Informatica™

Datenschutz – Privacy by Design

Ein agiler Ansatz zur Reduzierung des Datenschutzrisikos und Erhöhung des Vertrauens von Kunden

Einleitung

Die neue Datenlandschaft: Mehr, schneller, weiter

Der explosionsartige Datenanstieg ist ein zweischneidiges Schwert. Einerseits ermöglicht er es innovativen Unternehmen, wichtige Wettbewerbsvorteile zu nutzen und neue Produkte und Services zu entwickeln.

Doch andererseits führt er dazu, dass Unternehmen mehr sensible Daten haben als je zuvor. Und Schutz und Data Governance dieser Daten sind schwieriger denn je.

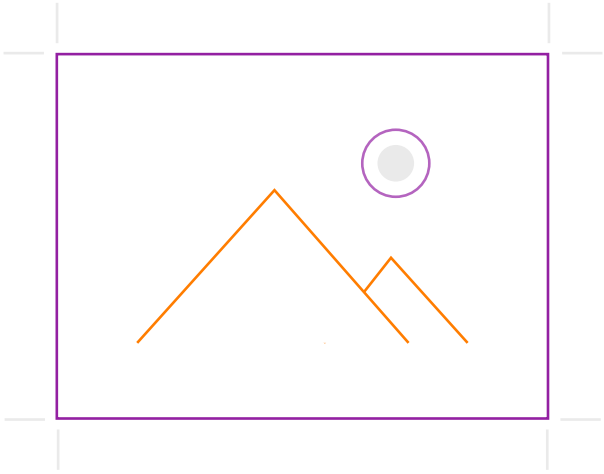
Dabei bereitet nicht nur das bloße Datenvolumen Probleme. Auch die Geschwindigkeit, in der Daten innerhalb und außerhalb von Unternehmen bewegt werden, steigt an. Zudem entwickeln sich auch die Daten selbst weiter. Zweck, Qualität und Standort von Datenbeständen können sich über Nacht ändern.

Kontinuierliche Änderungen, steigende Geschwindigkeit und wachsendes Volumen führen zu enorm hohen Risiken:

- Zusätzlich zu traditionell strukturierten Daten in Transaktionsanwendungen und relationalen Datenbanken gelangen auch IoT- und Social-Media-Daten in Ihre Data Lakes.
- Da Daten für Analytics, Prozessverbesserungen und Machine Learning genutzt werden sollen, steigt das Risiko, dass Daten unbeabsichtigt auf eine Art und Weise verwendet, kopiert und kombiniert werden, die gegen Consent Management und Vorschriften verstößt.
- Der verantwortungsbewusste Umgang mit Daten beeinflusst die Entscheidungen Ihrer Kunden darüber, mit welchen Unternehmen sie Geschäfte tätigen.
- Cyber-Angriffe werden immer gefährlicher und innerhalb und außerhalb Ihrer Unternehmensumgebung kommt es immer schneller zu immer mehr schädlichen Aktivitäten.
- Die Anzahl an Datenschutzvorschriften steigt weltweit an, genauso wie Bußgelder für Non-Compliance.

Traditionelle Sicherheits- und Schutzmodelle werden diesen Herausforderungen einfach nicht mehr gerecht. Früher handelte es sich hierbei um Zeitpunktaktivitäten, die jetzt in einen kontinuierlichen Prozess umgewandelt werden müssen, um sich ändernden Prioritäten und neuen Bedrohungen gerecht zu werden.

Daher ist ein neuer Ansatz erforderlich.



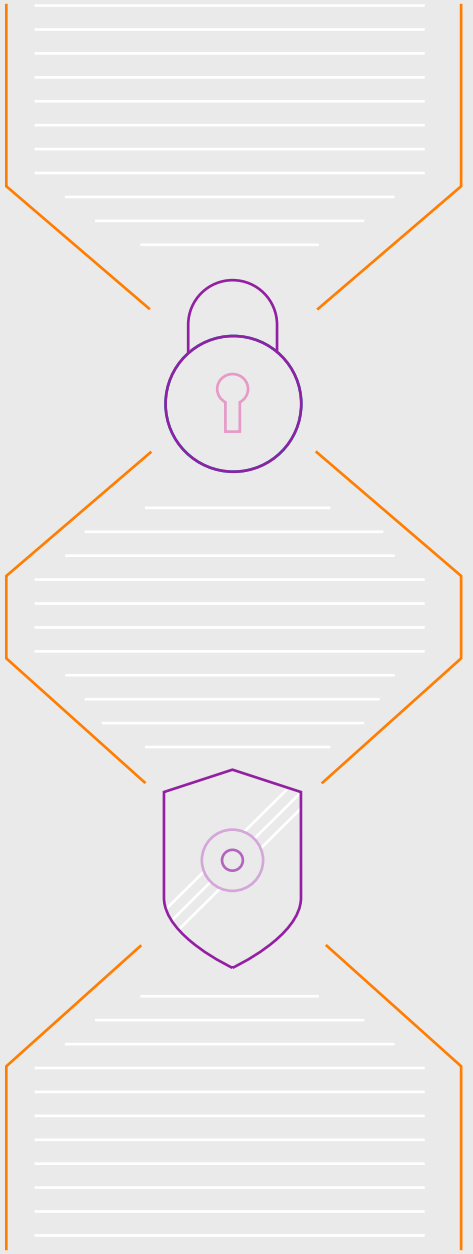
Datenschutz muss zu einem festen Bestandteil der Unternehmensstruktur werden. Sie muss unternehmensweit umgesetzt werden und alle Mitarbeiter einbeziehen, da jeder von ihnen mit Daten zu tun hat.

