifizierung müssen Manager Listen der Berechtigungen der ihnen direkt unterstellten Mitarbeiter prüfen und die Notwendigkeit einer Zugriffsberechtigung bestätigen oder ablehnen.

CA Identity Suite gestaltet diesen Prozess einfach und intuitiv und erhöht so die Zufriedenheit und Produktivität der Anwender. Die Anpassung eines Zertifizierungsprozesses an den spezifischen Bedarf eines Unternehmens ist für die effektive Überprüfung des Zugriffs und die Motivation zur Teilnahme an dem Prozess entscheidend. CA Identity Suite kann eine Überprüfung aus unterschiedlichen Perspektiven anfordern, beispielsweise von Anwendermanagern, Ressourcenverantwortlichen oder Rollenentwicklern. Zertifizierungsprozesse, die auch als Kampagnen bezeichnet werden, können mit unterschiedlichen

Zeitplänen, Workflows und genehmigenden Personen für jede dieser Perspektiven durchgeführt werden. Zudem können mehrere Kampagnen gleichzeitig ausgeführt werden. Jede zielt auf Teile des Unternehmens (z. B. Anwender in einem bestimmten Geschäftsbereich) oder die Hervorhebung unterschiedlicher Zugriffsarten (z. B. verdächtige Zuweisungen oder außerhalb des Rollenmodells zugeteilter Zugriff) ab. CA Identity Suite umfasst zuverlässige Verwaltungskontrollen und -workflows, um den Kampagnenfortschritt entsprechend den Anforderungen sicherzustellen. Dazu gehören E-Mail-Benachrichtigungen, Erinnerungen und Eskalationsprozesse zum Anfordern der Genehmigung von höherrangigen Managern. Wenn Abweichungen festgestellt werden und Änderungen an den Zugriffsrechten erforderlich sind, können zudem Fehlerbehebungsprozesse ausgelöst werden, indem Fehlerbehebungstickets den richtigen Besitzern zugewiesen werden oder über eine Integration in CA Identity Manager.

Laut dieser Verordnung gibt es einen wichtigen Teilnehmer, den Datenschutzbeauftragten (DPO), der von Unternehmen eingesetzt werden muss. Für den Inhaber dieser Rolle sind technologische Lösungen unerlässlich, die alle Security-Kontrollmechanismen aufrechterhalten und nachweisen, mit denen das Unternehmen personenbezogene Daten schützt. Mithilfe der Reporting-Funktionen der Lösungen von CA Technologies kann der DPO nachweisen, wie das Unternehmen die Verordnung einhält. Dies ist relevant für die Durchführung von Datenschutz-Folgenabschätzungen, wie in Art. 35 beschrieben.

CA Identity Suite umfasst außerdem eingebettete Identitätsprozessanalysen. Diese liefern detaillierte und leicht verarbeitbare Informationen, die den Funktionsablauf wichtiger Identitätsprozesse (etwa Onboarding von Anwendern) hervorheben. Diese Analysen helfen bei der Erkennung und Beseitigung von Engpässen, sodass eingegangene Service Level Agreements erfüllt werden können. CA Identity Governance umfasst einen umfangreichen Satz sofort einsetzbarer Berichte und Dashboards und unterstützt Ad-hoc-Anfragen für gerichtliche Anforderungen. Die Berichte bieten geschäftliche und technische Informationen unterschiedlicher Detailgrade, um den Bedarf unterschiedlicher Anwendertypen abzudecken. Dazu gehören beispielsweise gesonderte Berichte für Geschäftsbereichsleiter, Rollenentwickler, Compliance-Beauftragte, Auditoren und IT-Mitarbeiter.

CA Test Data Management

Die Verordnung wird weitreichende Auswirkungen darauf haben, was für Arten von Daten in Umgebungen außerhalb der Produktion verwendet werden können. Unternehmen müssen genau ermitteln, über was für Daten sie verfügen und wer diese verwendet, und sie müssen in der Lage sein, diese Verwendung auf Aufgaben zu beschränken, in die die betroffenen Personen eingewilligt haben. Eine Möglichkeit, personenbezogene Daten nicht in Testumgebungen offenzulegen, besteht darin, sie dort gar nicht erst bereitzustellen, nicht einmal in maskierter Form. Die Erzeugung synthetischer Daten ist eine Technik, mit der Unternehmen möglicherweise zu vollständig virtualisierten Testumgebungen übergehen können.

