DSGVO

Das ändert sich in Marketing & Vertrieb

Welche konkreten Änderungen ergeben sich aus der neuen Verordnung für Ihr Unternehmen?

michael prothmann consulting group

1. Ziele der neuen DSGVO

EU-DSGVO bedeutet EU-Datenschutzgrundverordnung. Thematisch befasst sich die DSGVO mit – wie der Name schon impliziert – dem Datenschutz personenbezogener Daten. Im März 2016 wurde die offizielle Fassung der DSGVO bestimmt. Im April 2016 hat der Ministerrat der EU über die DSGVO beraten und anschließend wurde die Verordnung für die Abstimmung ins EU-Parlament gegeben und ratifiziert.

Die Verordnung tritt ab dem 25.05.2018 in Kraft und greift ab diesem Stichtag sofort. Das bedeutet, dass alle Unternehmen sich bis dahin auf die DSGVO eingestellt haben müssen. Ab dem 25.05.2018 gelten nationale Gesetze zur Daten-verarbeitung nicht mehr. Lediglich 50 Öffnungsklauseln erlauben in Zukunft nationale Reglementierungen. In diesen 50 Öffnungs-klauseln greift die DSGVO nicht. Alle übrigen Regulierungen sind europaweit ohne Ausnahme bindend. Ein Entwurf des Bundestags wurde am 27.04.2017 beschlossen und am 12.05.2017 vom Bundesrat gebilligt.

Unsere Themen

Ziele der neuen DSGVO
S. 2

Anwendungsbereiche der DSGVO
S. 2

Inhalte der DSGVO
S. 4

Zehn Änderungen in der Praxis
S. 6

Unsere Empfehlung für Sie
S. 9

Das primäre Ziel der Verordnung ist eine Ausweitung der informellen Selbstbestimmung persönlicher Daten. Dies beinhaltet den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und damit einhergehend deren Recht, dass personenbezogene Daten geschützt werden. Trotz der Reglementierungen soll, parallel zum Schutz, auch der freie Verkehr personenbezogener Daten sichergestellt werden. Diese Ziele wurden bisher in Deutschland in folgenden drei Gesetzesbüchern reglementiert: im Bundesdatenschutzgesetz (BDSG), im Telemediengesetz (TMG) und im Telekommunikationsgesetz (TKG). Diese gelten dort wo die EU-DSGVO greift, nicht mehr.

Die EU-DSGVO soll dabei den Datenschutz in der EU nicht völlig reformieren, jedoch in der Praxis einige Dinge ändern und Datenschutz zur gelebten Praxis machen. Die DSGVO hat zur Folge, dass der gesamte Datenschutz zum einen in der ganzen EU vereinheitlicht wird und zum anderen, dass Datenschutz konsequent geahndet wird. Bußgelder werden grundsätzlich deutlich höher ausfallen als bisher. Somit sollten sich Unternehmen im eigenen Interesse an die Verordnung halten.

2. Anwendungsbereich der DSGVO

Das Anwendungsgebiet der DSGVO lässt sich in den sachlichen und den räumlichen Anwendungsbereich untergliedern. 2.1 behandelt den sachlichen Anwendungsbereich und 2.2 den räumlichen Anwendungsbereich.

2.1 Für wen gilt die DSGVO?

Grundlage für die DSGVO ist, dass ein gewerblicher Zweck der Datenerhebung zugeordnet werden kann. Das Ziel der Datenverarbeitung ist also, dass einer Person Produkte oder Dienstleistungen angeboten werden. Daten, die privat und familiär genutzt werden, sind nicht von der DSGVO betroffen.

Art. 2 DSGVO ist Grundlage für den sachlichen Anwendungsbereich der DSGVO. Der sachliche Anwendungsbereich regelt, für wen die Verordnung gilt. Grundsätzlich gilt die EU-DSVGO bei der Verarbeitung aller personenbezogenen Daten. Personenbezogene Daten sind Daten, die einer Person zugeordnet werden können. Daten, die nicht personenbezogen sind, sind nicht Gegenstand der DSGVO. Grundsätzlich betroffen sind Daten jeder Person oder Unternehmen, die durch die Verarbeitung einen ökonomischen Zweck erhalten.

2.2 Wo gilt die DSGVO?

Art. 3 DSGVO behandelt den räumlichen Anwendungsbereich der DSGVO – also das Wo.
Das Wo ist an die Verarbeitung der Daten gekoppelt, also wo die Daten verarbeitet werden. In erster Instanz gilt die DSGVO für alle Unternehmen, die personenbezogene Daten verarbeiten und ihre Niederlassung in der Europäischen Union haben.

