CGI

Experience the commitment®

Leitfaden zur Konformität mit der Datenschutz-Grundverordnung (DSGVO)

So machen Sie Ihr Unternehmen fit für die neuen Datenschutzanforderungen in der EU

Leonhardt Wohlschlager

Mai 2019

Management Summary

Strafen für Nichtkonformität mit der EU-Datenschutz-Grundverordnung (DSGVO)

TOP-MANAGER POSITIONIEREN DATENSCHUTZ NEU

Mit der neuen DSGVO (im Englischen General Data Protection Regulation, kurz GDPR) werden Unternehmen und Behörden innerhalb der Europäischen Union (EU) seit dem 25. Mai 2018 stärker in die Pflicht genommen. Bußgelder für Ordnungswidrigkeiten können gemäß Artikel 83 DSGVO zukünftig bis zu 20 Millionen Euro bzw. – bei Unternehmen – sogar bis zu vier Prozent des weltweiten Jahresumsatzes pro Einzelfall betragen, wobei der jeweils höhere Wert gewählt wird.

Die DSGVO kommt dabei in allen Mitgliedstaaten der EU zur Anwendung. Zweck der DSGVO ist es, die Datenschutzgesetzgebung, d. h. die Regeln zur Verarbeitung personenbezogener Daten, in diesen Staaten anzugleichen. Damit sollen die Ziele zum Schutz natürlicher Personen bei der Datenverarbeitung umgesetzt, ein freier Datenverkehr innerhalb des europäischen Binnenmarktes ermöglicht und Wettbewerbsverzerrungen aufgrund unterschiedlicher Datenschutzgesetze innerhalb der EU vermieden werden.

Unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten betroffener natürlicher Personen initiieren die Top-Manager der betroffenen Unternehmen und Behörden geeignete technische und organisatorische Maßnahmen, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten gemäß DSGVO erfolgt.

So sind viele Organisationen bereits seit dem 25. Mai 2018 in der Lage, der zuständigen Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten nach Art und Umfang binnen 72 Stunden zu melden, nachdem die Verletzung bekannt geworden ist (Art. 33 DSGVO), und die betroffene Person unverzüglich zu benachrichtigen (Art. 34), wenn ein hohes Risiko für die persönlichen Rechte und Freiheiten vorliegt.

In diesem Whitepaper finden Sie fünf Konzepte, die Sie beachten sollten, um Konformität mit der DSGVO zu erzielen. Außerdem erhalten Sie Empfehlungen zu Lösungen, die Ihnen das Leben mit der DSGVO maßgeblich erleichtern.

Wenn Sie einen kurzen Überblick benötigen, wie Ihnen CGI bei der DSGVO und dem Thema Cybersecurity helfen kann, fordern Sie das entsprechende Factsheet bei Ihrem CGI-Ansprechpartner einfach an.

Inhalt

Über dieses Dokument

Dieses Whitepaper ist Teil des Insurance-Business-Consulting-Portfolios. Es wurde in Zusammenarbeit mit der deutschlandweiten Insurance Practice erstellt. Mehr als 5.000 CGI-Mitglieder weltweit arbeiten täglich an der Umsetzung von Compliance-Themen und erhöhen den Geschäftswert der Kundenorganisationen.

Warum CGI?

- CGI setzt die Vorgaben und Anforderungen der DSGVO zuverlässig um.
- Das Vorgehen liefert Ansätze zur Erhöhung des Geschäftswerts.
- Unsere Experten kennen die Regulatorik und die Data-Governance-Methoden.
- Sie erhalten eine ausgewiesene Expertise dazu, wie moderne IT in diesem Feld unterstützen kann.

1. Einführung

Falls Ihre Organisation in der EU geschäftlich aktiv ist, haben Sie inzwischen gehört, dass die DSGVO seit dem 25. Mai 2018 zur Anwendung kommt.

Mit diesen neuen, gegenüber den bisherigen Regeln meist restriktiveren Vorschriften sollen die Datenschutzvorgaben in allen EU-Mitgliedstaaten harmonisiert werden. In manchen Staaten wurden dadurch bestimmte Regeln zum ersten Mal eingeführt, in anderen Staaten werden bereits existierende Rechte gestärkt oder erweitert, die auch bisher schon durch lokale Vorschriften gewährleistet wurden.