Beim Testing und bei der Entwicklung von Software ist es möglich, dass Daten in Test- und Entwicklungsumgebungen sowie in komplexe Umgebungen verteilt werden. Tester kopieren Daten möglicherweise zu einem bestimmten Zweck in ihre Umgebung, aber das Unternehmen muss wissen, wie lange die Daten dort verwendet werden und dass sie mit Einwilligung und zu einem legitimen Zweck verwendet werden. Eine Erstellung von Datenprofilen mit **CA Test Data Manager** kann zu diesem wichtigen Aspekt der Einhaltung von Vorschriften beitragen. Mit ihr wird unternehmensweit genau identifiziert, wo vertrauliche Daten gespeichert sind. Außerdem werden statistische Analysen verwendet, um personenbezogene Daten zu finden, die in mehreren Dateiformaten und Anwendungen gespeichert sind. CA Test Data Manager verwendet eine dreidimensionale Ansicht, um Daten genau darzustellen, und identifiziert vertrauliche Informationen, die in zugehörigen Systemen, Komponenten oder Daten widergespiegelt sind. Mit firmenspezifischen, mathematisch fundierten Filtern können Daten auf differenziertem Level gefiltert werden, um jede Instanz der Informationen zu einer Person zu identifizieren. Zu diesen Daten können Kreditkartennummern, E-Mail-Adressen, Postadressen und Ähnliches gehören. Damit können Unternehmen das Recht auf Datenübertragbarkeit erfüllen. Die Datenerkennung von CA Test Data Manager ist vollständig prüffähig, sodass Unternehmen nachweisen können, dass sie Kontrollmechanismen im Interesse der Compliance anwenden.

CA API Management

Um aktuelle Anwendungen, die personenbezogene Daten umfassen, mit dieser neuen Verordnung kompatibel zu machen und zugleich die Kosten für die Veränderung vorhandener Anwendungen zu vermeiden, gibt es nur eine Möglichkeit: APIs.

Mit der **CA API Management** Suite können Unternehmen die Herausforderungen der Freigabe von Informationen in der Application Economy mühelos meistern. Die Lösung kombiniert fortschrittliche Funktionen für die Back-End-Integration, die mobile Optimierung, die Cloud-Orchestrierung und das Entwicklermanagement. Sie ist einmalig in ihrer Fähigkeit, die gesamte Bandbreite dieser Anforderungen an das API Management eines Unternehmens zu bewältigen. Mithilfe von CA API Management können Unternehmen die Einhaltung der Verordnung nachweisen, ohne aktuelle Anwendungen austauschen zu müssen. Außerdem können mit **CA Live API Creator** neue APIs erstellt werden, die die geeigneten Kontrollmechanismen umfassen und die benötigten Informationen für Dritte offenlegen.

Beispielsweise können wir es mit CA API Management-Lösungen vermeiden, Anwendungen zu verändern und damit Risiken und Kosten einzugehen. Außerdem können wir Verhaltensweisen mit einer Lösung unter Kontrolle halten, die auf Regeln und Richtlinien basiert. So kann das Unternehmen Regeln für die Einholung der Einwilligung aufnehmen, Anwender über die Vorgaben in Artikel 15 und 20 informieren und über das **CA API Developer Portal** dokumentieren, wie auf die Daten zugegriffen werden darf. Die Access Controls für die Security werden von **CA API Gateway** bereitgestellt.

Um die Vorteile dieses Ansatzes zu verstehen, können Sie die Kosten berechnen, die für die Veränderung aller Anwendungen entstehen würden, mit denen Sie zurzeit personenbezogene Daten im Unternehmen verwalten. Diese können Sie mit den Kosten für eine einzelne, standardisierte Schnittstelle vergleichen, die auch zur Einhaltung anderer Vorschriften Ihrer Branche verwendet werden kann.