Doch auch Unternehmen, die keinen Sitz in der EU haben, sind von der DSGVO nicht befreit. Denn die DSGVO greift auch für alle Unternehmen deren Datenverarbeitung im Zusammenhang steht mit den Anbietern von Waren und Dienstleistungen innerhalb der EU, also auch für einen Online-Shop aus Indien, der lediglich E-Mail-Adressen von EU-Bürgern generiert, um diesen gezielt Waren anzubieten.

Die DSGVO greift auch, sobald Daten durch Beobachten von Personen innerhalb der EU erhoben werden. Dies ist relevant für Marktforschungen, oder Untersuchungen des Nutzerverhaltens von Personen in der EU.

All diese Kriterien greifen für Personen, die sich in der EU aufhalten. Auch ein kurzer Aufenthalt reicht aus – die DSGVO ist also nicht an eine Staatsbürgerschaft eines EU-Staats gebunden.
Die DSGVO greift jedoch nicht, wenn eine Webseite in der EU aufrufbar ist, oder eine Webseite auf einer Sprache ist, die in der Union gesprochen wird. Bedingung für das Greifen der Verordnung ist ein ökonomisches Ziel und eine Verarbeitung, Erhebung oder Speicherung personenbezogener Daten von Personen, die sich innerhalb der EU befinden.

3. Inhalte der DSGVO

Um die DSGVO inhaltlich zu verstehen, wird der Inhalt unterteilt in verschiedene Schwerpunkte. Begonnen wird mit den Grundsätzen der DSGVO. Da der Nutzer im Mittelpunkt der DSGVO steht, folgen danach die neuen Rechte, die ein Nutzer durch die DSGVO bekommt. Die Rechte werden analog zum Gesetzestext inhaltlich aufgeteilt und erläutert.

3.1 Was sind die Grundsätze der DSGVO?

An diesen Grundsätzen der DSGVO haben sich alle Datenverarbeitende zu orientieren:

- Rechtmäßigkeit der Speicherung
- Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit der Datenverarbeitung
- Begrenztes Speichern
- Integrität und Vertraulichkeit

Rechtmäßigkeit der Speicherung: Dies bedeutet, dass Daten nur gesetzeskonform gespeichert werden dürfen. Dies hört sich zunächst nach einer Selbstverständlichkeit an, jedoch sollte dies im Rahmen des Inkrafttretens
der DSGVO geprüft werden. Zu prüfen ist, ob die Daten auch ab Mai 2018 rechtens gespeichert werden und wurden. Als Grundsatz dient hier die Einwilligung der Person Art.6 Abs. 1 lit. a).

Treu und Glauben ist aktuell noch ein sehr schwammiger Begriff und ist rechtlich kaum zu fassen. Grundsätzlich geht es darum, ob ein bestimmtes Verhalten als anständig angesehen werden kann. Dieser Grundsatz wird erst mit vergangener Rechtsprechung zweifelsfrei zu verstehen sein, indem dieser Grundsatz durch Fallbeispiele konkretisiert wird.

Transparenz bedeutet, dass die Daten so gespeichert werden, dass eine Nachweisbarkeit jederzeit zu erbringen ist. Durch neue Rechte des Nutzers müssen Unternehmen alle Daten transparent offenlegen, die über den entsprechenden Nutzer gespeichert sind. Praktisch bedeutet dies, dass der Betroffene sein Recht auf informationelle Selbstbestimmung wahr-nehmen kann Art. 5 Abs. 1 lit a). Nichtsdestotrotz dürfen die Daten auch zu einem anderen Zweck genutzt werden, sofern diese nicht mit dem ursprünglichen Zweck unvereinbar sind.

Zweckbindung: Die Daten dürfen nur für den Zweck genutzt werden, zu dem sie generiert worden sind. Dies bedeutet: Gibt der Nutzer seine Einwilligung für den Erhalt eines Newsletters, dürfen diese gewonnenen Kundendaten nicht für andere Zwecke genutzt werden. Nichtsdestotrotz dürfen die Daten auch zu einem anderen Zweck genutzt werden, sofern die Zwecke der Weiterverarbeitung nicht mit dem ursprünglichen Zweck unvereinbar sind.

Datenminimierung: Daten sollten möglichst sparsam gespeichert werden. Dies bedeutet, dass quantitativ nur Daten gespeichert werden, die wirklich notwendig sein. Zudem impliziert der Grundsatz der Datensparsamkeit, dass ein Löschkonzept vorhanden sein muss.
Richtigkeit der Datenverarbeitung: Dies bedeutet, dass Daten nur richtig gespeichert werden und nicht manipuliert werden, so dass sie Unternehmenszwecken dienlicher sind.

