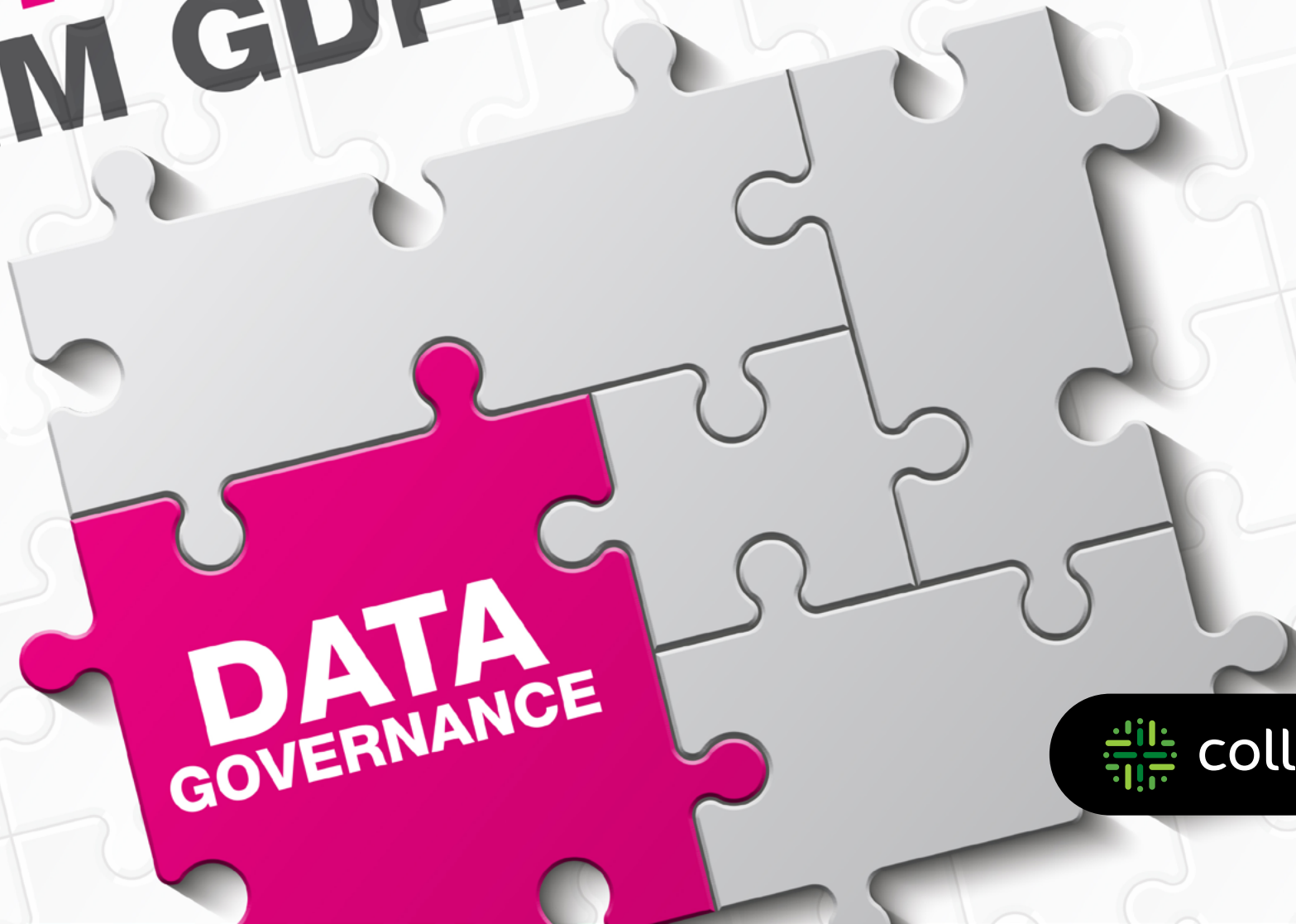
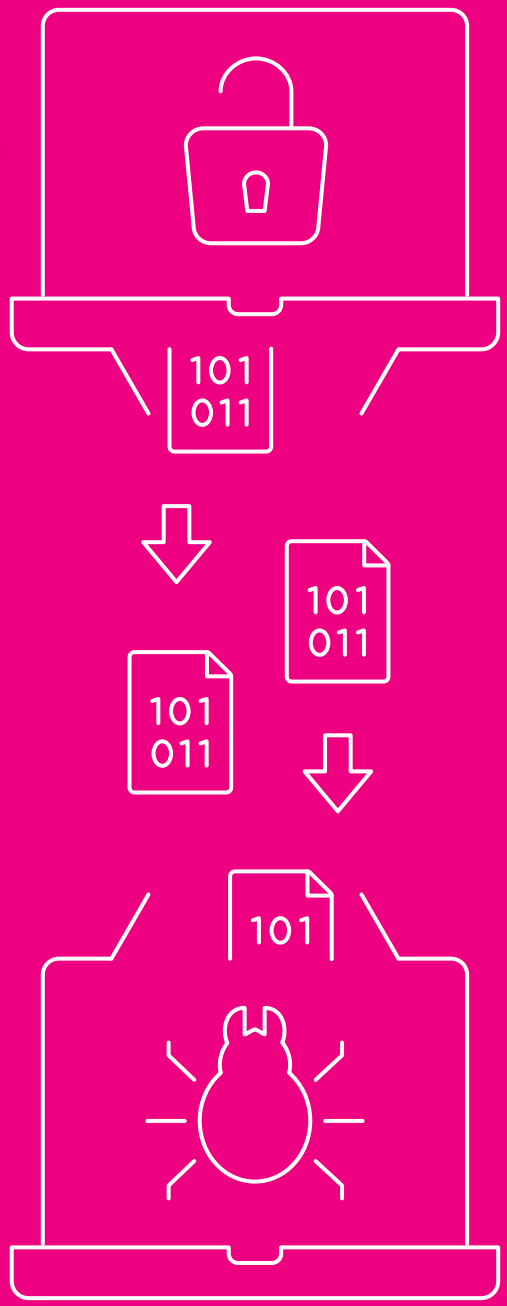
DAS FEHLENDE STÜCK IM GDPR-PUZZLE