In diesem E-Book wird solch ein neuer, ganzheitlicher Ansatz zur Sicherstellung des Datenschutzes vorgestellt. Zudem erfahren Sie, wie Sie die Herausforderungen einer sich ändernden Bedrohungslandschaft meistern.

Dieses E-Book ist das Ergebnis unserer Zusammenarbeit mit Duzenden von CISOs, Datenschutzbeauftragten, CDOs und CIOs zur Verbesserung von Datenschutz und -sicherheit, ergänzt durch unsere umfassenden Fachkenntnisse zum Thema Data Security Intelligence und Schutztechnologien.

Nach der Lektüre dieses E-Books wissen Sie, wie effektiver Datenschutz heutzutage aussieht und wie Sie das Gelernte in die Praxis umsetzen können.

Fangen wir an.



Teil 1: Datenschutz ist in aller Munde

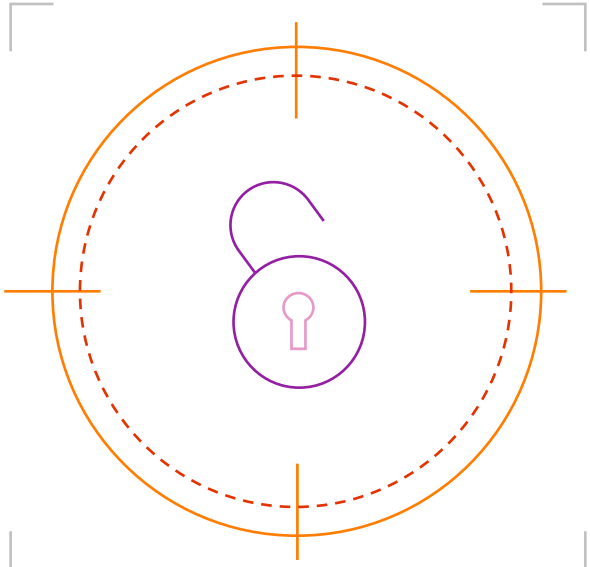
Was der Begriff „sensible Daten“ in diesem E-Book bedeutet

Es gibt Duzende von Definitionen für den Begriff „personenbezogene oder sensible Daten“, doch in diesem E-Book werden PII-Daten (personenbezogene Daten), PCI-Daten (Kreditkartendaten) und PHI (vertrauliche Gesundheitsdaten) als sensible Daten bezeichnet.

Datenschutzvorschriften konzentrieren sich auf personenbezogene Daten (PII). Dies ist ein Sammelbegriff für sämtliche Daten, die die Identifizierung einer Einzelperson ermöglichen. In der DSGVO werden 60 Elemente aufgeführt, die diese Kriterien erfüllen, darunter auch personenbezogene, demografische, finanzielle und gesundheitliche Daten.

Sensible Daten sind oft Zielscheibe von Angriffen, da sie sehr wertvoll sind. Cyber-Kriminelle können mithilfe von sensiblen Daten Bankkonten missbrauchen und auf andere, wertvolle Datenbestände zugreifen. Ein Hacker kann mithilfe der E-Mail-Adresse einer Person beispielsweise ihre Telefonnummer herausfinden. Diese Daten können dann schon ausreichen, damit ein Hacker auf das E-Mail-Konto eines Nutzers zugreifen kann.

Verstöße gegen den Datenschutz werden mit empfindlichen Strafen geahndet, wie Bußgeldern und rechtlichen Schritten. Zudem besteht das Risiko der Rufschädigung. Die Rufschädigung hat dabei meistens die schlimmsten Auswirkungen. Jede erfolgreiche Kundenbeziehung beruht auf gegenseitigem Vertrauen und wenn dieses Vertrauen missbraucht wird, lässt es sich nur schwer wiederherstellen.



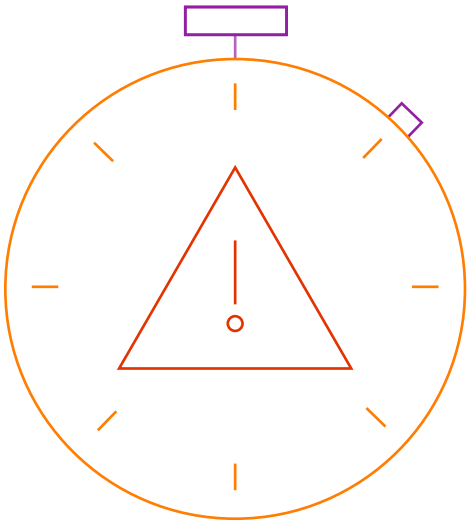
Ein dringendes Problem

Datenverlust ist für Unternehmen schon immer ein großes Problem gewesen, doch aufgrund verschiedener Faktoren ist dieses Problem heutzutage größer als je zuvor.

