IBM
Whitepaper

Fahrplan für die Einhaltung der Datenschutz-Grundverordnung

So bereiten Sie Ihr Unternehmen auf die neuen Datenschutzanforderungen in der Europäischen Union vor

IBM

Inhalt

Einführung

Wenn Ihr Unternehmen in der Europäischen Union geschäftlich tätig ist, wissen Sie wahrscheinlich, dass die Situation ab Mai 2018 erheblich komplizierter werden wird. Zu diesem Zeitpunkt tritt nämlich die neue Datenschutz-Grundverordnung für die EU in Kraft.

Mit diesen neuen, strikteren Vorschriften sollen die Datenschutzregeln in allen 28 EU-Mitgliedsstaaten möglichst harmonisiert werden. In einigen Fällen werden dadurch bestimmte Rechte, die bereits unter vielen lokalen Vorschriften sichergestellt sind, gestärkt oder erweitert, während in anderen Fällen bestimmte Rechte erstmals eingeführt werden.

Die EU hat über 500 Millionen Bürger und 20 Millionen aktive Unternehmen, von denen alle direkt der Datenschutz-Grundverordnung unterliegen. Darüber hinaus werden viele der Vorschriften integriert, damit sie für die Bürger mehrerer Nicht-EU-Mitgliedsstaaten (einschließlich Schweiz, Norwegen, Island und Liechtenstein) gelten, da diese Länder eine Standardisierung der Vorschriften in Bezug auf die in der Datenschutz-Grundverordnung enthaltenen Regeln vornehmen werden, sobald sie in das EWR-Abkommen von 1992 aufgenommen werden. (Es handelt sich derzeit um ein verabschiedetes Gesetz, das von EWR/EFTA geprüft wird.)

Was das Ganze noch komplizierter macht, ist die Tatsache, dass die neuen Verordnungen unter bestimmten erweiterten Bedingungen als ausdrücklich extraterritorial gelten. Das heißt, selbst wenn Ihr Unternehmen in der EU über keine physische Marktpräsenz verfügt, müssen Sie trotzdem die Datenschutz-Grundverordnung einhalten, sofern die folgenden Bedingungen gelten:

- Sie bieten betroffenen Personen in der EU bezahlte oder unbezahlte Waren oder Leistungen an
- Sie bearbeiten oder verarbeiten die personenbezogenen Daten betroffener Personen in der EU oder überwachen deren Verhalten

Wenn Sie darüber hinaus mit Partnern zusammenarbeiten, die in der EU geschäftlich tätig sind, werden diese höchstwahrscheinlich von Ihnen erwarten, dass Sie die Datenschutz-Grundverordnung einhalten, um ihr eigenes Risiko zu begrenzen. Die Datenschutz-Grundverordnung wird also schon bald eine Grundvoraussetzung für alle Unternehmen sein, die in Europa erfolgreich Geschäfte machen möchten.

Welche Nachteile können entstehen, wenn die Datenschutz-Grundverordnung nicht eingehalten wird?

Das finanzielle Strafmaß für die Nichteinhaltung der Datenschutz-Grundverordnung ist klar definiert: Für jede Nichteinhaltung können Unternehmen mit Geldbußen von bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes belegt werden, wobei der jeweils höhere Wert ausschlaggebend ist. Selbstverständlich berücksichtigt dies noch nicht den schweren Schaden, den ein solches Bußgeld – oder genauer gesagt, die Aktionen, die zu dem Bußgeld geführt haben – in Bezug auf Ihren Ruf bei Ihren Kunden und Mitarbeitern anrichten kann.

Dies könnte sogar soweit führen, dass Sie den europäischen Marktanteil an Mitbewerber verlieren, die sich besser vorbereitet haben. Einige IBM Kunden stellen die Einhaltung der Datenschutz-Grundverordnung bereits als Wettbewerbsvorteil heraus. Durch die proaktive Implementierung von Maßnahmen in den Bereichen Datenschutz und -sicherheit können diese Unternehmen ihren Ruf verbessern und verfügen zudem über ein wertvolles Verkaufsargument, um neue Kunden zu gewinnen.

Alles weist darauf hin, dass die Datenschutz-Grundverordnung ab dem ersten Tag strikt durchgesetzt werden wird. Unternehmen sollten nicht davon ausgehen, dass es eine Schonfrist geben wird, in der keine Bußgelder verhängt werden. Tatsächlich hat das Information Commissioner's Office (ICO) in Großbritannien bestätigt, dass Unternehmen, die die Datenschutz-Grundverordnung nicht einhalten, Gefahr laufen, direkt mit einem Bußgeld belegt zu werden.[1] Es verlautete jedoch auch, dass man in Bezug auf gesetzliche Vorgaben einen vernünftigen, pragmatischen Ansatz verfolge und die bereits getroffenen Vorbereitungen der Unternehmen mit in Betracht gezogen werden.

Darüber hinaus können Aufsichtsbehörden das laufende Geschäft unterbrechen, wenn sie den Verdacht haben, dass Ihr Unternehmen gegen die Datenschutz-Grundverordnung verstößt. Eine solche Untersuchung kann zu Ergebnissen führen, die zeigen, dass Sie noch erheblich weiter von einer Einhaltung der Datenschutz-Grundverordnung entfernt sind als die Aufsichtsbehörde – oder selbst Sie – ursprünglich dachten.