collibra™

Datenschutzverletzungen.
Hacker.
Cyberkriminalität.

Allein das Erwähnen dieser Begriffe lässt es einen eiskalt den Rücken herunterlaufen.



Heutzutage generieren Menschen und Firmen Daten mit atemberaubender Geschwindigkeit. Und gleichzeitig mit den Daten wächst auch die Anzahl der Datenschutzverletzungen und „Beinaheunfälle“ – Sicherheitsvorfälle, die zu schweren Datenschutzverletzungen hätten führen können, was aber (glücklicherweise) nicht passiert ist.

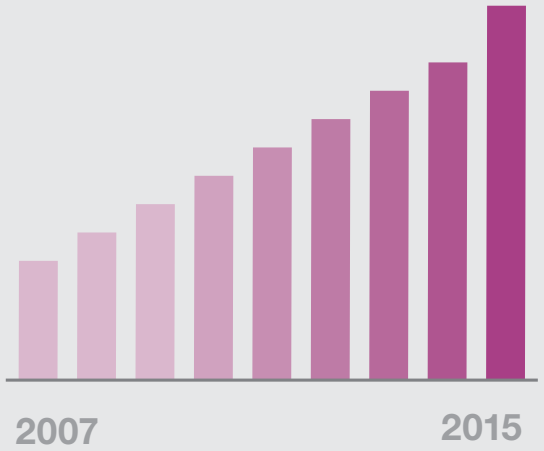
Aber darin besteht das offensichtliche Dilemma.

Diese so schnell erzeugte Datenmenge ist schwer zu kontrollieren. Und dabei geht es nicht nur um das Datenvolumen. Sondern auch um den Wert der Daten, die über Sie erfasst werden. Denken Sie an die Daten, die Sie freiwillig auf Internetseiten eingeben: Adresse, Geburtsdatum, Kreditkartennummern, Passwörter und vieles mehr.

Nehmen Sie dazu dann die ANDEREN Informationen, die über Sie unbemerkt erfasst werden: Suchverlauf, besuchte Webseiten, Artikel in Ihrem Warenkorb und Einkaufshistorie. Und die Liste geht noch weiter.

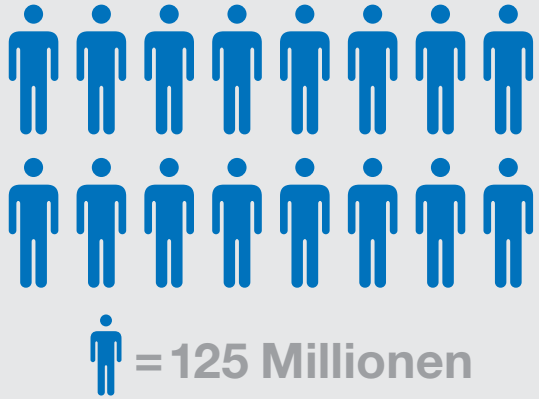
Je mehr der Wert dieser Daten steigt, desto mehr steigt auch das Interesse – und die Raffinesse – der Hacker.