Zuerst einmal ist der Datenverlust heutzutage höher als in der Vergangenheit. 2017 betrug die Anzahl an Datensätzen, die in veröffentlichten Datenschutzverletzungen offengelegt wurden, mehr als 2,5 Mrd., was gegenüber dem Jahr 2016 einem Anstieg von 88 Prozent entspricht.[1] Und aufgrund von Datenschutzverletzungen wandern sehr viele Kunden zur Konkurrenz ab.

- **69 Prozent der Verbraucher weltweit sind bereit, sich gegen Unternehmen zu stellen, die den Datenschutz ihrer Meinung nach nicht ernst nehmen.**
- **62 Prozent der Verbraucher suchen die Schuld bei Verstößen gegen den Datenschutz bei Unternehmen – und nicht bei Hackern.**
- **83 Prozent der Verbraucher in den USA tätigen einige Monate lang nach einer Datenschutzverletzung oder einem schweren Sicherheitsvorfall keine Geschäfte mit dem betroffenen Unternehmen.**
- **21 Prozent der Verbraucher in den USA wenden sich permanent von einem Unternehmen ab, bei dem ein Datenverlust aufgetreten ist.**

Aufgrund der hohen Anzahl an Verstößen gegen den Datenschutz und der Reaktionen der Verbraucher sind Datenschutz und -sicherheit nicht nur eine Frage der Compliance, sondern haben bei Unternehmen höchste Priorität.



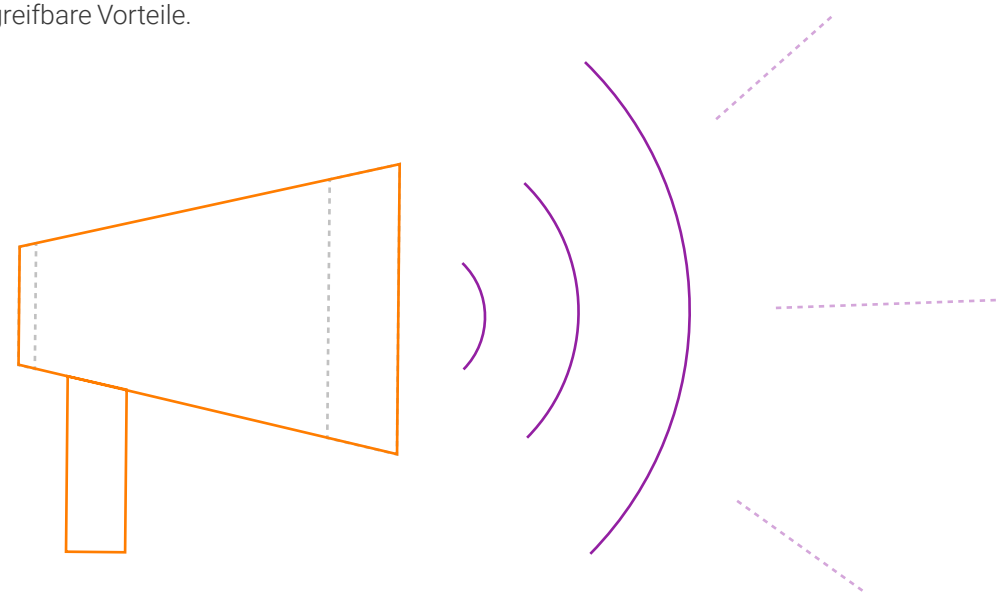
[1]Gemalto, Breach Level Index 2017, 2017

Was alleine letztes Jahr geschah:

- **Die DSGVO wurde endlich eingeführt**
  Diese wegweisende EU-Vorschrift ahndet Verstöße gegen den Datenschutz mit empfindlichen Geldstrafen und beinhaltet strenge Vorgaben, so dass Unternehmen ihre tagtäglichen Abläufe anpassen müssen.
- **Gesetzgeber haben gehandelt**
  In mehr als 80 Ländern gibt es Datenschutzvorschriften, und auch die Türkei, Indien, China, Brasilien, Singapur und weitere Länder gehen gegen Verstöße gegen die Datensicherheit an und setzen nationale und regionale Gesetze zum Umgang mit PII-, PCI- und PHI-Daten strikt um. 2018 haben 11 US-Bundesstaaten ihre Datenschutzgesetze aktualisiert.
- **Datenschutz wird groß geschrieben**
  Da in den Medien immer öfter von Datenschutzverletzungen und Datenmissbrauch die Rede ist, ist das Thema Datenschutz aktueller als je zuvor. Kunden interessieren sich immer stärker dafür, wie Unternehmen ihre Daten nutzen und misstrauen Unternehmen, die keine klar umrissenen Datenschutzrichtlinien haben.

Früher war der Datenschutz einzig und allein Sache der IT. Doch heutzutage ist das Thema sowohl für Kunden als auch für den Unternehmensvorstand, Partner und Regulierungsbehörden wichtiger als je zuvor.