Angesichts dessen ist es wichtig, im Kopf zu behalten, dass die Datenschutz-Grundverordnung sowohl Zuckerbrot als auch Peitsche sein kann: Es gibt Vorteile bei Einhaltung der Datenschutz-Grundverordnung und Risiken bei Nichteinhaltung. Die Implementierung der Datenschutz-Grundverordnung könnte der Auslöser sein, der Ihr Unternehmen zu einer strikteren allgemeinen Datenstrategie führt, die sich auf Jahre hinaus auszahlen könnte.

Indem Sie die Daten in Ihren Systemen intelligenter nutzen – sie schützen, ohne sie zu beschränken, sie effektiv steuern, sie kennen und sie professionellen Anwendern bereitstellen – können Sie Möglichkeiten für Innovationen und neue Umsatzquellen identifizieren, die Sie ansonsten vielleicht übersehen hätten. Ein proaktives Konzept für die Einhaltung der Datenschutz-Grundverordnung könnte daher der erste Schritt sein, mehr Geld mit Ihren Daten zu verdienen.

Was bringt die Einhaltung der Datenschutz-Grundverordnung mit sich?

Die Datenschutz-Grundverordnung ist nicht nur strikter als die bestehenden Datenschutzverordnungen in den einzelnen EU-Mitgliedsstaaten, sondern auch erheblich strikter als man es in den USA gewohnt ist. Für viele US-Unternehmen waren Daten lange nur eine Marktressource. Durch die Datenschutz-Grundverordnung müssen sie damit beginnen, Datensicherheit und Datenschutz als etwas anzusehen, das weit darüber hinausgeht. Die Verordnung umfasst Datensicherheit, Datenschutz und Daten-Governance. Wir vertreten daher die Ansicht, dass jegliche Strategie für die Einhaltung der Datenschutz-Grundverordnung, die Sie einsetzen, alle drei Aspekte entsprechend berücksichtigen muss, um effektiv zu sein.

Angesichts der technischen und organisatorischen Maßnahmen in der Datenschutz-Grundverordnung wird deutlich, dass eine Strategie für die Einhaltung der Datenschutz-Grundverordnung Personen, Prozesse und Technologien umfassen sollte. Die meisten Unternehmen werden einige der bereits bestehenden Prozesse beibehalten können und auf diesen aufbauen, um mögliche Lücken zu füllen.

Als eines der Ziele sollte Ihr Unternehmen die Entwicklung einer durchgängigen, vereinheitlichten Governance-Strategie verfolgen. Wenn diese Strategie entsprechend umgesetzt wird, können Sie damit die Datenschutz-Grundverordnung einhalten und eine bessere Ausgangslage für die Einhaltung anderer Datenschutzverordnungen erlangen, die jetzt oder in Zukunft für Ihr Unternehmen gelten.

Fünf Hauptkonzepte für die Einhaltung der Datenschutz-Grundverordnung

Aus unserer Sicht gibt es fünf Hauptkonzepte, die Sie kennen sollten, wenn es um Ihre Verpflichtungen im Rahmen der Datenschutz-Grundverordnung geht (vgl. Abbildung 1):

1. Rechte betroffener Personen in der EU
2. Sicherheit personenbezogener Daten
3. Rechtmäßigkeit und Einwilligung
4. Rechenschaftspflicht für die Einhaltung
5. Technik und Voreinstellungen