2015 erreichten die Hackervorfälle ein 9-Jahres-Hoch.



(Quelle: ITRC)

Allein 2016 wurden über 2 Milliarden Datensätze gestohlen



(Quelle: ZDNet, Nov. 2016)

Während der ersten Hälfte des Jahres 2016 kam es zu 974 öffentlich bekannt gegebenen Datenschutzverletzungen, die zum Diebstahl oder Verlust von 554 Millionen Datensätzen führten.

(Quelle: Gemalto)

Und diese Zahlen werden noch weiter ansteigen.

Das IDC rechnet damit, dass sich die Datenschutzverletzungen bis 2020 auf nahezu **25 %** der Weltbevölkerung auswirken werden.

Finanzieller Gewinn

stellt auch weiterhin
das Hauptmotiv für
Datenschutzverletzungen dar.

Aber haben Sie auch an die anderen beunruhigenden Motive für das Stehlen privater, personenbezogener Daten gedacht wie z. B. Menschen oder Gruppen zu einer Verhaltensänderung zu zwingen oder Organisationen, Einzelpersonen und sogar Nationen in eine peinliche Lage zu bringen?

Die Weltwirtschaft ist von Daten abhängig. Aber wir müssen sicherstellen, dass wir die Rechte der Bürger schützen, um deren Daten sich diese Welt dreht. Und mit „wir“ meinen wir alle Unternehmen, die personenbezogene Daten von Personen erfassen, nutzen und speichern.

Klingt vertraut, oder?

Dieser Datentsunami birgt inhärente Risiken. Wir verstehen kaum die vorhandenen Daten, geschweige denn die unvorhergesehenen Möglichkeiten, wie sie gebraucht werden könnten.

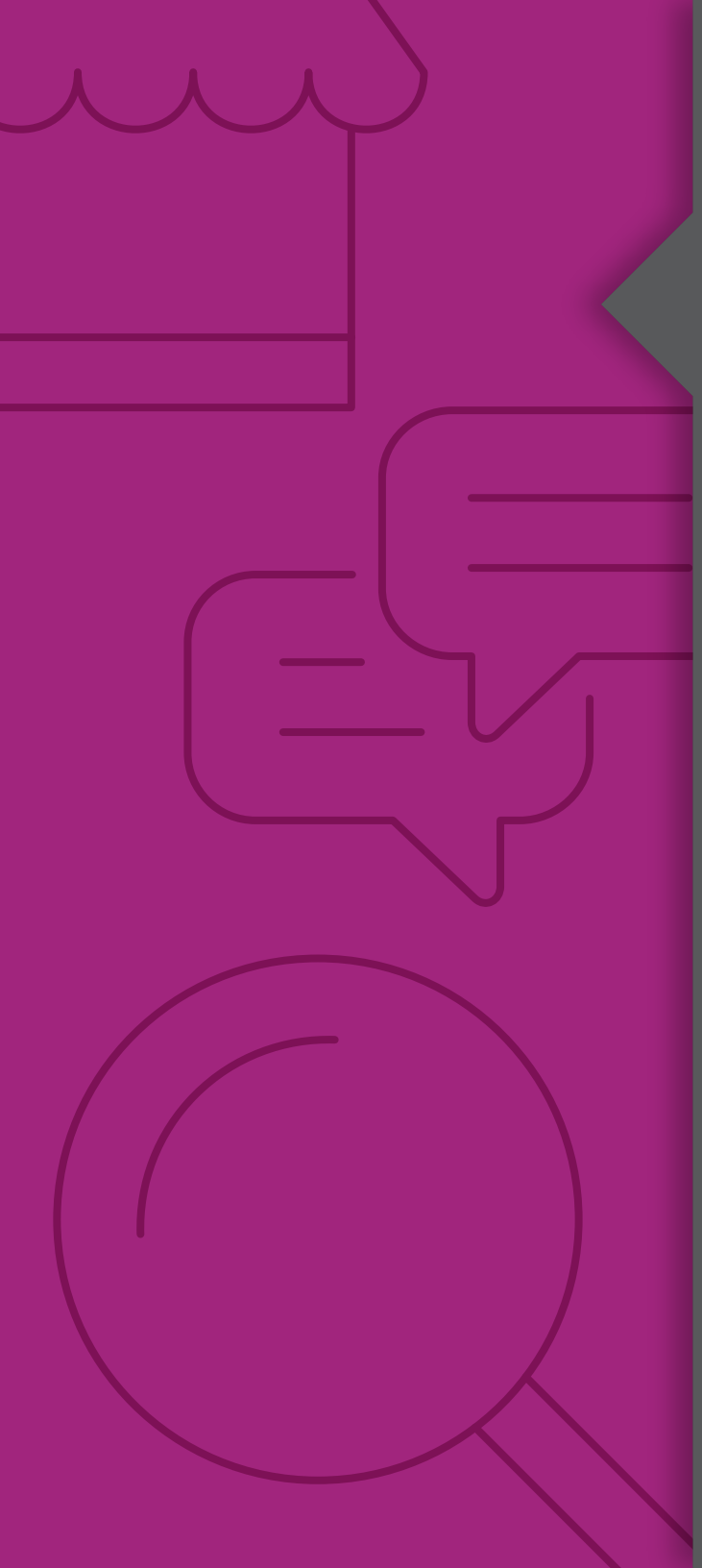
Fazit:
Das digitale Zeitalter benötigt eine Reihe von neuen Datenschutzregeln.