Dadurch wächst der Druck, dem Sie uns Ihr Team ausgesetzt sind, doch gleichzeitig entstehen auch ganz neue Möglichkeiten. Der Datenschutz bietet Unternehmen greifbare Vorteile.



Die digitale Transformation wird immer schneller

Aufgrund der Programme zur Sicherstellung von Datenschutz und Data Governance haben Sie die Möglichkeit, eine Datengrundlage für die digitale Transformation zu schaffen. So können Sie ermitteln, wo genau sich Daten in Ihrem Unternehmen befinden. Sie können Prozesse, Systeme und Anwender verstehen, die diese Daten nutzen. Zudem können Sie Richtlinien und Geschäftsregeln zur Sicherstellung der Qualität, des Schutzes und der Verwendung dieser Daten erstellen.

Ermittlung, Katalogisierung, Verknüpfung und Governance von Daten unterstützen digitale Unternehmensinitiativen, wie beispielsweise Folgende:

- **Analytics and Machine Learning: Datenexperten können Daten schneller finden und bereinigen.**
- **Optimierung von Geschäftsprozessen: Ein vereinfachter und automatisierter Datenaustausch zwischen Systemen.**
- **Kundenerlebnisse: Besseres Verständnis der Beziehungen zwischen Kunden, Produkten und Vertriebskanälen.**

Bessere Kundenbeziehungen

Verbraucher möchten bei Unternehmen einkaufen, die den Datenschutz nachweislich ernst nehmen. Laut Capgemini berücksichtigen 77 Prozent der Verbraucher Cybersicherheit und Datenschutz bei der Wahl eines Einzelhändlers[2], und 27 Prozent sagen, dass sie bereit sind, für bessere Sicherheits- und Datenschutzfunktionen mehr zu zahlen.[3]

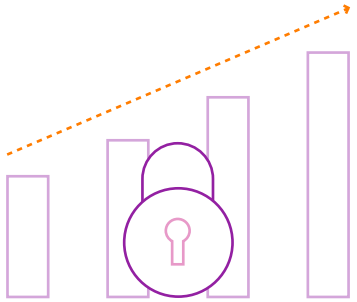
Doch nur wenige Unternehmen werden diesen Anforderungen gerecht. Nur 25 Prozent der Verbraucher sind der Meinung, dass Unternehmen verantwortungsvoll mit personenbezogenen Daten umgehen.[4]

Hier besteht für Unternehmen großes Potenzial. Wenn Sie strikte Richtlinien zum Datenschutz umsetzen, verantwortungsvoll mit personenbezogenen Daten umgehen und keine Verstöße gegen die Datensicherheit vorliegen, gewinnen Sie das Vertrauen der Verbraucher – die Voraussetzung für langjährige Kundenbeziehungen.

Geringere Versicherungskosten

Versicherungsgesellschaften, die Cyber-Versicherungen anbieten, integrieren Datensicherheit in ihre Analysen. Durch Programme für Privacy by Design, d. h. eingebauten Datenschutz, sowie Data Governance demonstrieren Sie ein striktes Risikomanagement, was zu geringen Versicherungsprämien führen kann.

Dies sind nur einige, wenige Beispiele. Zusammenfassend lässt sich sagen, dass Datenschutz mehr ist als nur Compliance – eine Grundvoraussetzung für jedes Unternehmen, das sich gegenüber der Konkurrenz durchsetzen möchte.



[2] Capgemini, Cybersecurity: The new source of competitive advantage for retailers, 2018
[3,4] PwC, Revitalizing privacy and trust in a data-driven world, 2018

Teil 2: Unternehmensdaten kennen und schützen

Warum nachhaltiger Datenschutz so schwierig ist

Bis vor kurzem waren Datenschutz und -sicherheit Zeitpunktaktivitäten zum Schutz einer klar begrenzten Umgebung. Dieser Ansatz funktioniert heutzutage jedoch nicht mehr. Privacy by Design erfordert kontinuierlichen Schutz auf Datenbestandsebene. Dies hat vier Gründe:

1. Ihre Daten sind überall

Sie werden unternehmensweit verwendet und verbergen sich in Datensilos, auf die oft kaum Zugriff möglich ist. Daten befinden sich auch außerhalb der traditionellen Unternehmensgrenzen, beispielsweise in AWS oder Azure. Zudem gelangen sie in SaaS-Anwendungen von Drittanbietern, die von Ihren Anwendern benötigt werden.