Die DSGVO betrifft 22 Millionen Unternehmen und 510 Millionen EU-Bürger in 28 Staaten. Hinzu kommen die Schweiz und die EWR-Staaten Island, Liechtenstein und Norwegen, sobald die in der DSGVO enthaltenen Vorschriften durch Beschluss des Gemeinsamen EWR-Ausschusses in das EWR-Abkommen aufgenommen werden.

Die Außenwirkung der DSGVO ist noch größer, weil die neue Verordnung unter bestimmten erweiterten Bedingungen auch über diese Grenzen hinaus gilt. Also selbst wenn Ihre Organisation keine physische Marktpräsenz in der EU hat, müssen Sie DSGVO-konform organisiert sein, wenn Folgendes gegeben ist:

- Sie verarbeiten personenbezogene Daten von EU-Bürgern oder überwachen deren Verhalten.
- Sie vermarkten in der EU bezahlte oder unbezahlte Waren oder Leistungen an EU-Bürger.
- Sie verarbeiten in der EU personenbezogene Daten von Nicht-EU-Bürgern.

Wenn Ihre Geschäftspartner in der EU geschäftlich tätig sind, werden sie höchstwahrscheinlich von Ihnen erwarten, dass Sie die DSGVO einhalten, um ihr eigenes Risiko entsprechend zu reduzieren. Die DSGVO hat sich damit als ein grundsätzliches Gesetzeswerk entpuppt, dessen Regeln eingehalten werden muss, wer Geschäfte in Europa erfolgreich tätigen will.

2. Welcher Schaden kann entstehen, wenn Sie Ihre Organisation nicht fit für die DSGVO machen?

Das wirtschaftliche Risiko für die Nichtkonformität mit der DSGVO ist klar definiert: Pro Fall einer fehlenden Einhaltung können Organisationen Bußgelder von bis zu 20 Millionen Euro oder von vier Prozent ihres weltweiten Jahresumsatzes auferlegt werden, wobei der jeweils höhere Wert gilt. Hinzu kommen der hohe Imageschaden und der große Vertrauensverlust, die der betreffenden Organisation in einem solchen Fall widerfahren. Dies kann sogar so weit gehen, dass Marktanteile an Mitwerber verloren gehen.

Die DSGVO wird seit dem 25. Mai 2018 durchgesetzt. Nach dem heutigen Stand ist eine längere Schonfrist, in der Organisationen nicht mit einem Bußgeld belegt werden, nicht zu erwarten. Die Verhängung einer Rekordstrafe der französischen Datenschutzbehörde Commission Nationale de l'Informatique et des Libertés (CNIL) in Höhe von 50 Millionen Euro gegen Google bestätigt, dass Organisationen, die nicht DSGVO-konform agieren, das Risiko eines wirtschaftlichen Schadens durch Verhängung eines Bußgelds eingehen. In Deutschland waren mit dem Bundesdatenschutzgesetz bereits vor Inkrafttreten der DSGVO verhältnismäßig restriktive gesetzliche Vorschriften gegeben. Daher trifft die DSGVO allein in Deutschland operierende Organisationen i. d. R. nicht so hart und die bereits getroffenen Vorkehrungen der Unternehmen können mit in Betracht gezogen werden.

Aufsichtsbehörden können den Betrieb Ihrer Organisation sogar unterbrechen, wenn sie den Verdacht äußern, dass Ihr Unternehmen nicht DSGVO-konform agiert. Eine nähere Untersuchung kann dann sogar ergeben, dass Sie noch weiter von der Konformität entfernt sind, als die Aufsichtsbehörde und Sie selbst dachten. Konformität wird also durch verschiedene Vorteile belohnt und Nichtkonformität ggf. durch hohe Schäden bestraft.

Einige Experten und Kunden führen die Konformität mit der DSGVO als einen errungenen Wettbewerbsvorteil an oder sehen darin einen hohen geschäftlichen Wert, so dass sie Datenschutz und Datensicherheit in das Design ihrer IT-Produkte, Systeme und Services aufnehmen, z. B. in der Bankbranche. Durch proaktive Design- und Implementierungsmaßnahmen können solche Organisationen ihr Image verbessern und auch Vertrauen und Kunden mit diesem Verkaufsargument gewinnen.

