DSGVO - Mit Übersicht zum Ziel

Schritt für Schritt zur erfolgreichen Umsetzung

Die bevorstehende Neuerung der Datenschutzgrundverordnung (DSGVO) scheint wie ein Damoklesschwert über den Unternehmen zu schweben – in Deutschland, wie auch in anderen europäischen Ländern. Das führt leider dazu, dass die Betroffenen oft wie ein Kaninchen vor der Schlange erstarren, anstatt sich mit einer positiven Herangehensweise den Herausforderungen dieser Datenschutznovelle zu stellen. Angst war noch nie ein guter Berater. Wichtig ist, die Übersicht über alle Aspekte zu behalten und planvoll an die Sache heranzugehen.

Grundsätzlich gilt die EU-DSGVO für alle Unternehmen, die einen Sitz oder eine Niederlassung in der EU haben oder die Angebote bereithalten, die sich an Personen innerhalb der EU richten. Die Verordnung gibt vor, wie künftig personenbezogene Daten durch definierte organisatorische Prozesse und technische Maßnahmen zu schützen sind. Ziel ist es, den vielfach lockeren Umgang mit personenbezogenen Daten zu unterbinden und dafür zu sorgen, dass personenbezogene Daten mit höchster Vertraulichkeit und Sicherheit behandelt werden. Darüber hinaus verfolgt die EU mit der Verordnung eine Harmonisierung des Datenschutzes innerhalb der Staatengemeinschaft.

Warum sollte man die DSVGO unbedingt beachten?

Um die Notwendigkeit dieses Anliegens zu unterstreichen, enthält die DSGVO neben verschiedenen Maßnahmen, die die Aufsichtsbehörden anordnen können, auch Sanktionen (bis hin zur Einstellung der Datenverarbeitung). Da die DSGVO festlegt, dass die Sanktionen wirksam und abschreckend sein sollen, sind die Folgen bei Missachtung dementsprechend drastisch: Bis zu 20 Millionen Euro oder vier Prozent des weltweiten Gesamtumsatzes eines Unternehmens kann die Strafe betragen – je nachdem wie schwerwiegend die Missachtung der Sicherheit der personenbezogenen Daten ist. Deshalb sollte niemand die Augen davor verschließen und hoffen, dass sein Unternehmen bei einer Prüfung mit einem blauen Auge davonkommt. Es ist davon auszugehen, dass es bereits zeitnah nach dem Stichtag zum 25.05.2018 erste Kontrollen geben wird, um Präzedenzfälle zu schaffen und einem all zu laschen Umgang mit der DSGVO entgegen zu wirken.

Wer glaubt, er könnte nach Anzeige eines Verstoßes und der Ankündigung einer Kontrolle noch Korrekturen vornehmen, der irrt. Alle Rechte der DSGVO können binnen kurzer Frist ausgeübt werden, so dass faktisch „nachträgliche" Dokumentationen oder Änderungen unmöglich sind. Umso wichtiger ist es, die eigenen Prozesse DSGVO-konform zu gestalten.

Was ist zu tun?

Das Wichtigste ist, einen Überblick über die einzelnen Aspekte der DSGVO zu bekommen. Dabei hilft die Erstellung einer DSGVO-Map. Eine solche Map basiert auf der Mindmapping-Methode und sorgt dafür, dass Zusammenhänge nachvollziehbar werden. Mit Icons, Prioritäten und Ressourcen lässt sich anhand einer DSGVO-Map sogar ein konkreter Umsetzungsplan generieren. Die Prozesse im eigenen Unternehmen so zu erfassen und zu prüfen, stellt übrigens auch eine Chance dar, Dinge, die „immer schon so getan wurden", zu hinterfragen.

Die Map in diesem Beitrag, die mit MindManager erstellt wurde, beinhaltet die Kernpunkte der DSGVO, ihre Herausforderungen

sowie die Folgen bei Missachtung. Sie kann als Grundlage für sämtliche individuelle DSGVO-Maps genommen werden. Darüber hinaus empfiehlt sich ein 6-stufiges Vorgehensmodell zur Realisation der neuen Rechtslage.