2. Ihre Daten werden auf immer neue Arten verwendet

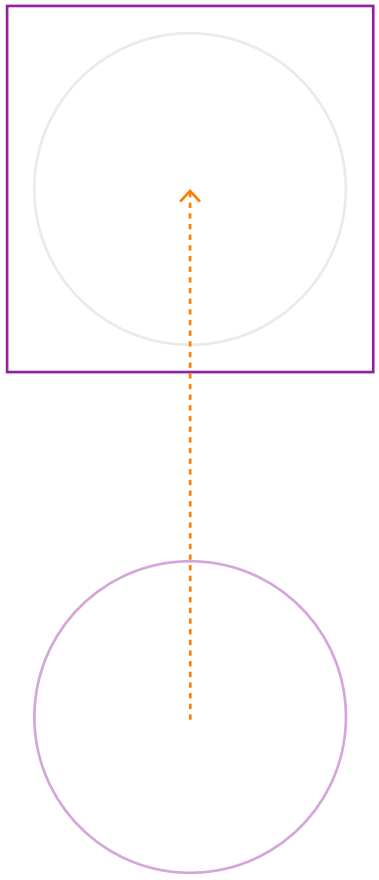
Die Anzahl der Abteilungen, Funktionen und Mitarbeiter, die Daten für Reporting-Zwecke, Analytics, neue Anwendungen und Services nutzen, steigt enorm schnell an. Und Menschen – ob gezielt oder unabsichtlich – stellen die größte Sicherheitsbedrohung dar.

3. Das Datenvolumen steigt an

Ihr Unternehmen wird von Daten überflutet, und dieser Trend steigt weiterhin an. Viele große Unternehmen bearbeiten Daten im Petabyte-Bereich. Und dieses Volumen steigt Monat für Monat um ein zusätzliches Terabyte an. Rund 30 Prozent dieser Daten sind sensibler Natur.

4. Die Datenschwindigkeit steigt an

Es wird immer einfacher, riesige Datenmengen mit nur einem Mausklick oder durch Antippen für verschiedene Systeme freizugeben. Dabei hat sich herausgestellt, dass traditionelle Sicherheitsmaßnahmen durch Social Engineering effektiv umgangen werden können.



Ein dringendes Problem

Wie wir bereits gesehen haben, müssten Sie miteiner riesigen Datenmenge fertig werden, die immer schneller immer weiter weg bewegt wird. Wenn Sie in der Lage sind, Sicherheitskontrollen auf Datenbestandsebene umzusetzen, können Sie Daten völlig unabhängig vom Speicherort schützen, selbst über die Unternehmensgrenzen hinaus.

Die Umsetzung eines effektiven Datenschutzprogramms ist zwar kein Kinderspiel, aber durchaus machbar. Mit den richtigen Menschen, Prozessen und Technologien können Sie die oben erwähnten Probleme meistern und sich auf eine ungewisse Zukunft vorbereiten.

Die folgenden sechs Schritte sind das Ergebnis unserer Zusammenarbeit mit Duzenden von CISOs, Datenschutzbeauftragten, CDOs und CIOs zur Verbesserung von Datenschutz und -sicherheit, ergänzt durch unsere umfassenden Fachkenntnisse zum Thema Data Security Intelligence und Schutztechnologien.

1. Festlegung von Richtlinien und Regeln

Verstehen Sie Zweck, Verwendung, Systeme und Menschen, die an der Verarbeitung personenbezogener und sensibler Daten beteiligt sind. So können Sie Datenschutzrichtlinien erstellen, Verantwortlichkeiten zuweisen und transparentes Consent Management ermöglichen.

2. Ermittlung und Klassifizierung von Daten

Finden Sie personenbezogene Daten im gesamten Unternehmen, völlig unabhängig vom Speicherort, und klassifizieren Sie Sensibilität und Wichtigkeit gemäß internen Richtlinien und externen Vorschriften. Finden Sie heraus, wann Daten in Länder übermittelt werden, für die spezielle Datenschutzvorschriften gelten und kennen Sie die Vorgaben für jede Region.

3. Verknüpfung von Identitäten

Identitäten sind das Kernstück des Datenschutzes. Personenbezogene und sensible Daten müssen präzise und ganzheitlich mit den Einzelpersonen verknüpft werden, die sie in den verschiedenen Systemen repräsentieren. Dies ist angesichts der Zugriffsrechte von Datensubjekten wichtig sowie hinsichtlich der erforderlichen Meldung von Verstößen.

4. Risikoanalyse

Stellen Sie das Datenschutzrisiko basierend auf Data Stores, Standorten und Richtlinien nach, um es zu bewerten. So können Sie Gegenmaßnahmen funktions-, landes- und bereichsübergreifend besser planen und priorisieren.

5. Schutz und Reaktion

Nutzen Sie Zugangsbeschränkungen und Sicherheitsmechanismen, wie Verschlüsselung, Anonymisierung und Pseudonymisierung. Überwachen und verfolgen Sie die Verwendung und Bewegung von Daten. Automatisieren Sie das Consent Management und die Anfragen von Datensubjekten zur Ausübung von Rechten.

6. Messung und Reporting

Verfolgen Sie Compliance- und Risiko-Indikatoren, um Datenschutzstrategie und -maßnahmen aufeinander abzustimmen. Bieten Sie Dashboards für mehr Transparenz und unterstützen Sie die funktionsübergreifende Zusammenarbeit und Verantwortung. Automatisieren Sie Erfassung und Abgleich von Informationen für das Audit Reporting.