CA Privileged Access Manager

Der Missbrauch privilegierter Anwenderaccounts ist oft ein entscheidender Faktor bei Datenschutzverletzungen, sei es, weil sie böswillig ausgeforscht oder durch einen legitimen Anwender unangemessen verwendet werden. Ihre Umgebung wird immer komplexer, und damit wächst auch die Herausforderung der Verteidigung gegen immer ausgeklügeltere – und schädlichere – Angriffe. Das Privileged Access Management von CA Technologies bietet eine umfassende Lösung. Diese umfasst netzwerk- und hostbasierte Kontrollmechanismen für das Unternehmen und für die hybride Cloud.

Unternehmen können in die Versuchung geraten, anzunehmen, dass der Schutz des Datenzugriffs über anwendungsbasierte Access Controls ausreicht. In Wirklichkeit werden die meisten Datenschutzverletzungen erreicht, indem Accounts privilegierter Anwender ausgenutzt werden. Damit werden gültige Access Controls umgangen und sind somit nutzlos. Deshalb müssen Unternehmen Security-Kontrollmechanismen implementieren, mit denen sie privilegierte Zugriffe verwalten und steuern.

CA Privileged Access Manager (CA PAM) ist eine einfach bereitstellbare, bewährte Lösung für das Privileged Access Management in physischen und virtuellen Umgebungen sowie Cloud-Umgebungen. CA Privileged Access Manager ist als gehärtete Hardware-Appliance für die Rack-Montage, als virtuelle Appliance im Open Virtualization Format (OVF) oder als Amazon Machine Instance (AMI) verfügbar. Mit dieser Lösung erreichen Sie eine Erweiterung der Security durch vertrauliche administrative Anmeldeinformationen (wie etwa Root- und Administratorpasswörter), die Steuerung von Zugriffen privilegierter Anwender, eine proaktive Erzwingung von Richtlinien sowie die Überwachung und Protokollierung der Aktivitäten privilegierter Anwender in sämtlichen IT-Ressourcen.

Eine Komponente von CA PAM, **CA Privileged Access Manager Server Control**, bietet umfassenden Schutz für Ihre unternehmenskritischen Server mit leistungsstarken, spezifischen Kontrollmechanismen für Zugriffe auf Betriebssystemebene und Aktionen privilegierter Anwender. Mit der Möglichkeit, Access Controls für mächtige native Superuser-Accounts zu erzwingen – wie „root“ unter UNIX und Linux® und „Administrator“ unter Microsoft® Windows® – steuert, überwacht und prüft diese hostbasierte Lösung auf Systemebene die Aktivitäten privilegierter Anwender. So erhöht sie die Security und vereinfacht Audits und die Einhaltung von Vorschriften.

Durch die Kombination von CA Privileged Access Manager Server Control für die Serverhärtung mit CA Privileged Access Management wird die vollständigste Lösung für das Management privilegierter Anwender und Zugriffe für Ihr Unternehmen bereitgestellt.

CA Single Sign-On

Die Interaktion zwischen Unternehmen und ihren Kunden hat sich aufgrund der Application Economy sehr verändert. Anwender verlangen jederzeit und von überall Zugriff auf Onlineservices und erwarten eine nahtlose und konsistente User Experience über mehrere Geräte und Zugriffs-Channels. Im Hinblick auf die DSGVO müssen Unternehmen ein Gleichgewicht zwischen dem einfachen Zugriff und dem Schutz der Daten, auf die zugegriffen wird, erreichen. Wie können Sie sicherstellen, dass nur die richtigen Personen auf vertrauliche Inhalte zugreifen, und nur, sofern es juristisch zulässig ist? Beispielsweise haben EU-Bürger das Recht, ihre persönlichen Daten zu sehen. Wie können sie jedoch auf ihre Daten zugreifen und sie ansehen, wenn sie sich von einem Land außerhalb der USA anmelden? Was ist mit Mitarbeitern des Unternehmens? Möglicherweise können sie auf diese Daten zugreifen, wenn sie sich von den USA aus anmelden, nicht jedoch bei Anmeldung aus einem anderen Land.