Wichtige Pflichten, Verpflichtungen und Sanktionen

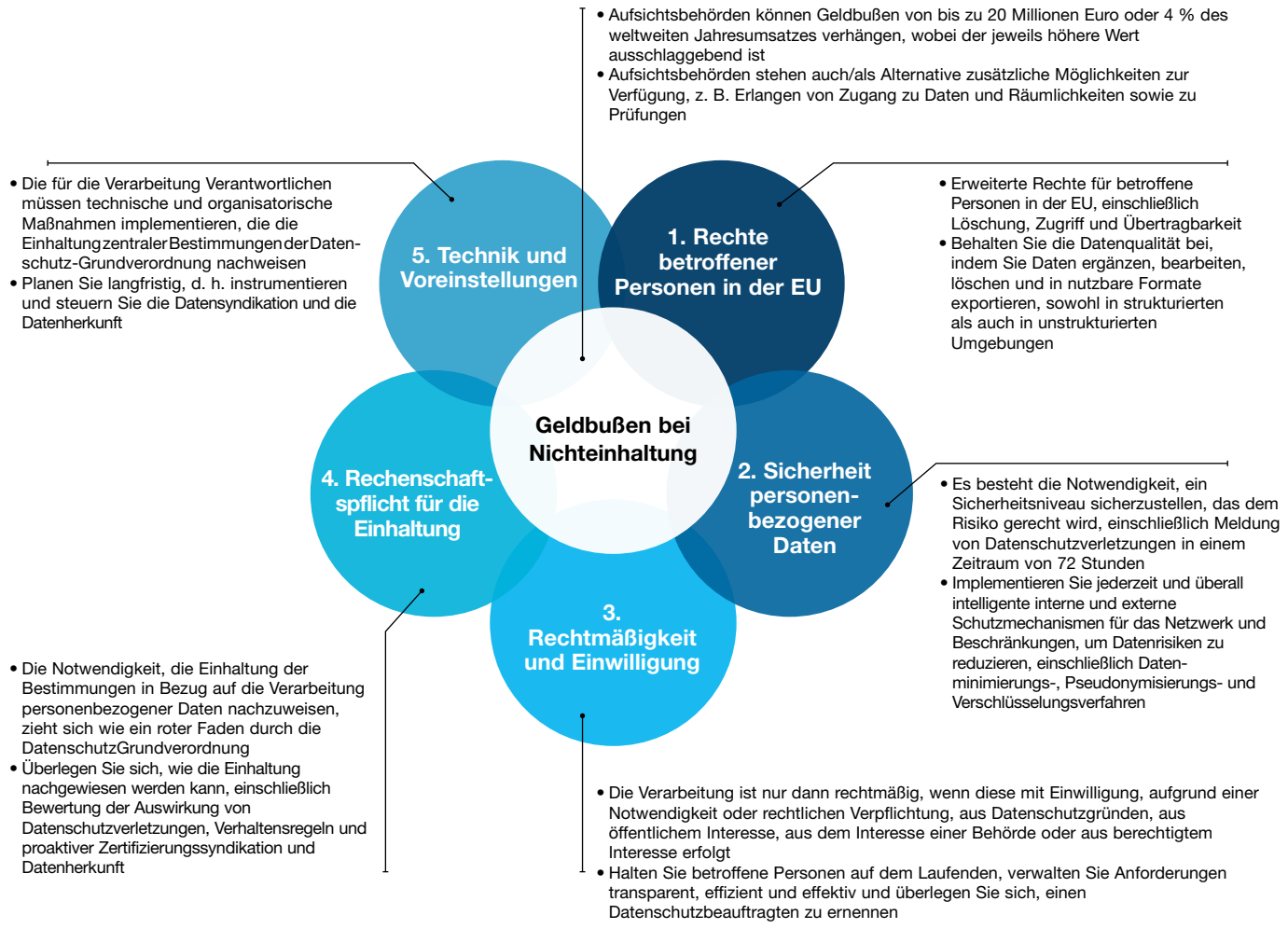

Abbildung 1: Aus IBM Sicht gibt es fünf Hauptkonzepte, die Sie kennen sollten, wenn es um Ihre Verpflichtungen im Rahmen der Datenschutz-Grundverordnung geht.

1. Rechte betroffener Personen in der EU

Rechte, die unter den entsprechenden Bedingungen für alle betroffenen Personen in der EU gelten, umfassen Rechte auf Information, Zugriff, Berichtigung, Löschung, Einschränkung der Verarbeitung, Übertragbarkeit und Widerspruch. Darüber hinaus muss es Ihr Unternehmen Kunden leicht machen, ihre Rechte in Bezug auf ihre personenbezogenen Daten kennenzulernen und bei der Geltendmachung von Rechten schnell alle Anforderungen zu erfüllen.

Ein wichtiger Schritt, um diesen Anforderungen gerecht zu werden, ist die Gewährleistung der Datenqualität. Wenn ROT-Daten (Redundant, Obsolete und Trivial) schnell identifiziert und gelöscht werden, können Sie damit nicht nur Kosten und Risiken reduzieren, sondern gleichzeitig die Einhaltung der Datenschutz-Grundverordnung unterstützen. Alle Daten, die danach noch übrig sind, sollten in nutzbarem Format verfügbar sein, sowohl in strukturierten als auch unstrukturierten Datenquellen. Dies hängt natürlich von Ihren Verpflichtungen gemäß den Grundsätzen der Datenschutz-Grundverordnung wie Datenminimierung und Speicherbegrenzung ab.

2. Sicherheit personenbezogener Daten

Ihr Unternehmen muss ein Sicherheitsniveau für Daten bieten, das den entsprechenden Risiken gerecht wird. Eine Anforderung der Datenschutz-Grundverordnung ist die Meldung von Datenschutzverletzungen innerhalb eines Zeitraums von 72 Stunden. Infolgedessen profitieren Sie von der Implementierung von Datensicherheitstools, die eine schnelle Reaktion unterstützen, wodurch Sie auch die Rufschädigung auf ein Minimum beschränken können.

Es ist zudem hilfreich, über vorbeugende Maßnahmen nachzudenken, die verhindern können, dass es überhaupt erst zu einer Datenschutzverletzung kommt. Verfahren, die Sie nutzen können, um dies zu erreichen, und die in der Datenschutz-Grundverordnung ausdrücklich genannt sind, umfassen unter anderem Minimierung, Pseudonymisierung und Verschlüsselung. Es können auch Verfahren der Informationsgovernance wie das Löschen von Informationen mit keinem rechtlichen, regulativen oder geschäftlichen Wert genutzt werden, um die Menge potenziell gefährdeter personenbezogener Daten zu reduzieren.