Schritt für Schritt zur DSGVO-Compliance

1. Grundsteine legen

Zunächst muss das Management sensibilisiert, Leitfäden und Auslegungshilfen herangezogen und Schwerpunkte definiert werden. Dann geht es darum ein DSGVO-Projekt aufzusetzen und diesem die entsprechenden Ressourcen zuzuordnen. Wichtig: Die Umsetzung der DSGVO-Compliance liegt in der Verantwortung der Geschäftsführung. Sicherlich kann das Projekt an sich federführend durch die IT mit Unterstützung der Fachabteilungen realisiert werden, die Haftung liegt aber letztlich bei der Geschäftsleitung.

2. Bestandsaufnahme durchführen

Nun sind die Prozesse der Datenverarbeitung zu untersuchen, die bestehenden Compliance-Maßnahmen zu identifizieren und Veränderungen bei den Datenverarbeitungsaktivitäten zu verfolgen. Dabei sind Datenströme und -speicherungen innerhalb des Unternehmens genauso relevant wie deren Austausch mit Dritten. Es sollte auch geprüft werden, ob das Unternehmen einen Datenschutzbeauftragten benennen muss. Dieser sollte im Folgenden in die Umsetzung der weiteren Schritte miteinbezogen werden.

3. Analyse & Ableitung von Handlungsnotwendigkeiten

Es gilt, die gesammelten Informationen zu systematisieren und auszuwerten. Dabei sollte auf vorhandenen Verfahren und Instrumenten aufgebaut werden. Schwachstellen müssen identifiziert und Spielräume ausgelotet werden können. Schließlich muss ein Projektplan mit Abhilfemaßnahmen aufgesetzt werden. Wichtig: Die Priorisierung der einzelnen Schritte und deren Abhängigkeit voneinander sollten dokumentiert werden.

4. Umsetzung

Nun sind neue Richtlinien und Aufsichtsstrukturen einzuführen sowie notwendige technische Änderungen vorzunehmen. Wichtig ist dabei, dass bei der Umsetzung die verfahrensmäßigen DSGVO-Vorgaben eingehalten werden. Deshalb müssen Verantwortlichkeiten neu zugeordnet und Mitarbeiter geschult werden. Damit dies gelingt, empfiehlt es sich, die Mitarbeiter bereits sehr frühzeitig in den Prozess einzubinden, damit sie die Notwendigkeit der Änderungen nachvollziehen und die neuen Prozesse ihrerseits unterstützen können.

5. Feinschliff

Optimaler Weise werden jetzt Maßnahmen mit geringerer Priorität realisiert und ein Reaktionsplan für zukünftige Änderungen aufgestellt.

6. Überwachung

Die DSGVO-Compliance sollte konsequent überwacht werden. Es sind Schulungsprogramme zu etablieren, Leitlinien auszuarbeiten und nationale Ausnahmeregelungen und deren Folgen zu beobachten. Die Abläufe sollten dabei möglichst so gestaltet sein, dass sie sich problemlos in die üblichen Unternehmensprozesse integrieren lassen, denn nur so lässt sich eine kontinuierliche Compliance realisieren.