Im April 2016 hat die EU-Kommission die EU-Datenschutz-Grundverordnung **(General Data Protection Regulation, GDPR)** ratifiziert, mit der die Regeln für die Erfassung, Kontrolle und Zustimmung für die Nutzung personenbezogener Daten vereinheitlicht werden.

Durch GDPR wird der Umfang der Datenschutzgesetze zum Schutz der Datenrechte von EU-Bürgern erweitert.

- Einzelpersonen haben damit mehr Kontrolle darüber, wer ihre Daten besitzt und wie sie verwendet werden.
- Datenschutzverletzungen müssen von Organisationen innerhalb von 72 Stunden gemeldet werden.
- Organisationen sind in Bezug auf die Zustimmung von Personen hinsichtlich der Verwendung ihrer Daten an strengere Regeln gebunden.

Unter GDPR wird klargestellt, dass die Verantwortung für den Schutz der personenbezogenen Daten von Kunden und potenziellen Kunden auf den Schultern Ihrer Organisation liegt.



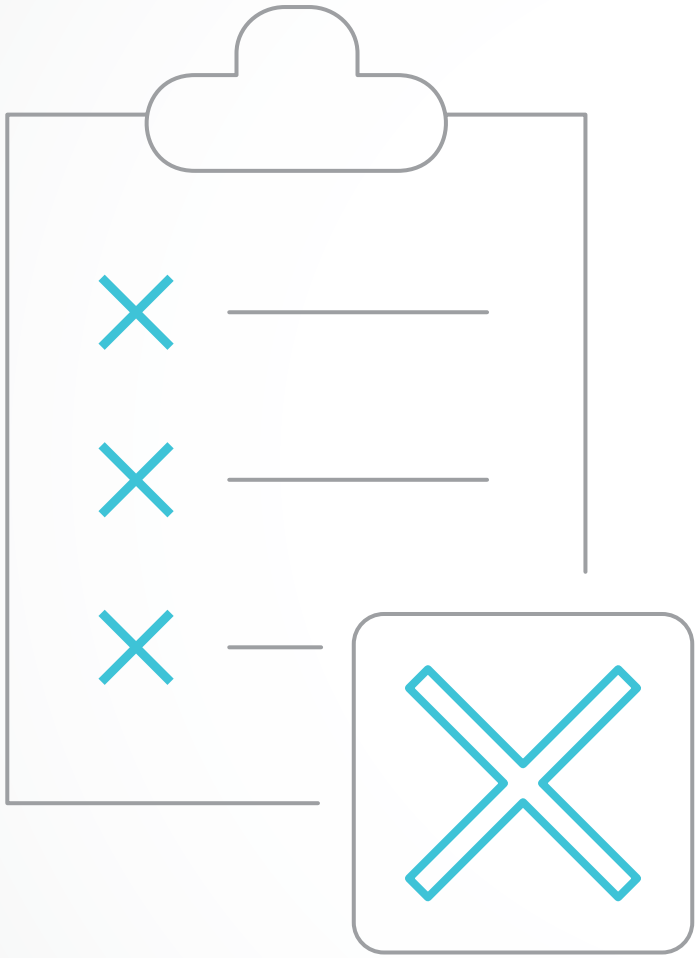
GDPR findet Anwendung auf personenbezogene Daten, die irgendwo innerhalb einer Organisation verwaltet und gespeichert werden.