3. Rechtmäßigkeit und Einwilligung

Unter den Bedingungen der Datenschutz-Grundverordnung wird es für Ihr Unternehmen höchstwahrscheinlich künftig deutlich schwieriger werden, Einwilligungen zu bekommen als bisher. Damit eine Einwilligung als gültig betrachtet wird, muss sie freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet werden. Im Gesundheitswesen, wo häufig spezielle Kategorien von Daten verarbeitet werden, muss eine Einwilligung zudem ausdrücklich erfolgen. Die betroffene Person kann ihre Einwilligung jederzeit zurückziehen, was die Situation noch erschwert.

Unabhängig davon, wie Sie Einwilligungen von betroffenen Personen einholen, muss dies auf eine Art und Weise geschehen, die die anderen rechtmäßigen Gründe für die Verarbeitung personenbezogener Daten berücksichtigt. Es gibt eine Anweisung des ICO für Aufsichtsbehörden, dass eine Einwilligung nur dann verwendet werden sollte, wenn dies angemessen ist und keine anderen rechtmäßigen Gründe vorliegen.

Eine Einwilligung muss über den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der personenbezogenen Daten im Einzelnen informieren. Damit Ihr Unternehmen all diesen Aspekten gerecht wird, sollten Sie die Nutzung eines Managementsystems für Einwilligungen in Betracht ziehen und unterstützende Aktivitäten, die als Best Practices betrachtet werden könnten, durchführen, wie z. B. Workflow-überwachung und Einführung einer „Single Source of Truth“ (zentrale, konsolidierte Informationsbasis).

Neben den Einwilligungen gibt es weitere Aspekte der Rechtmäßigkeit, die es zu beachten gilt, einschließlich Notwendigkeit und berechtigtes Interesse. Daher ist es äußerst wichtig, dass Sie genau wissen, über welche Daten Sie verfügen und warum Sie darüber verfügen. Datenzuordnung und -erkennung sind wichtige Schritte, mit denen Ihr Unternehmen dieses Ziel erreichen kann. Es kann auch hilfreich sein, sich rechtlich beraten zu lassen und einen Datenschutzbeauftragten für das Unternehmen einzustellen, selbst wenn Sie streng genommen gar keinen benötigen.

4.Rechenschaftspflicht für die Einhaltung

Es reicht jedoch nicht aus, dass ein Unternehmen nur auf die Einhaltung der Datenschutz-Grundverordnung hinarbeitet. Das Unternehmen muss darüber hinaus in der Lage sein, die Einhaltung der Datenschutz-Grundverordnung nachzuweisen oder zu dokumentieren, welche Fortschritte dahingehend gemacht werden. Dieses Ziel erreichen Sie am besten durch das Führen von Aufzeichnungen, die Bewertung der Auswirkung von Datenschutzverletzungen, Verhaltensregeln und proaktive Zertifizierung.

Artikel 30 der Datenschutz-Grundverordnung behandelt Verzeichnisse von Verarbeitungstätigkeiten, die im Allgemeinen als Art der Datenzuordnung anerkannt werden, und kann Sie dabei unterstützen, die Rechenschaftspflicht des Unternehmens zu erfüllen. Diese Verzeichnisse sollten idealerweise proaktiv mit entsprechenden Tools verwaltet werden, um statische und isolierte Spreadsheets zu vermeiden, die tendenziell nur begrenzte Einblicke bieten und schnell veraltet sind.

5.Technik und Voreinstellungen

Für die Grundsätze des Datenschutzes durch Technik (data protection by design) und durch datenschutzfreundliche Voreinstellungen (data protection by default) müssen die für die Verarbeitung Verantwortlichen technische und organisatorische Maßnahmen implementieren, die die Einhaltung zentraler Bestimmungen der Datenschutz-Grundverordnung nachweisen.

Im Zusammenhang mit der Technik wird der Grundsatz der Datenminimierung ausdrücklich als Bestandteil der Integration notwendiger Sicherheitsmaßnahmen in die Verarbeitung genannt, um dazu beizutragen, die Rechte von betroffenen Personen zu schützen und die Datenschutz-Grundverordnung einzuhalten. Im Zusammenhang mit den Voreinstellungen sollten nur personenbezogene Daten verarbeitet werden, die für die speziellen Zwecke einer Verarbeitungstätigkeit notwendig sind. Im Rahmen der Verordnung werden diese Daten während des gesamten Lebenszyklus, von der Erfassung bis zur Löschung, überwacht. Dabei liegt ein besonderer Schwerpunkt auf der Zugriffsbegrenzung für Personen, bei denen es sich nicht um die betroffene Person handelt.

Das Grundprinzip dieses Konzepts beruht darauf, sich über die personenbezogenen Daten, die verarbeitet werden, Gedanken zu machen. Bei unstrukturierten Daten sollten Unternehmen also Richtlinien in Bezug auf die Zuordnung, das Management und die Sicherheit von personenbezogenen Daten syndizieren, instrumentieren und umsetzen und damit die Informationsökonomie verbessern und Risiken reduzieren. Bei strukturierten Daten könnten Unternehmen Richtlinien- und Metadatenmanagement implementieren und gleichzeitig die Datenherkunft untersuchen und steuern, um Informationen zu generieren, die die Grundsätze der Datenschutz-Grundverordnung unterstützen.