Damit diese Funktionen effektiv sind, müssen Sie permanent angewendet werden, da sich Daten und Datenverwendung kontinuierlich ändern. Sie sollten integriert werden, damit Datenschutzbeauftragte und Sicherheitsexperten eine klare und zentrale Übersicht über Risiken und Bedrohungen erhalten. Zudem müssen sie skalierbar sein, um das Unternehmen bei Wachstum und Ausbau der Geschäftsaktivitäten zu unterstützen. Aufgrund der Menge an Daten, Anwendern und Anwendungen, die überprüft und geschützt werden müssen, geht es ohne Automatisierung nicht. Denn nur so wird die erforderliche Geschwindigkeit erreicht und vorhersehbare und zuverlässige Ergebnisse erzielt.

Und aufgrund der steigenden Anzahl an Datenschutzgesetzen und -vorschriften sorgt eine zentrale Verwaltung dafür, dass Richtlinien und Leitfäden des Unternehmens konsistent angewendet werden, um das Change Management zu vereinfachen. Aufgrund der vielfältigen Daten und Status bietet sich der Einsatz einer visuellen Lösung an, um komplexe Informationen auf eine einfache Art und Weise an technische und Business User weiterzuleiten.

Dabei spielt die Automatisierung eine tragende Rolle. Sie müssen Millionen von Datenpunkten schützen, so dass manuelle Prozesse zu zeitaufwändig und kostspielig sind. Sie sind oftmals so langsam, dass sie bereits veraltet sind, bevor sie überhaupt abgeschlossen worden sind.

Die Automatisierung von Zugangsbeschränkungen durch die Umsetzung von Richtlinien und die Nachverfolgung von Metadaten zahlt sich dabei aus, um in einer sich schnell ändernden Umgebung nicht die Kontrolle und den Überblick zu verlieren.

Das mag sich schwierig anhören, ist aber ansich ganz einfach. Künstliche Intelligenz ist heutzutage so weit, dass Data Security Intelligence Tools und Datenschutz-Tools „intelligente“ Datenschutzrichtlinien nutzen und in Echtzeit anwenden können.

In der Praxis können diese Systeme neue und vorhandene Daten überwachen und die jeweiligen Stakeholder (z. B. für Datenschutz verantwortliche Teams) über Anomalien informieren. Sie können auch Korrekturmaßnahmen oder Maßnahmen zum Blockieren von Bedrohungen vorschlagen.

In diesen Szenarien wird die Bedrohung beseitigt, und zwar unabhängig von der Quelle. Es geht darum, die Daten selbst zu schützen und Zugriffsmuster oder Verhalten von Anwendern zu erkennen, die auf einen unangemessenen oder unbefugten Zugriff hinweisen.

Daran wird deutlich, wie leistungsstark die Automatisierung wirklich ist. Automatisierung erleichtert nicht nur Datenschutz- und Sicherheitsexperten das Leben, indem manuelle Prozesse automatisiert werden, sondern sie erhöht auch die Sicherheit und macht das Unmögliche möglich.

Warum der Zugriff auf Daten so wichtig ist

Neue Datenschutzgesetze betonen, wie wichtig es ist, den Zugriff auf PII-Daten zu ermöglichen.

Laut der DSGVO müssen Sie in der Lage sein, Kundendaten auf Anfrage von Kunden zu löschen, zu verschieben oder zu ändern. Zudem haben Kunden das Recht, ihre Zustimmung zu erteilen bzw. zu widerrufen, und Sie müssen diesen Wünschen nachkommen.

Daher sind detaillierte Zugriffsbeschränkungen gefragt, die den Anforderungen der Nutzer in Abhängigkeit ihrer Rolle, ihres Standorts und des Zeitpunkts des Zugriffs gerecht werden. Es ist kontraproduktiv, sensible Daten durch so starre Sicherheitsmethoden zu schützen, dass das Consent Management nicht angepasst oder Daten nicht an Kunden weitergeleitet werden können.

Wählen Sie einen schrittweisen Ansatz

Da bei Datenschutz und -sicherheit zahlreiche Hürden zu bewältigen sind, sollten Sie nicht versuchen, alles auf einmal zu tun. Das wäre nicht nur unrealistisch, sondern auch gefährlich. Je weiter Sie Sicherheitsfunktionen strecken, desto wahrscheinlicher ist es, dass es zu Sicherheitslücken kommt.

Daher bietet sich ein schrittweiser Ansatz an. Beginnen Sie mit den sensibelsten Daten, einer kleinen Gruppe an Anwendern und einem klaren Ziel. Sobald Sie nachweisliche Ergebnisse erzielt haben, können Sie Ihr Programm erweitern, umneue Herausforderungen zu meistern.

Zunächst einmal müssen Sie festlegen, welche Daten der Begriff „sensible Daten“ beinhaltet. Dabei sind Frameworks zur Risikobewertung hilfreich. Dabei geht es darum, verschiedene Kriterien zur Festlegung sensibler Daten zu etablieren und Datenbestände dann entsprechend zu bewerten. So können Sie erkennen, wie sensitiv Daten sind und eine einheitliche und objektive Definition sensibler Daten festlegen.

Bei diesem Ansatz wird auch die Kurzlebigkeit von Daten berücksichtigt. Wenn sich ein Merkmal eines Datenbestands ändert, beispielsweise Speicherort, Verwendung, Verbreitung usw., kann die Risikobewertung entsprechend angepasst werden.