Mit **CA Single Sign-On** können Sie diese Herausforderungen bewältigen. Mitarbeiter, Kunden, Partner und Zulieferer erhalten ein sicheres Single Sign-On für Onlineanwendungen, ganz gleich, wo diese bereitgestellt sind, über was für ein Gerät auf sie zugegriffen wird oder wie sich der Anwender für die Website authentifiziert: direkt, über Social Media oder über eine Federation von einer Partnerwebsite. Außerdem erhöht die Lösung die Security durch die Bereitstellung einer gemeinsamen Richtlinienebene, die das Risiko von Lücken beim Zugriff minimiert.

Die DSGVO schreibt vor, dass Unternehmen Anwendern Zugriff erteilen, aber die Anzahl der Personen begrenzen müssen, die auf diese personenbezogenen Daten zugreifen können. Eine umfassende Access-Management-Lösung wie CA Single Sign-On kann die passenden Web Access Controls für beide Arten von Anwendern zentral bereitstellen. Diese Security aus den Anwendungen auszulagern, unterstützt das Security-by-Design-Konzept in DevSecOps.

CA Directory

Die DSGVO stellt eine wesentlich veränderte Neufassung vorhandener Datenschutzgesetze dar. Zwar befindet sich der Großteil dieser Daten auf Mainframes in großen Unternehmen; ein wesentlicher Teil dieser Daten befindet sich jedoch auch in Verzeichnissen. Unternehmen werden zunehmend abhängig von ihren Online- und Mobilanwendungen, über die sie ihren Anwendern wichtige Services bereitstellen. Sie stehen vor Herausforderungen hinsichtlich der Performance und der Verfügbarkeit, weil bei der zugrunde liegenden Verzeichnisinfrastruktur Probleme wie die folgenden auftreten:

- **Explosives Wachstum:** Die explosionsartige Zunahme an Anwenderidentitäten und Geräten sowie die Notwendigkeit, die für eine überlegene User Experience notwendige Reaktionsfähigkeit aufrechtzuerhalten, stellen für viele Legacy Repositories Herausforderungen dar.
- **Identitätssilos:** Im Laufe der Zeit wurden von unterschiedlichen Unternehmensbereichen mehrere Verzeichnisse bereitgestellt. Diese verursachen jetzt Herausforderungen wie z. B. eine schlechte User Experience, Security-Risiken und erhöhte Betriebskosten.
- **Neue Anforderungen:** Sicherheitsanforderungen ändern sich von der einfachen Anwenderauthentifizierung hin zur Nachverfolgung detaillierter Anmeldedaten und personalisierter Informationen in Verbindung mit dynamischen Geschäftstätigkeiten.

Daher bemühen sich viele Kunden, ihre Identity-and-Access Management-Infrastruktur zu verstärken, indem sie zu einem Verzeichnisservice der nächsten Generation migrieren, der eine bessere Performance zu geringeren Gesamtbetriebskosten bietet. Auch die DSGVO beeinflusst jedoch ihre Evaluierungskriterien auf interessante Weise. Ihr Verzeichnisservice der nächsten Generation sollte die Möglichkeit bieten, den Verzeichnisbaum auf mehrere Server aufzuteilen, sodass das Unternehmen weiß, wo personenbezogene Daten physisch gespeichert sind. Außerdem sollte er es Ihnen ermöglichen, selektiv zu bestimmen, welche Daten auf unterschiedliche Knoten repliziert werden, damit Sie verhindern können, dass Daten eine bestimmte Region verlassen.