Fahrplan für die Einhaltung der Datenschutz-Grundverordnung

Vielen Unternehmen ist bewusst, dass sie jetzt handeln müssen, um sich auf die Datenschutz-Grundverordnung vorzubereiten, sind jedoch nicht sicher, wie sie am besten damit anfangen sollen. Es gibt dafür tatsächlich kein Geheimrezept; wo Sie anfangen hängt größtenteils von Ihrer aktuellen Situation ab. Daher hat IBM bestehende Kundenprojekte untersucht und mehrere allgemeine Lösungen identifiziert, die für die meisten Unternehmen angesichts der unmittelbaren Anforderungen für die Einhaltung der Datenschutz-Grundverordnung von höchster Priorität waren, sowie verschiedene andere Lösungen, die Unternehmen möglicherweise in Zukunft nutzen möchten.

Lösungen für den direkten Einsatz

Bewertung der Einhaltung der Datenschutz-Grundverordnung

Falls Sie es nicht bereits getan haben, sollten Sie zuerst den aktuellen Status des Datenschutzes in Ihrem Unternehmen sowie die Risiken in Bezug auf die Datenschutz-Grundverordnung bestimmen, denen Sie das Unternehmen aussetzen, wenn Sie jetzt nicht handeln. Dies umfasst idealerweise eine Zusammenfassung des Datenbestands, damit Sie wissen, wo im Unternehmen sich personenbezogene Daten befinden. In weiteren Schritten kann diese Zusammenfassung erweitert werden.

Ein wichtiges Ergebnis der Bewertung der Einhaltung der Datenschutz-Grundverordnung sollte eine Planung sein, die Sie dabei unterstützt, die identifizierten Risikoquellen zu vermeiden. Dies umfasst die Identifizierung bestehender Initiativen des Unternehmens, auf denen aufgebaut werden kann, sowie spezifischer Lücken in Bezug auf die Datenschutz-Grundverordnung, die es zu schließen gilt. Sobald Sie eine Planung haben, die Ihre nächsten Schritte auf dem Weg zur Einhaltung der Datenschutz-Grundverordnung priorisiert, können Sie Projektverantwortliche zuordnen, die bei diesen Aufgaben in Zukunft die Führung übernehmen.

Erkennung personenbezogener Daten

Mit der Erkennung personenbezogener Daten, die während oder nach der Bewertung der Einhaltung der Datenschutz-Grundverordnung durchgeführt werden kann, können Sie Ihr Wissen über Ihre Datenquellen und deren Inhalt vertiefen.

Viele Unternehmen wissen recht genau, wo sich ihre strukturierten Datenquellen befinden und wie deren Inhalt aussieht. Dies ist jedoch bei unstrukturierten Datenquellen nicht unbedingt der Fall. Datenquellen wie alte Dateifreigaben, gemeinsam genutzte Laufwerke, SharePoint und Content-Repositorys geraten leicht in Vergessenheit und enthalten daher häufig personenbezogene Daten, für die kein ordnungsgemäßer Nachweis möglich ist.

Selbst in Fällen, in denen Sie wissen, dass Sie über personenbezogene Daten verfügen, die geschützt werden müssen, wissen Sie möglicherweise nicht genug über den Umfang dieser Daten, die zugehörigen betroffenen Personen oder vergleichbare Einzelheiten. Im Zusammenhang mit der Einhaltung der Datenschutz-Grundverordnung haben wir herausgefunden, dass es äußerst wichtig ist, alte Daten zu löschen und gleichzeitig Daten, die aufbewahrt werden müssen, in ein leistungsfähiges Programm für Informationsgovernance und -sicherheit zu übertragen, damit sie in Zukunft bekannt sind, geschützt und berücksichtigt werden können.

IBM bietet seinen Kunden eine schnelle und effektive Lösung für die Einhaltung der Datenschutz-Grundverordnung, die von der Leistung von Tools wie IBM Information Analyzer, IBM Information Governance Catalog und IBM StoredIQ profitiert und sowohl strukturierte als auch unstrukturierte Datenquellen abdeckt. Ziel ist die Erstellung eines klar definierten Plans, um Sie dabei zu unterstützen, Ihre Bemühungen in Bezug auf die Einhaltung der Datenschutz-Grundverordnung innerhalb von vier bis sechs Wochen nach der Analyse voranzutreiben.

Im Rahmen des Projekts für die Einhaltung der Datenschutz-Grundverordnung wird Ihr Unternehmen möglicherweise mit Routinen konfrontiert, die als standardisierte und wiederholbare Prozesse genutzt werden, um in Ihrem Datenumfeld personenbezogene Daten zu identifizieren. Darüber hinaus arbeitet IBM mit Ihnen zusammen, um die Menge personenbezogener Daten in Ihren Datenspeichern zu minimieren, indem Daten identifiziert werden, die Sie nicht mehr aus geschäftlichen Gründen aufbewahren müssen. Durch die Minimierung dieser Daten – Begrenzung der Art der gespeicherten Daten und des Zeitraums der Speicherung – können Sie die Risiken in Bezug auf die Datenschutz-Grundverordnung minimieren.