Viele der Kriterien Ihres Frameworks gelten spezifisch für Ihr Unternehmen. Doch es gibt einige allgemeine Fragen, die Sie sich stellen können:

- **Welche Art von Daten nutzen wir und für welchen Zweck?**
- **Welche rechtlichen Vorschriften regeln Verwendung und Sicherheit von Daten?**
- **Wer sind die Dateneigentümer auf betrieblicher und technischer Seite?**
- **Wie oft werden die Daten aufgerufen und der Zugriff kontrolliert?**

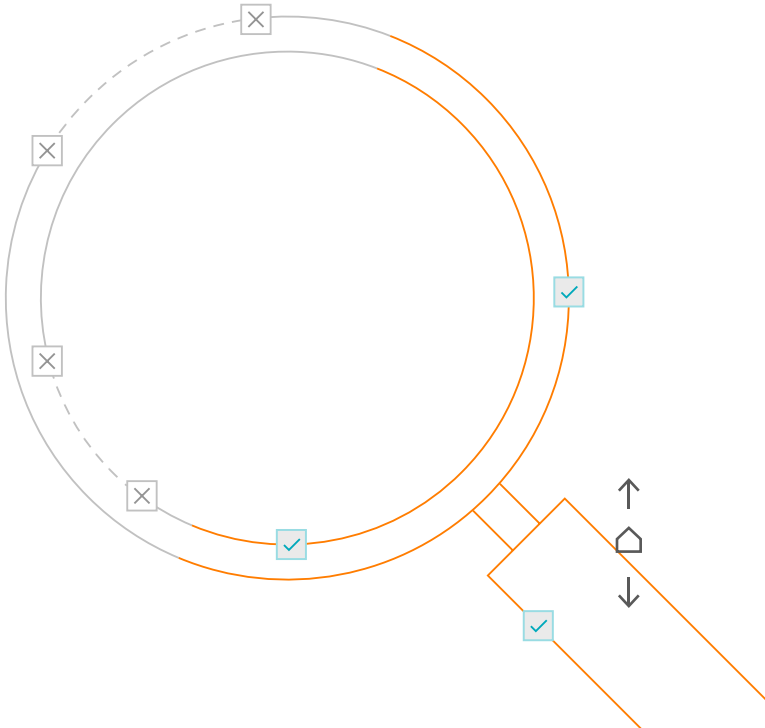
Sie können diese Fragen wahrscheinlich nicht alleine beantworten, sondern benötigen die Mithilfe der Mitarbeiter, die tagtäglich mit diesen Daten zu tun haben. In Gesprächen, Umfragen und Einschätzungen mit Anwendungseigentümern, Sicherheitsanalysten, DBAs, Business-Analysten und Mitarbeitern mit Kundenkontakt werden sich Datentypen und Nutzerrollen, Dateneigentümer und Verwendungszwecke herauskristallisieren.

Sobald Sie Ihre Daten definiert haben, können sie mithilfe automatisierter Prozesse ermittelt und klassifiziert werden. Zudem können Sie die Risikobewertung nutzen, um Prioritäten aufgrund folgender Faktoren festzulegen: wie Daten genutzt, wohin sie verschoben und wie sie geschützt werden.

Mit diesem Prozess können Sie Daten über Geschäftsprozesse, Regionen und funktionale Gruppen hinweg miteinander verknüpfen. Darüber hinaus erhalten Sie Antworten auf dringende Fragen, wie:

- **Wo befinden sich personenbezogene Daten und wie werden sie über verschiedene Datenquellen miteinander verknüpft?**
- **Welche potenziellen Risiken gibt es, und werden Daten angemessen geschützt?**
- **Entspricht der Datenschutz des Unternehmens den Vorgaben der Regionen, in denen das Unternehmen tätig ist?**
- **Sind Investitionen in den Datenschutz und Ressourcen auf die richtigen strategischen Ziele und betrieblichen Aktivitäten ausgerichtet?**

Die Antworten auf diese Fragen geben Aufschluss darüber, welche Maßnahmen Sie ergreifen sollten. Wenn sich beispielsweise herausstellt, dass Fehler von Mitarbeitern ein Risiko für den Datenschutz darstellen, könnten Sie beispielsweise Mitarbeiterschulungen anbieten.