Fazit

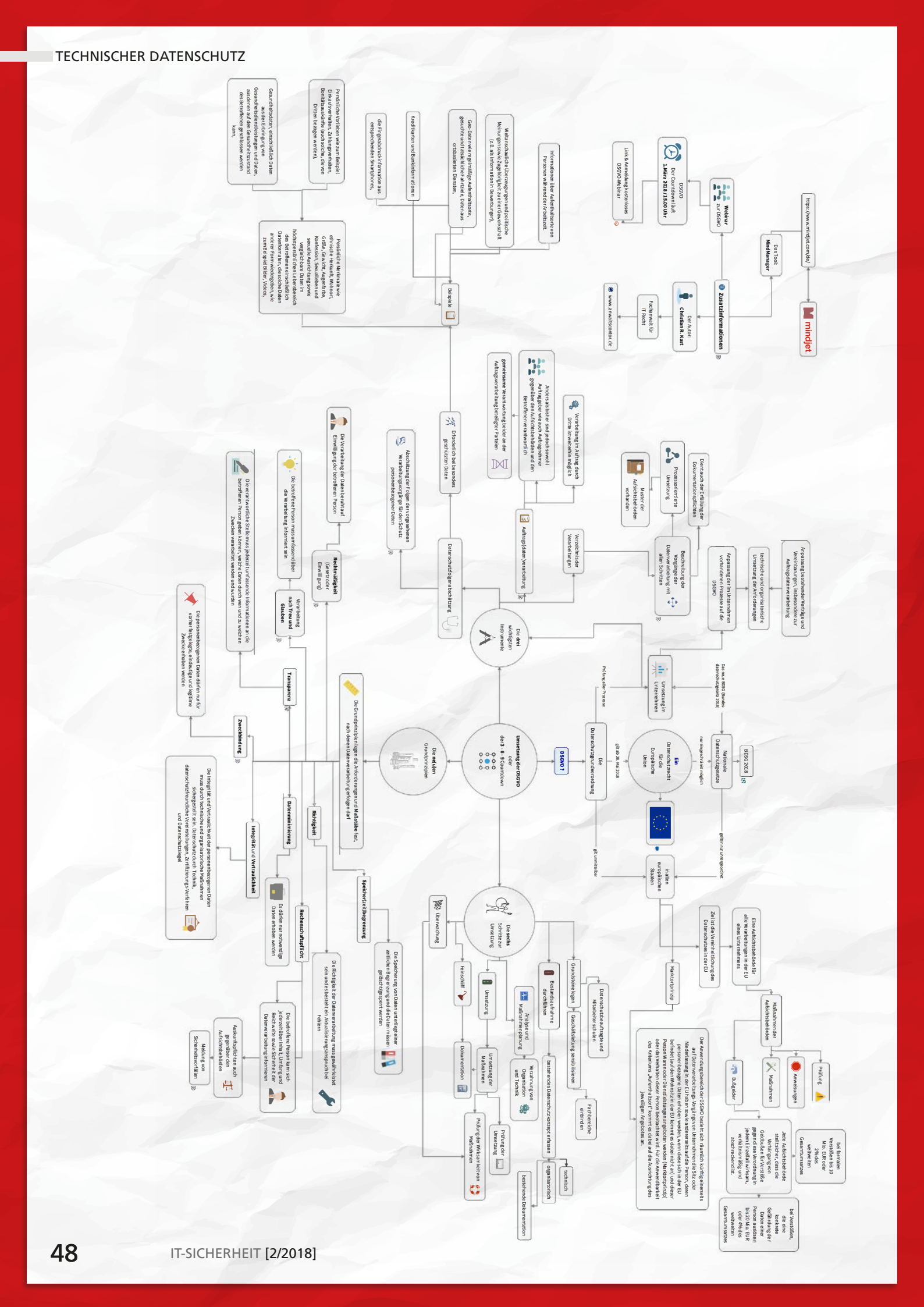
Das DSGVO ist weniger eine Bedrohung als vielmehr eine Chance. Es ist die Möglichkeit, Prozesse zu digitalisieren, Strukturen neu zu ordnen und das Business zukunftssicher aufzustellen. Man sollte die DSGVO auch nicht als Einschränkung empfinden und behandeln, sondern vielmehr zum Anlass nehmen über neue Grundsätze in punkto Datensicherheit zu reflektieren – schließlich sind dergleichen Regelungen kein Selbstzweck, sondern sollen helfen, die internationale Wirtschaft und ihre Prozesse abzusichern. Darüber hinaus wird insbesondere die Datensicherheit auch aus Kundensicht künftig ein Merkmal sein, das über das Eingehen einer Kundenbeziehung entscheiden kann. ■

DER EXPERTEN-TIPP

Vor der Umsetzung dieser Schritte empfiehlt sich durchaus eine Rückversicherung bei einem Datenschutz-Spezialisten. In Deutschland gibt es eine Vielzahl von Fachanwälten, die sich auf IT-Recht und Datenschutz spezialisiert haben. Außerdem stehen im Internet, insbesondere auch auf den Seiten der Aufsichtsbehörden und in entsprechenden Expertenforen, Whitepaper oder Best Practices zur Verfügung.