Sie können damit beginnen, die personenbezogenen Daten, die Ihr Unternehmen verarbeitet, in nur zwei Monaten ab der Implementierung zu erkennen.

Datenbestand

Wenn Sie auf der bei der Bewertung der Einhaltung der Datenschutz-Grundverordnung festgelegten Grundlage aufbauen, wird alles, was Sie über Ihre personenbezogenen Daten gelernt haben, einschließlich der Datenquellen und deren physischer Position, im Datenbestand konsolidiert. Unserer Ansicht nach sollte dies im Rahmen der Anforderungen für Verzeichnisse von Verarbeitungstätigkeiten gemäß den Angaben in Artikel 30 der Datenschutz-Grundverordnung durchgeführt werden.

Die beste Möglichkeit, einen umfassenden und aktuellen Datenbestand zu erstellen, ist unserer Ansicht nach die Kombination eines Bottom-up-Ansatzes (unter Verwendung von Datenbestandstools) mit einem Top-down-Ansatz (wobei Gespräche mit Benutzern aus dem Geschäfts- und Technikbereich geführt werden, um aus erster Hand zu erfahren, welche Daten sich wo befinden und welchen geschäftlichen Nutzen Benutzer aus diesen Daten ziehen). Dieser Prozess sollte sich im Laufe der Zeit wiederholen, um mit Veränderungen Schritt zu halten.

IBM Tools wie Information Analyzer und StoredIQ unterstützen Sie dabei, den Prozess der Datenzuordnung für strukturierte und unstrukturierte Daten zu beschleunigen und zu erweitern. Durch die schnelle Analyse und Klassifizierung der Inhalte Ihrer Datenspeicher können Sie diese Tools und die anderen durchgeführten Aktivitäten für die Top-down-Zuordnung – zusammen mit IBM Information Governance Catalog – dabei unterstützen, einen detaillierten Katalog mit Datenspeichern für personenbezogene Daten, Speicherorten, Zwecken, Eigentümern, Arten von betroffenen Personen etc. zu erstellen. Sie können all das erreichen, während Sie den manuellen Aufwand reduzieren.

Ein umfassender und genauer Datenbestand kann die Grundlage für eine durchgängige Strategie für die Informationsgovernance sein. Daher sind die Vorteile nicht auf die Einhaltung der Datenschutz-Grundverordnung begrenzt; diese Strategie kann Sie zudem bei der Einhaltung anderer Vorschriften unterstützen, die jetzt oder in Zukunft für Sie gelten. Sie stellt zudem den ersten Schritt zur Unterstützung fundierterer Geschäftsergebnisse dar, indem professionellen Anwendern im gesamten Unternehmen geschäftskritische Daten bereitgestellt werden.

Maskierung, Verschlüsselung und Neubearbeitung

IBM Angebote, die Sie bei der Einhaltung der Datenschutz-Grundverordnung unterstützen können, umfassen unter anderem IBM Optim für die Maskierung und Neubearbeitung sowie IBM Guardium für die Verschlüsselung. Zusammen stellen diese Tools sicher, dass Daten jederzeit und überall verfügbar bleiben, und minimieren gleichzeitig das Risiko, dass auf ruhende Daten zugegriffen werden kann.

Mit Optim können Unternehmen den Grundsatz der Datenminimierung verfolgen. Informationen werden möglichst anonymisiert und es werden nur die Datenpunkte beibehalten, die für Verarbeitungstätigkeiten wie Analysen und Tests benötigt werden.

Durch die Verwendung der verschiedensten Maskierungsverfahren kann Optim dazu beitragen, Daten wie Kreditkartennummern, E-Mail-Adressen und Sozialversicherungsnummern zu schützen, ohne die zugrunde liegende kontextbezogene Bedeutung zu verlieren. Einfach gesagt, sieht eine maskierte Kreditkartennummer weiterhin wie eine Kreditkartennummer aus und funktioniert in Testworkloads auch so, ohne dass die Nummer selbst offengelegt wird.

Die Maskierung wird für Cloud- und On-Premises-Workloads mit vordefinierten Datenschutzklassifizierungen und -regeln durchgeführt, die die Zeit bis zur Implementierung verkürzen und Ihre Berichtsanforderungen vereinfachen. Auch wenn Daten, die nicht für die Verarbeitung benötigt werden, direkt redigiert werden können, kann das Unternehmen weiterhin Nutzen aus maskierten Daten ziehen. Dies ist nur eine der vielen Möglichkeiten, wie die Einhaltung der Datenschutz-Grundverordnung ein Unternehmen dabei unterstützen kann, seine Daten besser und vernünftiger zu nutzen.

Mit Datenverschlüsselungsservices von Guardium GDPR Accelerator kombiniert mit Funktionen für die Speicher- und Hardwareverschlüsselung kann sichergestellt werden, dass nur Personen mit berechtigtem Bedarf auf sensible personenbezogene Daten zugreifen können. Um den Anforderungen der Datenschutz-Grundverordnung gerecht zu werden, deckt diese Verschlüsselung den gesamten Datenlebenszyklus ab, von dem Zeitpunkt, an dem die Daten zum ersten Mal in das Unternehmen gelangen, bis zu dem Zeitpunkt, an dem sie entweder gelöscht oder maskiert werden.