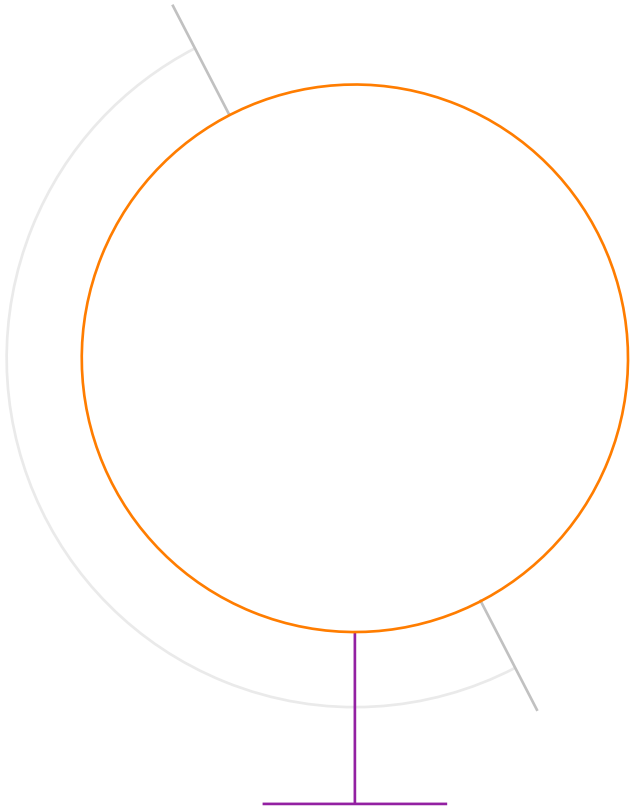


Schlussfolgerungen

Ohne Datenschutz geht es nicht

Datenschutzvorschriften sind zurzeit in aller Munde, doch dabei dürfen wir nicht aus den Augen verlieren, dass es um mehr geht als nur um Compliance. Die strikten Richtlinien und Programme zur Sicherstellung von Data Governance und Datenschutz, die gesetzlich vorgeschrieben sind, wirken sich auch maßgeblich auf den Unternehmenserfolg aus. Ihre Kunden, Mitarbeiter und Partner erwarten, dass Sie verantwortungsvoll mit ihren Daten umgehen. Und auch für die digitale Transformation sind Daten erforderlich, um neue Absatzchancen zu erkennen, Geschäftsprozesse zu optimieren, Kosten zu reduzieren und Risiken zu steuern.

Diese Aufgabe erscheint auf den ersten Blick fast unlösbar, doch mithilfe eines schrittweisen Ansatzes und unserer sechs Schritte können Sie groß denken, klein beginnen und schnell skalieren. Neue Technologien unterstützen Sie bei der Automatisierung von Aufgaben, der Erhöhung der Transparenz und der Förderung der Zusammenarbeit – kontinuierlich und präzise. Mit einem ganzheitlichen Ansatz und einer zentralen Technologie-Strategie sind Sie für die schnelllebige Datenschutz-Landschaft bestens gewappnet.

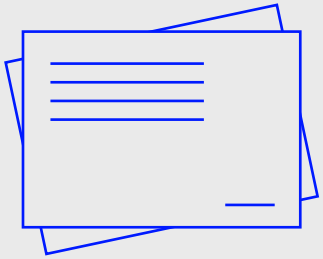


Weitere Informationen

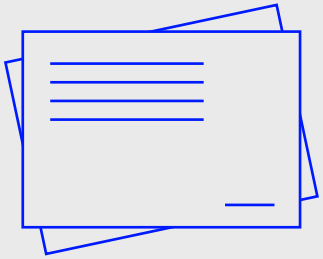
Weitere Ressourcen

Video zu Datenschutz und -sicherheit

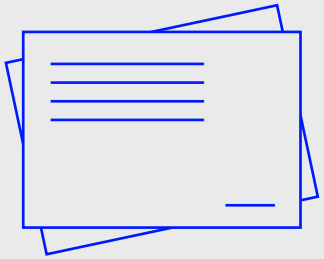
GDPR for Dummies



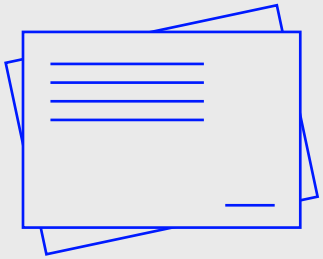
Datenblatt zu Secure@Source



White Paper zu Datenschutz und -sicherheit



Datenblatt zu Data Masking



Informationen zu Informatica

Die digitale Transformation ändert unsere Erwartungshaltung hin zu besserem Service und schnellerer Lieferung zu geringeren Kosten. Unternehmen müssen sich neu orientieren, um wettbewerbsfähig zu bleiben. Dabei spielen Daten eine zentrale Rolle.

Als führender Anbieter für Enterprise Cloud Data Management unterstützt Informatica Sie dabei, sich als innovativer Vorreiter zu etablieren – völlig unabhängig von Ihrer Branche, Kategorie oder Nische. Wir ermöglichen eslhnen, agiler zu werden, neue Wachstumsmöglichkeiten wahrzunehmen und Innovationen voranzutreiben.

Informatica ist zu 100 % auf Daten fokussiert, und bietet Unternehmen vielseitige Lösungen, um sich am Markt durchzusetzen.

Entdecken Sie jetzt das gesamte Angebot von Informatica, um das komplette Potenzial Ihrer Daten zu nutzen und so die nächste intelligente Innovation auf den Weg zu bringen.

Weitere Informationen:

Informatica GmbH
Ingersheimer Str. 10, 70499 Stuttgart
Tel.: +49 (0) 711 139 84-0
Fax: +49 (0) 711 139 84-600
Gebührenfrei in den USA: 1.800.653.3871

www.informatica.com/de
linkedin.com/company/informatica
twitter.com/Informatica
facebook.com/InformaticaLLC/

KONTAKT

IN19-0119-3582

Informatica™