Sie wird sich auf alle Bereiche eines Unternehmens auswirken. Marktplätze im Web, Social Networks, Suchmaschinen und andere internetbasierte Unternehmen – sowie Unternehmen in den Bereichen Finanzdienstleistungen, Einzelhandel, Konsumgüter, Kommunikation und natürlich das Gesundheitswesen – sind klare Ziele für die GDPR.

Heute handelt es sich um eine EU-Verordnung. Aber denken Sie an Ihre Kunden. Sind darunter auch EU-Bürger? GDPR gilt für alle Unternehmen innerhalb und außerhalb der EU, die europäischen Bürgern Waren und Dienstleistungen anbieten. Auch Ihre Organisation wird sich voraussichtlich an GDPR halten müssen.

GDPR muss von allen Organisationen ernst genommen werden.

Organisationen müssen sie ab dem ersten Tag **100%ig einhalten**.



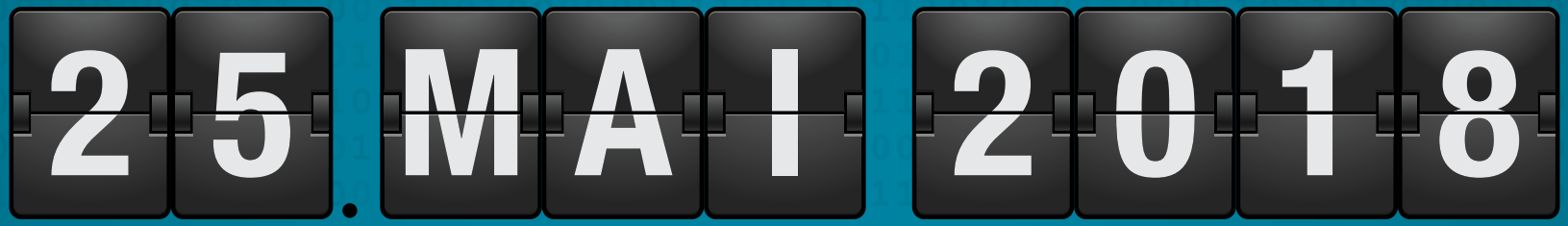
Die Regulierungsbehörden werden bei Nichteinhaltung von GDPR beträchtliche Strafen verhängen: bis zu **2–4 % des weltweiten Umsatzes** bei Nichteinhaltung der Verordnung.

Rechnen Sie nach.

Nur eine einzige Verletzung könnte bereits das Ende Ihres Unternehmens bedeuten.

Und je nach Verstoß könnte der Reputationsschaden dann langanhaltend oder sogar unüberwindbar sein. Ein einfaches „Es tut uns leid“ wird dann nicht ausreichen.

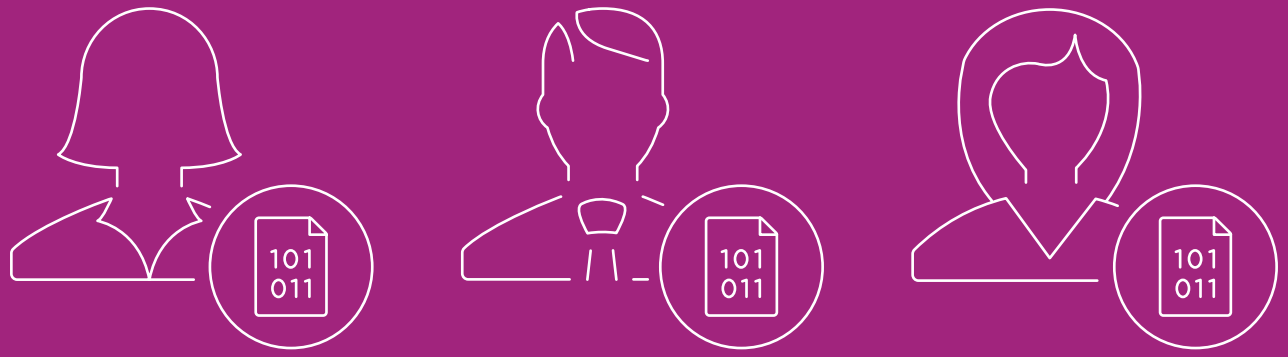
GDPR tritt am



in Kraft.