Eine weitere Chance besteht in der Einführung einer organisationsweiten, kunden- bzw. bürgerorientierten Datenstrategie, die sich allein schon wegen der Einhaltung der DSGVO, aber auch wegen des Personenbezugs der Daten und der Synergieeffekte einer homogenen Datenarchitektur mittel- bis langfristig auszahlt. Ein proaktives Konzept zur DSGVO-Konformität kann daher der erste

Schritt sein, mehr geschäftlichen Wert aus Ihren Daten herauszuholen, indem Sie die Daten und Ihre Verantwortlichkeiten im Hinblick auf Ihre IT-Systeme kennen, die personenzentrischen Daten effektiv steuern, sie schützen, ohne ihren Wert zu beschränken, sie professionellen Anwendern zur Verfügung stellen und sie intelligenter anwenden.

3. Welchen Nutzen hat die DSGVO-Konformität?

Die DSGVO ist strenger als die bestehenden Datenschutzgesetze in den einzelnen EU-Mitgliedstaaten und z. B. auch strenger als die Datenschutzregelungen in den USA. Viele Organisationen in Nordamerika konnten personenbezogene Daten bisher als frei verfügbare Marktressource beliebig nutzen. Nun erkennen diese Organisationen wegen der DSGVO, wie wichtig es ist, den Schutz und die Sicherheit der personenbezogenen Daten als zusätzlichen geschäftlichen Wert anzusehen. Zudem wird ihnen bewusst, dass die gesetzlichen Vorgaben eine Data-Governance vorsehen, d. h. ein Management der Benutzerfreundlichkeit, Verfügbarkeit, Authentizität, Vertraulichkeit, Integrität und Sicherheit der Daten.

In einer Datenstrategie müssen daher Schutz, Sicherheit und Governance der Daten berücksichtigt werden. Im Hinblick auf die umzusetzenden technischen und organisatorischen Maßnahmen, welche die DSGVO einfordert, wird damit schnell klar, dass eine Strategie zur Konformität mit der DSGVO sowohl Personen, Prozesse als auch Technologien umfassen sollte. Da die Organisationen bereits Prozesse implementiert haben, können sie auf dieser Grundlage etwaige Datenschutz- und Sicherheitslücken identifizieren und bearbeiten.

Ein wichtiges Ziel besteht also in der Entwicklung einer durchgängigen, vereinheitlichten Daten- und Governance-Strategie. Wenn Sie eine solche Strategie entsprechend umsetzen, können Sie die DSGVO einhalten und eine bessere Ausgangslage für die Einhaltung zukünftiger oder anderer internationaler Datenschutzverordnungen erreichen.

4. Fünf Konzepte für die Herstellung der DSGVO-Konformität

Aus unserer Sicht sollten Sie fünf Konzepte kennen, wenn es um DSGVO-Vorschriften und Ihre damit verbundenen Pflichten geht:

1. Rechte betroffener EU-Bürger
2. Einwilligung
3. Schutz und Sicherheit personenbezogener Daten
4. Meldepflicht und Rechenschaftspflicht zur Konformität
5. Technik und eingebauter Datenschutz

Abbildung 1: CGI-Strukturmodell zur DSGVO

RECHTE BETROFFENER EU-BÜRGER

Rechte, die im Rahmen der DSGVO für alle EU-Bürger gelten, beinhalten Rechte auf Information, Zugriff, Änderung, Löschung, Widerspruch, Begrenzung der Verarbeitung und Portabilität, was die Daten anbelangt. Vor allem muss Ihre Organisation die Kunden über ihre Rechte hinsichtlich der personenbezogenen Daten unterrichten und bei Geltendmachung dieser Rechte in einem teilweise strikten Zeitrahmen reagieren.

Ein bedeutsamer Schritt, um entsprechenden Wünschen gerecht zu werden, ist die **Sicherstellung der Datenqualität**. Wenn Sie Daten, die ihren Zweck nicht mehr erfüllen, schnell erkennen und löschen, können Sie sowohl Kosten und Risiken reduzieren als auch für DSGVO-Konformität sorgen. Dabei sind die im

Regelwerk geforderten Grundsätze für die Verarbeitung personenbezogener Daten – z. B. Transparenz, Datenminimierung, Speicherbegrenzung, Richtigkeit, Integrität und Vertraulichkeit – zu beachten. Andererseits sollten die Daten so verfügbar und portabel sein, dass Sie sie schnell dem Kunden zustellen können.