Darüber hinaus ist es auch denkbar, anlässlich der Einführung der DSGVO, einen sogenannten „Data Process Manager" zu benennen und mit dem Projekt zu betrauen. Data Process Manager verfügen in der Regel über einen juristischen oder technischen Background und haben zudem konkrete Erfahrung in der Unternehmens-IT. Vielfach handelt es sich um IT-Profis, mit ITIL-Erfahrung, Audit-Kenntnissen und einer weitreichenden Expertise im Bereich Compliance.

CHRISTIAN R. KAST,
Fachanwalt für IT-Recht


https://www.mindjet.com/de/
mindjet
Das Tool: Mindmanager
Zusatzinformationen
Webinar zur DSGVO
DSGVO Der Countdown läuft 1. März 2018 / 15.00 Uhr
Link & Anmeldung kostenloses DSGVO-Webinar
Der Autor: Christian R. Kast
Fachanwalt für IT-Recht
www.anwaltscontor.de
Beispiele
Webanschauliche Überzeugungen und politische Meinungen sowie Zugehörigkeit zu einer Gewerkschaft (z.B. als Information in Bewerbungen),
Geo-Daten wie regelmäßige Aufenthaltsorte, gesuchte und tatsächliche Fahrziele, Daten aus ortsbasierten Diensten,
Kreditkarten und Bankinformationen
die Fingerabdruckinformation aus entsprechenden Smartphones,
Informationen über Aufenthaltsorte von Personen während der Arbeitszeit,
Persönliche Vorlieben wie zum Beispiel Einkaufsverhalten, Zahlungsverhalten, Bonitätsauskünfte (auch solche, die von Dritten bezogen werden),
Persönliche Merkmale wie ethnische Herkunft, Wohnort, Größe, Gewicht, Augenfarbe, Konfession, Sexualleben und sexuelle Ausrichtung sowie höchstpersönlichen Lebensbereich des Betroffenen einschließlich Datenformaten, die solche Daten anderer Form wiedergeben, wie zum Bsp. Bilder, Videos,
Gesundheitsdaten, einschließlich Daten aus der Erbringung von Gesundheitsdienstleistungen und Daten, aus denen auf den Gesundheitszustand des Betroffenen geschlossen werden kann,
Anpassung bestehender Verträge und Vereinbarungen, insbesondere zur Auftragsdatenverarbeitung
technische und organisatorische Umsetzung der Anforderungen
Anpassung der im Unternehmen vorhandenen Prozesse auf die DSGVO
Das neue BDSG (Bundesdatenschutzgesetz 2018)
BDSG 2018
Nationale Datenschutzgesetze
nur eingeschränkt möglich
gelten nur ergänzend
Ein Datenschutzrecht für die Europäische Union
gilt ab 25. Mai 2018
DSGVO ?
Die Datenschutzgrundverordnung
gilt unmittelbar
In allen europäischen Staaten
Umsetzung im Unternehmen
Pickup aller Prozesse
Die drei wichtigsten Instrumente
Beschreibung der Vorgänge mit allen Schritten
Verzeichnis der Verarbeitungen
Auftragsdatenverarbeitung
Prozessorientierte Umsetzung
Muster der Aufsichtsbehörden verfügbar
Dient auch der Erfüllung der Dokumentationspflichten
Verarbeitung im Auftrag durch Dritte grundsätzlich möglich
Anders als bisher sind jedoch sowohl Auftraggeber wie auch Auftragnehmer gegenüber den Aufsichtsbehörden und den Betroffenen verantwortlich
gemeinsame Verantwortung beider an der Auftragsverarbeitung beteiligter Parteien
Erforderlich bei besonders geschützten Daten
Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten
Datenschutzfolgenabschätzung
Umsetzung der DSGVO oder der 3 - 6 - 9 Countdown
Die sechs Schritte zur Umsetzung
Die neuen Grundprinzipien