CA Cleanup

CA Cleanup erkennt anhand eines angegebenen Zeitschwellenwerts ungenutzte Konten und erzeugt Befehle zum Entfernen von ungenutzten Anwender-IDs, Rechten, Berechtigungen sowie Profil- und Gruppenverbindungen, die ein Anwender besitzt, aber nicht nutzt. Mit der Lösung können Sie die Anhäufung veralteter und überflüssiger Zugriffsrechte effektiv beseitigen, die sich sonst im Laufe der Zeit in einer Sicherheitsdatei ansammeln – eine wesentliche Anforderung für die Einhaltung vieler Vorschriften. CA Cleanup kann innerhalb eines Tages vollständig bereitgestellt werden und ermöglicht Folgendes:

- Identifizieren und Entfernen einzelner Anwender, Rechte und Zugriffsgruppen, die nicht mehr verwendet werden
- Identifizieren von Rechten (wie Berechtigungen und Regeln), die tatsächlich verwendet werden, und Erstellung von Befehlen, um die nicht verwendeten zu entfernen; dies schließt auch vom Anwender definierte Ressourcen ein
- Identifizieren von Anwender-IDs, die wirklich verwendet werden, und Erstellen von Löschbefehlen für die nicht entfernen; dies basiert auf der tatsächlichen Security-Nutzung, nicht auf berichteten Zeitpunkten der „letzten Verwendung“, die häufig unzuverlässig sind
- Erstellen von Berichten, in denen genutzte und ungenutzte Rechte aufgeführt sind
- Erzeugen von Befehlen zur Durchführung oder Wiederherstellung einer Security-Bereinigung

Wenn Sie CA Cleanup mit CA ACF2™ verwenden, können Sie zwischen aktiven und inaktiven Anwenderkennungen, Regelgruppen und Regeln unterscheiden. Dazu werden unter anderem vom Anwender definierte Ressourcenklassen und im ACF2 die NEXTKEY-Regeln für Quellen und Ziele verwendet. Wenn Sie CA Cleanup mit CA Top Secret® verwenden, können Sie zwischen aktiven und inaktiven ACIDS, Berechtigungen und Profilverbindungen unterscheiden. Hierzu gehören vom Anwender definierte Ressourcen und der *ALL*-Datensatz. Wenn Sie CA Cleanup mit IBM® RACF® verwenden, können Sie zwischen aktiven und inaktiven Anwender-IDs, Profilen, Berechtigungen, Gruppenverbindungen und Ressourcengruppen von IBM RACF unterscheiden. Die Nutzung von Berechtigungen wird bis zu jedem einzelnen Eintrag der Zugriffsliste verfolgt, ganz gleich, ob diskret, generisch oder bedingt.

CA Compliance Event Manager

CA Compliance Event Manager bietet ein proaktives Security Monitoring und hilft Ihnen, die Kosten, die Komplexität und den Aufwand für das Monitoring und Reporting zur Mainframe Security und Compliance zu reduzieren. CA Compliance Event Manager umfasst mehrere Komponenten, die konzipiert sind, um Informationen zu externen Security-Manager-Ereignissen zu verarbeiten und Systeme nahtlos auf Veränderungen an wichtigen Informationen zu überwachen. Die Lösung bietet Warnungen, Untersuchungen und Schutz für erfolgsentscheidende Mainframe-Daten. Wichtige Stakeholder erhalten Echtzeitbenachrichtigungen zu potenziellen Security-Verstößen.

Für die Einhaltung der DSGVO ist es sehr wichtig, wie Daten zukünftig erfasst werden. Ein wesentlicher Schwerpunkt liegt jedoch auch auf den Daten, die Unternehmen bereits besitzen. Da sich auf vielen Mainframes Generationen alte Daten befinden, ist ein manuelles Daten-Audit völlig unrealistisch. Hierbei hilft CA Compliance Event Manager. Diese Lösung bietet drei wichtige Funktionen:

- **Warnen:** Die Lösung überwacht gesamte Systeme von Security-Unterlagen, Security-Konfigurationspunkten, Systemdatengruppen und Konfigurationselementen für IBM z/OS® in Echtzeit mit sofortigen Benachrichtigungen über relevante Verstöße, Zugriffe und Veränderungen auf kritischen Security-Systemen und Ressourcen. So erhalten Stakeholder sofortige, kritische Einblicke in das Potenzial und die Größenordnung der Datenoffenlegung auf dem Mainframe, um proaktiv negative Security-Ereignisse zu verhindern.
- **Untersuchen:** Wenn Bedrohungen durch offengelegte Daten erkannt wurden, erzeugt CA Compliance Event Manager erweiterte Audit- und Compliance-Informationen, die in standardmäßigen Security-Berichten nicht zur Verfügung stehen. Die Lösung bietet eine ausgefeilte Datenerfassung, ein umfassendes Auditing und Unterstützung für Data Warehouses. Sie ermöglicht es Anwendern, alle Security-Ereignisse von der Aufzeichnung wiederzugeben, forensische Analysen anhand der aufgezeichneten Security-Rohdaten durchzuführen sowie Protokolldaten zu durchsuchen, zu filtern und zu analysieren, wobei Magnetbänder automatisch herausgesucht werden. All dies bietet tiefere Einblicke in Security- und Compliance-Probleme und einen besseren Schutz vor Risiken.
- **Schützen:** Indem Sie Echtzeit-Benachrichtigungen erhalten und die Datenoffenlegungen untersuchen können, um eine schnelle Problemtriage durchzuführen, erhalten Sie mehr Kontrolle über Ihre Mainframe-Daten. Sie sind besser in der Lage, herauszufinden, wer auf Daten zugreifen kann, die der DSGVO unterliegen – von Mitarbeitern über Kunden bis hin zu Unternehmenspartnern, und zwar ehemaligen und aktuellen. So können Sie sicherstellen, dass geeignete Berechtigungen angewendet werden.

Abschnitt 4:

Fazit

Die Einhaltung der DSGVO kann durch ein Zusammenwirken von Personen, Prozessen und Technologien erreicht werden. In diesem Dokument wurden Lösungen beschrieben, die Unternehmen den Weg mit der DSGVO erleichtern können. Sie können diesen Schutz jedoch sogar noch erweitern und die Security-Kontrollmechanismen noch verstärken, indem Sie eine strenge und risikobezogene Authentifizierung oder eine Workload-Automatisierung verwenden. So können Sie die DSGVO und ähnliche Auflagen erfüllen. In Vorschriften werden meist die zu erfüllenden Mindeststandards festgelegt. In der Application Economy müssen offene Unternehmen jedoch sicherstellen, dass sie angemessene Sorgfalt walten lassen und eines der wichtigsten und empfindlichsten Assets schützen: die privaten Daten von Kunden.

Es ist wichtig, die DSGVO nicht isoliert zu betrachten, sondern im Kontext vieler anderer Gesetze und Vorschriften – einschließlich branchenspezifischer – für den Schutz von Daten in der Application Economy. Strenge Kontrollmechanismen für die Security und den Schutz von Daten sowie für Datennutzung und -zugriff sind für Unternehmen unerlässlich, um derartige Gesetze und Vorschriften einzuhalten, unabhängig von der Branche.

Sehen Sie sich die folgenden Ressourcen an, um mehr über Lösungen von CA Technologies und die DSGVO zu erfahren:

- eBook: „Einhalten der EU-Datenschutz-Grundverordnung: Die Auswirkungen auf das Test Data Management“
- White Paper: „EU-Datenschutz-Grundverordnung (DSGVO): Sind Sie dafür bereit?“

Kontaktieren Sie CA Technologies unter ca.com/de.

CA Technologies (NASDAQ: CA) entwickelt Software, die Unternehmen bei der Umstellung auf die Application Economy unterstützt. Software steht in allen Branchen und in allen Unternehmen im Mittelpunkt. Von der Planung über die Entwicklung bis hin zu Management und Security arbeitet CA Technologies weltweit mit Unternehmen zusammen, um die Art, wie wir leben, Transaktionen durchführen und kommunizieren, neu zu gestalten – ob mobil, in der privaten oder öffentlichen Cloud oder in verteilten Systemen oder Mainframe-Umgebungen.
Weitere Informationen finden Sie unter ca.com/de.

CS200-255926_0217