EINWILLIGUNG

Wegen der Sensibilisierung betroffener Personen für das Datenschutzthema wird es vor dem Hintergrund der DSGVO für Ihre Organisation mit an Sicherheit grenzender Wahrscheinlichkeit zur Herausforderung, die Einwilligung einer betroffenen Person zur Verarbeitung ihrer personenbezogenen Daten zu erhalten. Denn damit die Einwilligung als gültig betrachtet werden kann, muss die Bekundung dieser Entscheidung der betroffenen Person freiwillig, für den konkreten Fall und unmissverständlich erfolgen.

Eine einmal geäußerte Einwilligung ist aber nicht in Stein gemeißelt und kann vom Betroffenen mit Wirkung für die Zukunft jederzeit widerrufen werden. Eine Einwilligung ist überhaupt nur dann verwendbar, wenn sie angemessen ist und keine anderen rechtmäßigen Gründe zur Verarbeitung der personenbezogenen Daten vorliegen, z. B. das berechtigte Interesse oder die Notwendigkeit des Informierens eines verantwortlichen Dritten.

Eine Einwilligung bezieht sich konkret und im Einzelnen auf den Zweck der Erhebung, Verarbeitung und Verwendung der personenbezogenen Daten. Damit Ihre Organisation diese Aufgabe aber stemmen kann, bedarf es eines **zentralen Managements der Einwilligungen**. Aus unserer Sicht kann diese Aufgabe nur durch eine einzige, aktuelle, konsolidierte und organisationsweit verbindliche Informationsbasis zu den Einwilligungen sowie eine entsprechende Überwachung des Workflows wirksam und effizient unterstützt werden. Dabei sind alle Kommunikationskanäle, in denen von den betroffenen Personen Einwilligungen bekundet werden, einzubeziehen und mit der zentralen Informationsbasis zu koppeln.

Die Konsultation eines Datenschutzbeauftragten, der zu Aspekten der Rechtmäßigkeit der Verarbeitung personenbezogener Daten berät, kann dabei hilfreich sein, da es zu erkennen gilt, wer bestimmte personenbezogene Daten erhalten darf, ohne dass eine Einwilligung erforderlich ist. Diese Daten müssen den betreffenden Verantwortlichen schließlich auch zugeordnet werden.

SCHUTZ UND SICHERHEIT PERSONENBEZOGENER DATEN

Ihr Schutz- und Sicherheitsbedarf im Hinblick auf die Gefährdungspotenziale, denen die personenbezogenen Daten, aber auch andere Daten in Ihrer Organisation ausgesetzt sind, muss durch vorbeugende und korrektive **Risikomanagementmaßnahmen** gedeckt werden.

Vorbeugende Maßnahmen zielen auf die Vermeidung von Risiken ab, sorgen also dafür, dass Datenschutzverletzungen vermieden werden. In der DSGVO explizit genannte Maßnahmen sind die Verschlüsselung zur Herstellung der Abhörsicherheit der Daten, die Pseudonymisierung zur Vermeidung der Identifizierbarkeit der Personen (und entsprechender Zuordenbarkeit der Personen zu ihren personenbezogenen Daten) sowie die Minimierung der Verarbeitung personenbezogener Daten zur Reduzierung der Gefährdungspotenziale. Data-Governance-Tools können zur Vermeidung von Datenschutzverletzungen eingesetzt werden, indem sie zu löschende Daten identifizieren, die Ihrer Einstufung nach keinen geschäftlichen Wert mehr haben.

Angesichts der zeitlichen Dringlichkeit zur Abhilfe bei bereits eingetretenen Schäden ist es sinnvoll, über korrektive Maßnahmen nachzudenken. Hier sehen wir vor allem den Einsatz von Datensicherheitstools als Mittel der Wahl an, mit denen sich sicherheitsrelevante Störfälle schnell erkennen und beheben und somit auftretende Schäden entsprechend schnell begrenzen lassen.

MELDEPFLICHT UND RECHENSCHAFTSPFLICHT ZUR KONFORMITÄT

Eine Anforderung, die ebenfalls eher den korrektiven Risikomanagement-maßnahmen zuzurechnen ist, besteht in der Meldung von Datenschutz-verletzungen innerhalb von 72 Stunden an die Aufsichtsbehörde. Mit einem geeigneten **Melde- und Berichtswesen** können Sie die Folgeschäden, etwa Imageschäden, auf das Kleinste eindämmen.