Der Countdown zur Compliance läuft also.

Aber auch wenn die GDPR-Regelung klar besagt, was getan werden muss, ringen viele Organisationen damit, wie es umgesetzt werden soll.



Beim Schützen und Sichern von Daten geht es nicht darum, für einen Schleier der Geheimhaltung zu sorgen. Es geht um das Aufbrechen von Strukturen. Es geht um Kontrolle. Es geht darum, die Daten bei Bedarf für die gesamte Organisation transparent zu machen.

Schließlich können Sie nur das schützen, was Sie auch kennen.

Um die Einhaltung von GDPR zu gewährleisten, müssen Sie zwei kritische Fragen beantworten und dies auch belegen können:

- Wo sind meine Daten?
- Wer ist für diese Daten verantwortlich?

Die Klassifizierung steht im Mittelpunkt von GDPR.

Die Identifizierung und Klassifizierung Ihrer Daten ist der erste Schritt zur Beantwortung dieser Fragen.

Beispiel:

- Welche Arten personenbezogener Daten sind bei Ihnen gespeichert?
- Wo befinden sie sich?
- Welcher Sicherheitsstandard ist erforderlich?
- Wer hat Zugriff?
- Wie werden die Daten verwendet?
- Sind Sie dazu berechtigt, diese Daten zu verwenden?

Die Fähigkeit, über Daten Bericht zu erstatten, ist von außerordentlicher Bedeutung, wenn es um die größten Herausforderungen in Bezug auf GDPR geht: Benachrichtigungen bei Verletzungen.

Unter dieser Verordnung müssen Firmen bestimmte Datenschutzverletzungen innerhalb von 72 Stunden nach dem Auftreten melden. Aber ohne Kontext ist es einfach nicht möglich, Antworten auf die wesentlichsten Fragen der Regulierungsbehörde zu geben.

Und nicht antworten zu können, kann sehr teuer werden. Erinnern Sie sich an die zuvor erwähnten heftigen Strafen?

Durch GDPR und die damit eingeführten weitreichenden Regeln für die Verwaltung, die Verarbeitung und das Löschen von Daten wird der Datenschutz noch komplizierter.

Es geht nicht mehr nur um das Aufspüren von Daten und die Gewährleistung ihrer Sicherheit. Es geht um die Erfassung des Datenkontexts und die Fähigkeit, nachzuweisen, alles für den Schutz der Daten einer Person und der Rechte der Person selbst zu tun.

Bei GDPR handelt es sich um eine weitreichende Verordnung.
Wo fängt man bei 99 Artikeln an?

Data governance führt Sie auf diesem Weg.

Data Governance kann als Unterstützung zur GDPR-Compliance dienen.

Es liefert die Rahmenbedingungen für den Umgang mit und die Definition von unternehmensweiten Richtlinien, Geschäftsregeln und Datenbeständen, um den erforderlichen Grad an Datenschutz und Qualität bereitzustellen.

Und durch Data Governance erhalten Ihre Daten einen Kontext. Es liefert die Antworten, die Sie für die Handhabung komplexer Angelegenheiten rund um die GDPR-Compliance benötigen.

Wenn Sie die Daten finden und verstehen können, können Sie auch darüber Bericht erstatten. So können Sie die für die Regulierungsbehörden erforderlichen Beweise bereitstellen und Ihre Organisation auf GDPR vorbereiten.

Verantwortlichkeit und **Rechenschaftspflicht**

ind die Merkmale einer guten Data Governance. Und sie sind für die GDPR-Compliance von höchster Bedeutung.

Darum sind Data Governance und GDPR das perfekte Paar.

Verantwortlichkeit

Datenschutz muss auf Vorstandsebene diskutiert werden. Die International Association of Privacy Professionals (IAPP) schätzt, dass Unternehmen nahezu 75.000 Datenschutzbeauftragte einstellen müssen, damit die Anforderungen von GDPR erfüllt werden.

Aufgabe:
Bestimmen Sie einen Chief Data Officer (CDO), der die Einführung von Kontrollen und Prozessen, die im Bezug auf Datenschutz und Privatsphäre erforderlich sind, überwacht.