Unternehmen können auch IBM Enterprise Content Management-Lösungen nutzen, um unstrukturierte Inhalte basierend auf Benutzerrollen zu verwalten und zu redigieren. Benutzern werden die Daten angezeigt, die sie sehen müssen, um ihre Arbeit zu erledigen. Nicht mehr.

Das IBM Framework zur Datenschutz-Grundverordnung

IBM hat ein Framework zur Datenschutz-Grundverordnung erstellt, das fünf Phasen umfasst, um die Einhaltung der Datenschutz-Grundverordnung zu erreichen, wie in Abbildung 2 dargestellt: Bewertung, Gestaltung, Transformation, Betrieb und Konformität. Ziel des Framework ist es, Kunden dabei zu unterstützen, effektives Management von Sicherheit und Datenschutz aus Risikoperspektive zu betreiben, um ihr Risiko und damit Vorfälle zu reduzieren.

Bewertung, Gestaltung, Transformation, Betrieb und Konformität

Phase	**Bewertung**	**Gestaltung**	**Transformation**	**Betrieb**	**Konformität**
Aktivität	• Führen Sie Bewertungen in Bezug auf die Datenschutz-Grundverordnung in den Bereichen Datenschutz, Governance, Personen, Prozesse, Daten und Sicherheit durch • Entwickeln Sie eine Planung für die Einhaltung der Datenschutz-Grundverordnung • Identifizieren Sie personenbezogene Daten	• Gestalten Sie Standards für Governance, Schulungen, Kommunikation und Prozesse • Gestalten Sie Standards für Datenschutz, Datenmanagement und Sicherheitsmanagement	• Entwickeln und integrieren Sie Verfahren, Prozesse und Tools • Stellen Sie Schulungen zur Datenschutz-Grundverordnung bereit • Entwickeln/Integrieren Sie Standards unter Verwendung von Privacy by Design-, Security by Design- und Daten-management-Richtlinien	• Führen Sie alle wichtigen Geschäftsprozesse aus • Überwachen Sie Sicherheit und Datenschutz unter Verwendung von technischen und organisatorischen Maßnahmen • Verwalten Sie Zugriffs- und Einwilligungsrechte betroffener Personen	• Überwachen, bewerten, prüfen, melden und evaluieren Sie die Einhaltung der Standards in Bezug auf die Datenschutz-Grundverordnung
Ergebnis	**Bewertungen und Planung**	**Definierter Implementierungs-plan**	**Abgeschlossene Prozesse und Erweiterungen**	**Betriebliches Framework vorhanden**	**Fortlaufende Überwachung und Berichterstellung**
	Identifizieren Sie die Auswirkungen der Datenschutz-Grund-verordnung und planen Sie technische und organisatorische Maßnahmen	Umfasst die zu implementierenden Datenschutzkontrollen, -prozesse und -lösungen	Technische und organisatorische Maßnahmen: Erkennung, Klassifizierung und Governance personen-bezogener Daten	Arbeiten Sie fortan unter Einhaltung der neuen Datenschutz-Grund-verordnung	Überwachen Sie die Einhaltung der technischen und organisatorischen Maßnahmen: bieten Sie einen Nachweis für interne und externe Beteiligte

Abbildung 2: Das IBM Framework zur Datenschutz-Grundverordnung.

Zusätzliche Lösungen für die Zukunft

Auch wenn wir der Ansicht sind, dass die im vorhergehenden Abschnitt genannten Lösungen die logischsten Ausgangspunkte für die meisten Unternehmen sind, die sich auf die Datenschutz-Grundverordnung vorbereiten, gibt es viele verschiedene andere Bereiche, von denen Sie profitieren können, nachdem Sie die grundlegenden ersten Schritte eingeleitet haben.

Plan für den Schutz kritischer Daten: Identifizieren und klassifizieren Sie die kritischen Assets Ihres Unternehmens in Bezug auf die Datenschutz-Grundverordnung, einschließlich „Kronjuwelen“ und anderer geschützter Informationen.

Master Data Management: Nutzen Sie eine 360-Grad-Ansicht der einzelnen betroffenen Personen, der Art von Daten, die Sie für diese speichern, und des genauen Speicherorts.

Anforderung von Zugriffsrechten durch betroffene Personen: Bieten Sie betroffenen Personen eine einfache und effektive Möglichkeit, ihre Rechte auf Rückfrage, Berichtigung und Löschung auszuüben.

Einwilligungsmanagement: Legen Sie für jede Nutzung und jeden Bürger spezielle Anforderungen für die Datenverarbeitung und die Nutzungseinwilligung fest.

Sicherheitsimplementierung und Korrektur: Stellen Sie Informationssicherheit für alle Funktionen für die Verarbeitung personenbezogener Daten zur Verfügung.

Incident-Management: Stellen Sie über IBM Resilient-Angebote proaktive Funktionen für Incident-Vorbereitung, -Management und -Berichterstellung bereit.

Datenentsorgung: Entfernen Sie Daten auf allen Systemen, die keinem geschäftlichen Zweck mehr dienen.