Ebenfalls sollte Ihre Organisation angesichts der in der DSGVO definierten Rechenschaftspflicht fähig sein, die hergestellte Konformität bzw. die Verbesserungen hierzu zu dokumentieren und nachzuweisen. Dieses Ziel erreichen Sie am wirksamsten durch Aufzeichnung, Bewertung der Auswirkung von Verletzungen des Datenschutzes, proaktive Verhaltensregeln und Zertifizierung. Auch die Dokumentation und der Nachweis der Konformität können mit den schon erwähnten Melde- und Reporting-Tools bewerkstelligt werden.

Durch die Erstellung von Verzeichnissen der Verarbeitungstätigkeiten kann Ihre Organisation personenbezogene Daten zuordnen und ihrer Rechenschaftspflicht nachkommen. Diese Verzeichnisse sollten möglichst proaktiv unter Nutzung einer zentralen **Datenbank** verwaltet werden, damit statische Spreadsheets vermieden werden können, die schnell veralten und eher einen isolierten Einblick in die Verarbeitungsaktivitäten erlauben.

TECHNIK UND EINGEBAUTER DATENSCHUTZ

Zur Herstellung eines in die IT-Systeme von vornherein **eingebauten Datenschutzes** („Data Protection by Design“ und „Data Protection by Default“), z. B. des Einbaus von Prüfalgorithmen für Löschfristen, müssen die für die Verarbeitung personenbezogener Daten Verantwortlichen organisatorische

und technische Maßnahmen implementieren, mit denen DSGVO-Konformität letztlich hergestellt und nachgewiesen werden kann. Um die Rechte der Betroffenen zu schützen und die DSGVO einzuhalten, müssen dabei vor allem die Grundsätze der Datenminimierung und der Speicherbegrenzung beachtet werden. Der Schwerpunkt liegt dabei auf einem Rechtemanagement nach dem „Need-to-know“-Prinzip, d. h. einer Zugriffsbegrenzung für unberechtigte oder nur teilweise berechtigte Personen im gesamten Lebenszyklus der Daten, also von der Erfassung bis zur Löschung.

Das Prinzip dieses Konzepts basiert auf der Erkennung derjenigen personenbezogenen Daten, die verarbeitet werden sollen. Bei unstrukturierten personenbezogenen Daten sollten Organisationen Richtlinien und Standards in Bezug auf die Zuordnung, Verwaltung und Sicherheit erstellen, publizieren und verbindlich machen, um so die Datenqualität zu verbessern und die Risiken abzusenken. Falls die Daten strukturiert sind, sollten Organisationen außer Richtlinien und Standards auch ein Management der Metadaten einführen, damit personenbezogene Daten bei Bedarf schnell gefunden und gelöscht werden können.

5. Leitfaden zur Herstellung der DSGVO-Konformität

Die meisten Organisationen erkennen angesichts der DSGVO intuitiv ihren Handlungsbedarf, wissen jedoch nicht, wie sie am besten mit der Umsetzung beginnen sollen. Dabei hängt dies von ihrer individuellen Situation ab. CGI hat diverse Kundenprojekte untersucht und mehrere allgemeine Lösungen identifiziert, die für die meisten Organisationen angesichts der einheitlichen Anforderungen zur Konformität mit der DSGVO von besonderer Wichtigkeit waren, sowie weitere Lösungen, die Organisationen möglicherweise in Zukunft nutzen möchten.

AUFSETZEN EINER LÖSUNG

Wenn Sie es bisher nicht getan haben, sollten Sie zuerst das Datenschutzniveau in Ihrer Organisation sowie die in Kauf genommenen Risiken in Bezug auf die DSGVO identifizieren, denen Ihre Organisation weiterhin ausgesetzt wäre, falls Sie jetzt nicht handeln würden. Dies beinhaltet idealerweise die Erstellung einer organisationsweiten groben Datenlandkarte in Zusammenarbeit mit den verschiedenen Geschäftsbereichen, in der die personenbezogenen Daten und idealerweise Ihre Verantwortlichkeiten verortet werden. Diese Datenlandkarte kann sukzessive erweitert werden.

Besonders wichtig bei der Planung sollte es sein, identifizierten Gefährdungspotenzialen und ihren Auswirkungen möglichst entgegenzuwirken. Dabei sollten bereits initiierte Vorhaben der Organisation und spezifische Lücken bezüglich der DSGVO identifiziert werden. Sobald Sie Ihre nächsten Schritte auf dem Weg zur Konformität priorisiert haben, können Sie Projektverantwortliche zuordnen, die bei dieser Herausforderung zukünftig die Führung übernehmen.