Begrenztes Speichern: Daten sollen möglichst begrenzt gespeichert werden. Dieser Grundsatz zielt praktisch auf das Unterbinden von Big-Data ab. Es sollen keine Massen an Daten gespeichert werden, die zweckentfremdend angereichert und benutzt werden können. Dies bezieht sich auch auf den zeitlichen Faktor des Speichers. Sobald der Zweck der personellen Datenerhebung nicht mehr gegeben ist – die verarbeitende Maßnahme also vollendet ist – müssen die Daten gelöscht werden und dürfen nicht ewig gespeichert werden.

Integrität und Vertraulichkeit: Daten dürfen nicht einfach weitergegeben und -verkauft werden. Dies ist kein genereller Ausschluss von der Weitergabe der Daten, denn sofern die DSGVO nicht verletzt wird, können Daten weitergegeben werden. Zudem müssen Daten so gespeichert werden, dass sie nicht unrechtmäßig verarbeitet, vor Unbefugten geschützt und nicht unbeabsichtigt zerstört werden. Der Datenverarbeitende, also das Unternehmen hat hierfür geeignete technische und organisatorische Maßnahmen zu treffen.

3.2 Welche neuen Rechte hat der Nutzer?

Informationsrecht: Sobald Daten über eine Person erhoben werden, muss diese gemäß Art.13 DSGVO über die Erhebung informiert werden. Einen Sonderfall gibt es nur, wenn der Betroffene bereits weiß, dass über ihn oder sie Daten erhoben worden sind.
Bei der Erhebung der Daten müssen folgende Daten dem Betroffenen offengelegt werden:

- Name und Kontaktdaten des Verantwortlichen (ggf. auch des Vertreters)
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zweck und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen (bei Verarbeitung nach Art. 6 DSGVO)
- Empfänger bzw. Kategorien von Empfängern
- Übermittlung in Drittland oder an internationale Organisation
- Dauer der Speicherung
- Bestehen eines Rechts auf Auskunft, Berichtigung, Löschung, Einschränkung, Widerspruch und auf Datenübertragbarkeit
- Bestehen eines Rechts auf Widerspruch der Einwilligung
- Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- Information, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist und mögliche Folgen der Nichtbereitstellung
- Information über eine mögliche Zweckänderung der Datenverarbeitung
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Das Profiling stellt eine Ausnahme dar, da die Daten nicht beim Betroffenen selbst generiert werden. Art. 14 DSGVO regelt diesen Sonderfall. Die DSGVO schreibt, dass bei Profiling der Betroffene darüber informiert werden muss, wo die Daten erhoben worden sind. Praktisch heißt dies: Wenn Datensätze über Profiling generiert werden, muss jeder dort enthaltenen Person mitgeteilt werden, welche Quelle den Daten zu Grunde liegt.

Auskunfsrecht: Dieses wird in Art. 15 DSGVO abgehandelt.

Inhaltlich ist das Auskunftsrecht fast deckungsgleich mit dem Informationsrecht, jedoch greift das Informationsrecht bei der Erhebung
der Daten und das Auskunftsrecht, wenn der Betroffene eine Auskunft wünscht.

Dem Betroffenen ist durch eine Kopie der personenbezogenen Daten auf gängigem Postweg (auch elektronisch) Auskunft zu erteilen. Die Frist der Auskunft beträgt maximal einen Monat. Zudem hat der Betroffene
das Recht, Auskunft in regelmäßigen zeitlichen Abständen einzufordern.

Mindestens folgende Informationen müssen Betroffenen mitgeteilt werden:

- Zwecke der Datenverarbeitung
- Kategorien der Daten
- Empfänger oder Kategorien von Empfängern
- Dauer der Speicherung
- Recht auf Berichtigung, Löschung und Widerspruch
- Beschwerderecht bei einer Aufsichtsbehörde
- Herkunft der Daten (wenn nicht bei Betroffenen erhoben)
- Übermittlung in Drittland oder an internationale Organisation
- Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Recht auf Berichtigung oder Löschung: Durch das informelle Selbstbestimmungsrecht der Betroffenen, ergibt sich das Recht auf Berichtigung und Löschung.