Rechenschaftspflicht

Eine ordentliche Data Governance schließt die unternehmensweite Anstrengung zur Umsetzung der Rechenschaftspflicht innerhalb einer Organisation mit ein. Sie bricht Strukturen auf und ermächtigt die Daten-Stewards, für die Daten verantwortlich zu sein – damit sicher gestellt ist, dass diese korrekt, vertrauenswürdig und zugänglich sind.

Aufgabe:
Schaffen Sie in sich geschlossene Governance-Rahmenbedingungen für die gesamte Organisation, um so dauerhaft Risiken überwachen, Lücken schließen und den Fortschritt verfolgen zu können.

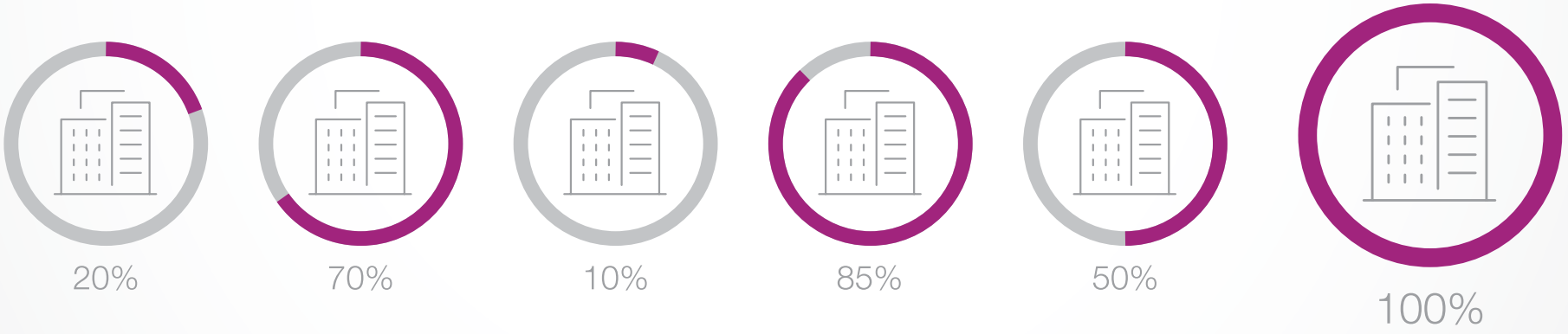
Durch GDPR wurde der Einsatz für Datenschutz und Datensicherheit erhöht.

Durch die Ankündigung hoher Geldstrafen bei Nichteinhaltung signalisiert die EU, wie Ernst sie es mit der Compliance meint.

Um GDPR zu entsprechen, benötigen Sie im Bezug auf Datenschutz und Privatsphäre neue Ansätze und Werkzeuge. Manuelle Ansätze und Tabellen werden nicht ausreichen. Ebenso wenig reicht ein weiteres, nachträglich installiertes IT-System aus. Wählen Sie einen dieser Wege, sollten Sie schon einmal das Firmenscheckbuch für die Bezahlung der Geldstrafen bereithalten.

Und wenn Sie die Planung und Budgetierung sowie die Organisations- und Infrastrukturänderungen für die Gewährleistung der GDPR-Compliance bedenken, wird schnell klar, dass die Vorbereitung der Organisation auf die Einhaltung von GDPR nicht über Nacht erfolgen kann.

Aber trotz des sich abzeichnenden Termins hat bisher lediglich ein kleiner Anteil der Firmen damit begonnen, Schritte zur Gewährleistung der Compliance einzuleiten.