IDENTIFIKATION PERSONENBEZOGENER DATEN

Während oder nachdem Sie die Konformität mit der DSGVO prüfen bzw. geprüft haben, können Sie Ihr Wissen über die Quellen und Inhalte der personenbezogenen Daten weiter vertiefen und erweitern.

Die meisten Organisationen wissen ziemlich genau, wo ihre strukturierten Daten zu verorten sind und wie deren Inhalt aussieht. Bei unstrukturierten Daten ist das jedoch oft nicht so. Denn Datenquellen wie alte Dateifreigaben, gemeinsam genutzte Laufwerke, Archive, SharePoints, Dokumentenmanagementsysteme und andere Content-Repositorys vergisst man leicht und daher enthalten sie oft personenbezogene Daten, für die kein ordnungsgemäßer Nachweis möglich ist.

Selbst wenn Sie wissen, dass Sie über diese personenbezogenen Daten verfügen, die geschützt werden müssen, wissen Sie möglicherweise nicht

genug über deren Umfang, die zugehörigen Personen oder Ähnliches. Im Zusammenhang mit der DSGVO-Konformität haben wir ermittelt, dass es extrem wichtig ist, alte Daten zu löschen und gleichzeitig Daten, die aufbewahrt werden müssen, in ein leistungsfähiges Programm für Data-Governance und Datensicherheit zu übertragen, damit sie zukünftig bekannt und geschützt sind und einbezogen werden können.

CGI bietet seinen Mandanten die notwendige Marktexpertise, eine schnelle und effektive Lösung zur Konformität mit der DSGVO zu finden, die sowohl strukturierte als auch unstrukturierte Datenquellen abdeckt. Dabei profitiert CGI vom eigenen langjährigen technologischen, herstellerübergreifenden Anwendungswissen über State-of-the-Art-Werkzeuge zur Analyse und Governance unstrukturierter und strukturierter Informationen, Daten und großer Datenmengen (Big Data). Ziel ist die Erstellung eines klar formulierten Plans, um Ihnen dabei zu helfen, Ihre Arbeiten in Bezug auf die Konformität mit der DSGVO innerhalb von wenigen Wochen nach der Analyse voranzutreiben.

Im Rahmen des Projekts zur Konformität mit der DSGVO wird Ihre Organisation sicherlich mit Routinen konfrontiert, die als wiederholbare, standardisierte Prozesse genutzt werden, um personenbezogene Daten in Ihren Datenlandschaften zu identifizieren. Zudem arbeitet CGI mit Ihnen zusammen, um die Menge personenbezogener Daten in Ihren Datenspeichern zu minimieren, so dass Daten identifiziert werden können, die Sie nicht mehr aufbewahren müssen. Durch diese Datenminimierung können Sie Ihre Risiken im Hinblick auf die DSGVO reduzieren.

DATENBESTAND

Wenn Sie auf der festen Grundlage aufbauen, die Sie sich bei der Bewertung der Konformität mit der DSGVO erarbeitet haben, wird alles, was Sie über Ihre personenbezogenen Daten gelernt haben, inklusive der Datenquellen und deren physischer Position, im Datenbestand konsolidiert. Unserer Meinung nach sollte dies im Rahmen der Anforderungen für Verzeichnisse von Verarbeitungstätigkeiten gemäß Artikel 30 DSGVO durchgeführt werden.

Die beste Möglichkeit, einen umfassenden und aktuellen Datenbestand zu erstellen, ist unseres Erachtens die Kombination eines Top-down-Ansatzes, nach dem Interviews mit den Fach- und Technikbereichsmitarbeitern durchgeführt werden, mit einem Bottom-up-Ansatz unter Verwendung von Datenbestandstools. Beim Top-down-Ansatz werden Gespräche durchgeführt, um zu erfahren, welche Daten sich wo befinden und welchen geschäftlichen Nutzen Benutzer aus diesen Daten ziehen.

Tools zur Datenanalyse und Data-Governance helfen Ihnen dabei, den Prozess der Datenzuordnung für strukturierte Daten zu beschleunigen und zu erweitern. Durch schnelle Analyse und Klassifizierung der Inhalte Ihrer Datenspeicher mit diesen Tools und im Rahmen der durchgeführten Aktivitäten für die

Top-down-Zuordnung können Sie einen granularen Katalog über Speicherort, Speicherzweck, Eigentümer und Arten von betroffenen Personen etc. erstellen. Sie können all dies erreichen, während Sie gleichzeitig den manuellen Aufwand hierfür reduzieren.