Die Grundprinzipien liegen die Anforderungen und Maßstäbe fest, nach denen Datenverarbeitung erfolgen darf
Rechtmäßigkeit (Gesetz oder Einwilligung)
Die Verarbeitung der Daten bedarf auf Einwilligung der betroffenen Person
Verarbeitung nach Treu und Glauben
Die betroffene Person muss zum Beispiel über die Verarbeitung informiert sein
Transparenz
Die verantwortliche Stelle muss jederzeit umfassende Informationen an die betroffenen Person geben können, welche Daten durch wen und zu welchen Zwecken verarbeitet werden und wurden
Zweckbindung
Die personenbezogenen Daten dürfen nur für vorher festgelegte, eindeutige und legitime Zwecke erhoben werden
Datenminimierung
Es dürfen nur notwendige Daten erhoben werden
Richtigkeit
Integrität und Vertraulichkeit
Die Integrität und Vertraulichkeit der personenbezogenen Daten muss durch technische und organisatorische Maßnahmen sichergestellt sein. Datenschutz durch Technik, datenschutzfreundliche Voreinstellungen, Zertifizierungs-Verfahren und Datenschutzsiegel
Rechenschaftspflicht
Die Richtigkeit der Datenverarbeitung muss gewährleistet sein und es besteht ein Anspruch auf Berichtigung, Sperrung oder Löschung
Die betroffene Person kann sich jederzeit über Inhalt, Umfang und Reichweite sowie Sicherheit der Datenverarbeitung informieren
Auskunftspflichten auch gegenüber den Aufsichtsbehörden
Meldung von Sicherheitsvorfällen
Speicherzeitbegrenzung
Die Speicherung von Daten unterliegt einer zeitlichen Begrenzung und die Daten müssen gelöscht/gesperrt werden
Überwachung
Die sechs Schritte zur Umsetzung
Grundsteine legen
Bestandsaufnahme durchführen
Analyse und Maßnahmenplanung
Umsetzung
Umsetzung Maßnahmen
Prüfung der Umsetzung
Feinschliff
Dokumentation
Prüfung der Wirksamkeit von Maßnahmen
Geschäftsleitung sensibilisieren
bestehendes Datenschutzkonzept erfassen
Verzahnung von Organisation und Technik
organisatorisch
technisch
bestehende Dokumentation
Fachbereiche einbinden
Datenschutzbeauftragte und Mandanten schulen
Marktortprinzip
Zielt die Vereinheitlichung des Datenschutzes in der EU
Eine Aufsichtsbehörde für alle Verarbeitungen in der EU einer Unternehmens
Maßnahmen der Aufsichtsbehörden
Maßnahmen
Anwesungen
Prüfung
bis 10 Mio. EUR oder 2% des weltweiten Gesamtumsatzes
Bußgelder
Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen für Verstöße gegen diese Verordnung in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.
bis 20 Mio. EUR oder 4% des weltweiten Gesamtumsatzes
bei Verstößen, die eine konkrete Gefährdung der Daten einer Person auslösen
Die Anwendungsbereiche der DSGVO bezieht sich räumlich künftig einerseits auf Datenverarbeitungs-Vorgänge von Unternehmen die Sitz oder Niederlassung in der EU haben sowie andererseits auf die Person, deren personenbezogene Daten erhoben werden, wenn diese sich in der EU befindet (auf den Wohnsitz in der EU kommt es dabei nicht an) und dieser Person Waren oder Dienstleistungen angeboten werden (Marktortprinzip) oder das Verhalten dieser Person beobachtet wird. Für die Anwendbarkeit des Kriteriums „Aufenthaltsort" kommt es dabei auf die Ausrichtung des jeweiligen Angebotes an.