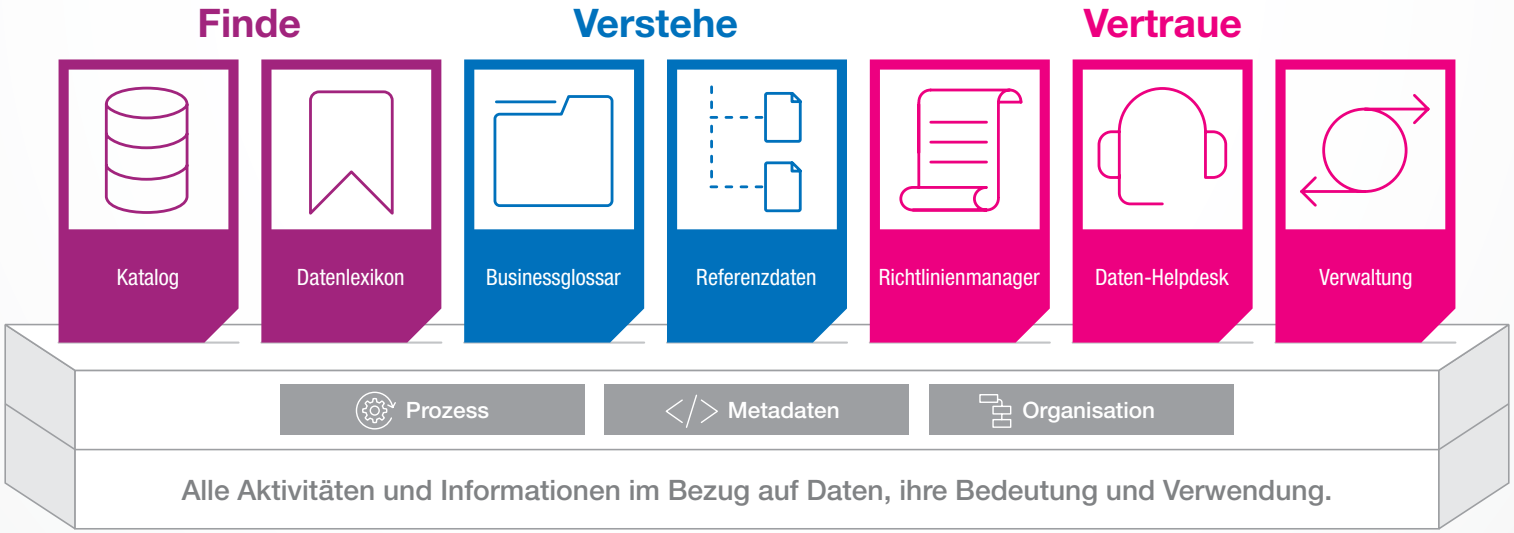


Das Navigieren der GDPR-Anforderungen ist kein geringfügiges Unterfangen.

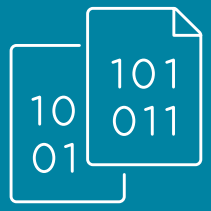
Aber Sie müssen diese Aufgabe nicht allein bewältigen.

Collibra unterstützt Organisationen bei dem Nachweis, dass sie einen korrekten Umgang mit Daten pflegen.

Collibra ist eine Plattform, die Personen, Richtlinien, Datenvereinbarung (Data Sharing-Vereinbarungen) und Definitionen steuert, mit einem Wort: alle Aktivitäten und Informationen in Bezug auf Daten, deren Bedeutung und deren Verwendung.



Eine ordentliche Data Governance bietet Organisationen viele Vorteile, indem Richtlinien, Kontrollen und Arbeitsabläufe bereitgestellt werden für:

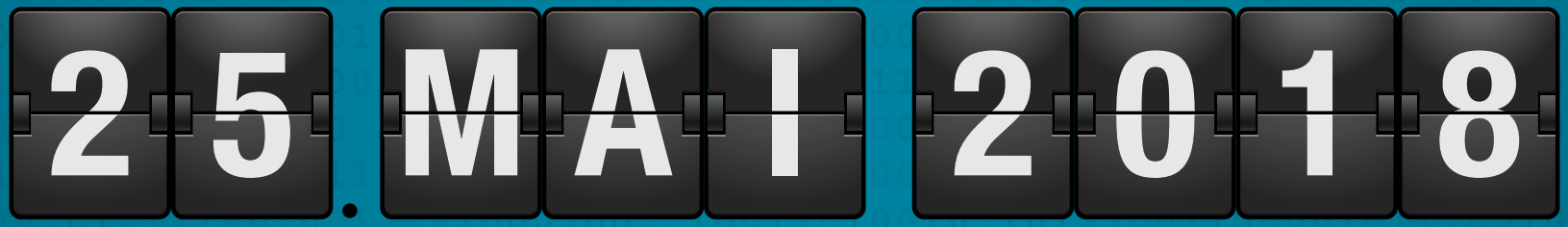


Dokumentieren von Daten und deren Herkunft

Festlegen entsprechender Richtlinien (und deren Durchsetzung).

Einführen von Rollen und Verantwortlichkeiten für alle Personen, die mit diesen Daten arbeiten.

Data Governance kann Ihnen bei der GDPR-Compliance unterstützend zur Seite stehen. Aber die Uhr tickt.



Gefährden Sie nicht Ihre Schlußfolgerung. Oder Ihre Reputation.

collibra™

collibra.com

info.collibra.com

Follow Us:
twitter.com/collibra