Ein exakter und vollständiger Datenbestand kann die Basis für eine konsequente Strategie für die Data-Governance sein. Daher ist der Nutzen nicht auf die Konformität mit der DSGVO begrenzt; denn die Strategie kann Sie zudem bei der Einhaltung anderer oder zukünftiger Vorschriften unterstützen. Außerdem ist ein vollständiger und präziser Datenbestand die Grundlage für bessere Geschäftsergebnisse, indem die gesamte Organisation mit geschäftskritischen Daten versorgt wird.

VERSCHLÜSSELUNG UND ANONYMISIERUNG

Empfehlungen von CGI, die Sie bei der Erzielung der Konformität mit der DSGVO unterstützen können, umfassen u. a. Datenmanagementlösungen zur Verschlüsselung und Anonymisierung. Zusammen stellen diese Tools sicher, dass Daten vertraulich, integer und authentisch sind sowie jederzeit und überall verfügbar bleiben.

Mit Lösungen zur Anonymisierung kann Ihre Organisation die in der DSGVO angesprochene Datenminimierung vorantreiben. Informationen werden hierzu möglichst maskiert und es werden nur die Daten beibehalten, die für Verarbeitungstätigkeiten wie Analysen und Tests verwendet werden. Durch die Anwendung unterschiedlicher Anonymisierungsverfahren können entsprechende Datenmanagementlösungen dazu beitragen, Daten wie Krankheitsbefunde, Rentenversicherungsnummern, Kreditkartennummern, Kredit-Scores, Adressen oder ähnlich vertrauliche Informationen zu schützen, ohne dass ihre Bedeutung im Kontext verloren geht. Eine anonymisierte Rentenversicherungsnummer z. B. sieht weiterhin wie eine Rentenversicherungsnummer aus und funktioniert in Workloads für Tests, auch ohne dass sie selbst offengelegt wird.

Datenverschlüsselungsfunktionen, kombiniert mit Funktionen für die Speicher- und Hardwareverschlüsselung, wiederum bewirken, dass nur berechtigte Personen auf sensible personenbezogene Daten zugreifen können. Um den Anforderungen der DSGVO gerecht zu werden, deckt diese kombinierte Verschlüsselung den gesamten Datenlebenszyklus ab – von dem Zeitpunkt, an dem die Daten zum ersten Mal die Organisation erreichen, bis zu dem Zeitpunkt, an dem sie entweder gelöscht oder anonymisiert werden.

Organisationen können ebenso Content-Management-Lösungen nutzen, um unstrukturierte Inhalte basierend auf Benutzerrollen zu verwalten und für die Veröffentlichung zu bearbeiten. Dabei werden den Benutzern nur diejenigen Daten angezeigt, die sie gemäß der DSVGO wirklich sehen müssen, um ihre Arbeit effektiv erledigen zu können.

6. Der CGI-Rahmen zur DSGVO

CGI hat einen Rahmen zur DSGVO erstellt, der fünf Phasen enthält, um die Konformität mit dieser Verordnung zu erreichen, wie in der Abbildung unten dargestellt ist: Evaluation, Standardisierung, Implementierung, Betrieb und Konformität.

Ziel des Rahmens ist es, Kunden dabei zu helfen, ein effektives Management des Datenschutzes und der Datensicherheit aus Risikoperspektive zu betreiben, damit sie ihr Risiko und ihre Störfälle von vornherein reduzieren können.

Abbildung 1: CGI-Rahmen zur DSGVO

7. Ausblick auf künftige Lösungen für den Datenschutz

Die oben genannten Lösungen erscheinen als dringlichste und wichtigste Ansatzpunkte für die meisten Organisationen, die Konformität mit der DSGVO erzielen wollen. Sie können jedoch, nachdem die ersten Schritte eingeleitet sind, auch in anderen Bereichen weiteren geschäftlichen Wert generieren:

Management der Änderungen: Schaffen Sie – ergänzend zu den in diesem Dokument beschriebenen organisatorischen und technischen Änderungsmaß-nahmen – eine offene Unternehmenskultur.

Schutz der Wettbewerbsvorteile: Erkennen und klassifizieren Sie die kritischen Daten-Assets („die Diamanten“) Ihrer Organisation bezüglich der DSGVO. Auf diese Weise können Sie Ihre Wettbewerbsvorteile bewahren und hieraus weiterhin geschäftlichen Wert generieren.