Personen- und Prozessänderungsmanagement: Schaffen Sie eine Unternehmenskultur, die alle in diesem Dokument beschriebenen technischen Änderungen ergänzt.

Pflichten im Rahmen der Datenschutz-Grundverordnung

Wie dieses Dokument veranschaulichen möchte, ist die Einhaltung der Datenschutz-Grundverordnung alles andere als einfach. Es handelt sich um einen Prozess, der komplex, schwierig und kostenintensiv sein kann, aber auch notwendig ist. Zusätzlich zu der einfachen Tatsache, dass Sie damit erhebliche Geldbußen vermeiden können, können Sie die Einhaltung der Datenschutz-Grundverordnung jetzt als Geschäftskosten verbuchen, wenn es um die erfolgreiche Interaktion mit der Europäischen Union geht.

Darüber hinaus sind wir der Ansicht, dass die Implementierung der Datenschutz-Grundverordnung der erste Schritt zur Öffnung eines einzigen digitalen Markts für ganz Europa sein kann. Unternehmen, die jetzt handeln, haben die beste Ausgangslage, um in dieser neuen Realität erfolgreich zu sein.

Die Einhaltung der Datenschutz-Grundverordnung ist zudem eine hervorragende Möglichkeit, das Vertrauen Ihrer Kunden und Mitarbeiter zu gewinnen, die Transparenz und das Wissen in Bezug auf Ihr Unternehmen zu verbessern, jedem professionellen Anwender qualitativ hochwertige Daten bereitzustellen, effizienter zu werden und potenziell neue und bessere umsatzgenerierende Geschäftschancen zu identifizieren. Die Vorteile der Einhaltung der Datenschutz-Grundverordnung sind wie die Risiken einer Nichteinhaltung ein guter Grund, zu handeln.

Jetzt, da Sie die Dringlichkeit der Einhaltung der Datenschutz-Grundverordnung sowie einige der ersten Schritte kennen, stehen Ihnen die Mitarbeiter, Prozesse und Technologien von IBM zur Verfügung, um Sie dabei zu unterstützen, weiterzukommen. Unabhängig davon, ob Sie Hilfe bei der Identifizierung der erforderlichen Schritte benötigen oder ob Sie bereit sind, eine umfassende Plattform für die Informationsgovernance einzusetzen – wir bieten Ihnen die notwendige Unterstützung.

Weitere Informationen

Wenn Sie mehr über die Ansicht von IBM zur Einhaltung der Datenschutz-Grundverordnung erfahren möchten, besuchen Sie uns noch heute unter **ibm.com**/gdpr oder wenden Sie sich an Ihren IBM Ansprechpartner.

IBM Deutschland GmbH
IBM-Allee 1
71139 Ehningen
ibm.com/de

IBM Österreich
Obere Donaustraße 95
1020 Wien
ibm.com/at

IBM Schweiz
Vulkanstrasse 106
8010 Zürich
ibm.com/ch

Die IBM Homepage finden Sie unter:
ibm.com

IBM, das IBM Logo, ibm.com, StoredIQ, Optim, Guardium und Resilient sind eingetragene Marken oder Marken der IBM Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite „Copyright and trademark information“ unter **ibm.com**/legal/copytrade.shtml

Dieses Dokument ist zum Datum seiner Erstveröffentlichung aktuell und kann jederzeit von IBM geändert werden. Nicht alle IBM Angebote sind in jedem Land, in welchem IBM tätig ist, verfügbar.

Dieses Dokument wird auf der Grundlage des gegenwärtigen Zustands (auf „as-is“-Basis) und ohne jede Gewährleistung für die Handelsüblichkeit und die Verwendungsfähigkeit für einen bestimmten Zweck zur Verfügung gestellt. Für IBM Produkte gelten die Gewährleistungen, die in den Vereinbarungen vorgesehen sind, unter denen sie erworben werden.

Hinweis: Jeder Kunde ist für die Einhaltung der geltenden Gesetze und Verordnungen, einschließlich der Datenschutz-Grundverordnung der Europäischen Union, selbst verantwortlich. Es obliegt allein den Kunden, sich von kompetenter juristischer Stelle zu Inhalt und Auslegung aller relevanten Gesetze und gesetzlichen Bestimmungen beraten zu lassen, die ihre Geschäftstätigkeit und die von ihnen eventuell einzuleitenden Maßnahmen zur Einhaltung dieser Gesetze und Bestimmungen betreffen. Die in diesem Dokument beschriebenen Produkte, Services und sonstigen Funktionen eignen sich nicht für alle Kundensituationen und sind möglicherweise nur eingeschränkt verfügbar. IBM erteilt keine Rechts- oder Steuerberatung und gibt keine Garantie bezüglich der Konformität von IBM Produkten oder Services mit den geltenden Gesetzen und gesetzlichen Bestimmungen.

Erklärung zu geeigneten Sicherheitsvorkehrungen: Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines gesetzeskonformen, umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

1 The Privacy Advisor, *ICO's Wood: GDPR grace period? No way.* https://iapp.org/news/a/icos-wood-gdpr-grace-period-no-way/

© Copyright IBM Corporation 2017

Bitte der Wiederverwertung zuführen

ASW12436-DEDE-02