Privacy bzw. Security by Design: Bauen Sie Datenschutz und Datensicherheit von vornherein in alle Funktionen Ihrer Anwendungssysteme zur Verarbeitung personenbezogener Daten ein.

Design einer Kundenrundumsicht: Implementieren Sie eine 360-Grad-Sicht auf Ihre Kunden und managen Sie die Daten, die Sie für sie speichern, und die genauen Speicherorte.

Implementierung eines Einwilligungsmanagements: Qualifizieren und spezifizieren Sie für jede Nutzung und jeden Kunden die speziellen Anforderungen zur Einwilligung in die Nutzung.

Management der Zugriffsrechte: Bieten Sie den Betroffenen eine einfache und effektive Möglichkeit, ihre Rechte auf Anlage, Lesen, Änderung, Löschung und Herausgabe der Daten auszuüben.

Vorfallsmanagement: Stellen Sie ein effizientes Vorfallsmanagement zur Verfügung.

Datenlöschung: Löschen Sie Daten in allen Systemen, sobald die gesetzliche Löschfrist eingetreten ist und/oder sie keiner geschäftlichen Verwendung mehr dienen.

8. Verpflichtungen aus der DSGVO

Dieses Dokument soll zeigen, dass die Konformität mit der Datenschutz-Grundverordnung eine komplexe unternehmensweite Gesamtaufgabe ist, mit der Organisationen hohe Geldbußen und Folgekosten vermeiden können.

Wir sind darüber hinaus der Meinung, dass die Befolgung der DSGVO das Potenzial für erheblichen geschäftlichen Wert bietet, da die Daten-Assets, aus denen Sie diesen geschäftlichen Wert und weitere Wettbewerbsvorteile generieren, auf diese Weise gehoben werden können bzw. zukünftig noch sicherer sind. Für den Fall, dass Sie von den angesprochenen Daten-Assets noch nicht profitieren, bietet die Einhaltung der DSGVO erhebliche weitere Potenziale.

Zudem bietet Ihnen dieser Schritt eine sichere „digitale“ Präsenz auf einem harmonisierten digitalen Markt für ganz Europa. Organisationen, die dies erkennen, sind gut für diesen neuen europäischen Markt gewappnet.

Die Konformität mit der DSGVO ist eine einzigartige Herausforderung, das Vertrauen Ihrer Kunden und Mitarbeiter zu bestätigen, Ihre Organisation transparenter zu gestalten, jedem Mitarbeiter Ihrer Organisation qualitativ hochwertige Daten bereitzustellen, neue Geschäftschancen zu identifizieren und Ihre Geschäftsprozesse effizienter durchzuführen.

Handeln Sie jetzt!

Da Sie die Dringlichkeit der Konformität mit der DSGVO nun kennen, stehen Ihnen die Experten, Prozesse und Technologien von CGI zur Verfügung, um Ihnen bei der Implementierung zu helfen. Unabhängig davon, ob Sie bei der Toolauswahl objektiv beraten werden möchten, ob Sie eine spezielle Expertise suchen oder ob Sie bereit sind, ein umfassendes Einführungskonzept für weiteren geschäftlichen Wert zu implementieren – wir bieten Ihnen das entsprechende Know-how und die nötige Unterstützung.

KONTAKT UND WEITERE INFORMATION

Wenn Sie mehr über die Projekte von CGI zur Konformität mit der DSGVO erfahren möchten, kontaktieren Sie Ihren CGI-Ansprechpartner.

“… the new GDPR legislation will make the value of data impossible to overlook.”

Phil Beckett, Managing Director, Alvarez and Marsal

[1] Europäische Union (Hrsg.): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

[2] CGI (Hrsg.): DSGVO – Datenschutz und Cybersecurity wachsen zusammen. Factsheet. O. O., 2017.

[3] CGI (Hrsg.): PSD2 vs. GDPR: Navigating the differences. White Paper. O. O., 2018.

[4] Ebenda.

de.cgi.com

CGI ist ein globaler Dienstleister für IT- und Geschäftsprozesse mit 77.000 Mitarbeitern, der seit der Gründung im Jahr 1976 seinen Kunden IT und Business Consulting, Systemintegration, Outsourcing Services und Intellectual Property auf Top-Niveau bietet.