Art. 16 DSGVO besagt, dass der Betroffene das Recht hat, dass die über ihn erhobenen Daten ohne Verzögerung berichtigt werden müssen. Für Unternehmen bedeutet dies, dass Daten immer ad hoc und ohne Zeitverzug bearbeitet werden müssen. Hierfür bedarf es eines guten Datenmanagements, welches eine transparente Organisation hat. Art. 17 DSGVO definiert zudem, wann Daten gelöscht werden müssen. Dies ist immer dann der Fall, wenn:

- die Speicherung der Daten nicht mehr notwendig ist
- der Betroffene eine Löschung wünscht
- die Einwilligung zur Datenverarbeitung zurückgezogen wurde
- die Daten nicht rechtmäßig verarbeitet wurden
- Daten nach EU- oder nationalem Recht gelöscht werden müssen

Der für die Veröffentlichung der Daten Verantwortliche muss sicherstellen, dass der Datenverarbeitende die Anweisung zur Datenlöschung erhält, wenn der Nutzer dies wünscht. Zudem muss der Verantwortliche Maßnahmen treffen, dass die Löschung vollzogen werden kann.

Nach Art. 19 DSGVO hat der Verantwortliche allen Datenverarbeitenden unverzüglich mitzuteilen, wenn Daten berichtigt oder gelöscht werden. Es sei denn, dies ist unmöglich oder mit unverhältnismäßigem Aufwand verbunden.

Recht auf Datenübertragbarkeit: Die Betroffenen der Erhebung personenbezogener Daten haben das Recht, dass die von ihnen zur Verfügung gestellten Daten auf eine andere, zweckähnliche Anwendung eins zu eins übertragen werden können. Diesem Recht liegt die informationelle Selbstbestimmung zu Grunde. Diese Thematik wird in Art. 20 DSGVO beschrieben.

Das Ziel der Datenübertragbarkeit soll sein, dass bspw. Anbieterwechsel für den Kunden leichter gemacht und mit weniger Aufwand verbunden sein sollen.Auch hier muss das Unternehmen die Daten sorgfältig und wohl organisiert speichern, damit die Daten dem Kunden zum Anbieterwechsel einfach und ohne großen Aufwand bereitgestellt werden können.

3.3 Was sind die rechtlichen Pflichten der Unternehmen?

Grundsätzlich besteht die erste Pflicht für Unternehmen darin, die Verantwortlichkeit für die Verarbeitung der Daten zu klären. Denn nach Art. 24 DSGVO ist derjenige verantwortlich, der maßgeblich über die Verarbeitung von personenbezogenen Daten entscheidet. Dies kann eine natürliche oder juristische Person, Behörde oder Einrichtung sein. Hinzu kommen weitere Pflichten, welche beachtet werden müssen, um der neuen DSGVO gerecht zu werden.

Technischer Datenschutz: Der Datenverarbeitende hat geeignete technische und organisatorische Maßnahmen
zu treffen, um den technischen Datenschutz bestmöglich zu gewährleisten. Dies ist eine sehr schwammige Formulierung. Heute kann keine zweifelsfreie Aussage getroffen werden, was die Formulierung für praktische Implementierungen meint. Es bleibt abzuwarten, wie erste Urteile und Bußgelder in der Thematik ausgesprochen werden.

Wichtig ist jedoch: Das Unternehmen, das Daten verarbeitet, muss gemäß Art. 24 DSGVO in der Auswahl der geeigneten technischen und organisatorischen Maßnahmen die Art, den Umfang und den Zweck der Speicherung berücksichtigen. Dies impliziert die Risiken für die persönliche informationelle Freiheit und Rechte. Für die Praxis bedeutet dies: je sensibler die gespeicherten Daten sind und je größer die quantitative Speicherung ist, desto sicherere technische und mehr organisatorische Maßnahmen müssen getroffen werden. Es gilt das Vorsorgeprinzip.

Zudem muss ein Unternehmen eine interne Strategie festlegen, die die langfristige Auswahl an Datenschutzmaßnahmen beinhaltet. Hier kommt der Grundsatz „Datenschutz durch Technik" zur Geltung. Denn die Strategie muss dem genannten Grundsatz entsprechen. Dies beinhaltet folgende datenschutzfreundliche Voreinstellungen:

- Minimiertes Bearbeiten von personenbezogenen und u.U eine Pseudonymisierung der Daten
- Transparenz der Datenverarbeitung
- Der Betroffene hat die Möglichkeit die getroffenen Maßnahmen zu überwachen
- Der Mitarbeiter, der die Daten verarbeitet, und somit praktisch am meisten mit den Daten zu tun hat, hat die Möglichkeit Sicherheitsfunktionen zu verbessern und zu implementieren

„Wer bislang noch keine Maßnahmen ergriffen hat, seine Server technisch konform abzusichern, sollte dies schnellstens nachholen..."

(Michael Prothmann, CEO von MPCG)

Meldepflicht: Bei der Meldepflicht handelt es sich um eine Pflicht, die im Notfall vorgeschrieben ist. Um einen Notfall im datenschutzrechtlichen Sinne handelt es sich, wenn der Datenschutz verletzt wurde. Ist dies der Fall, muss das Unternehmen, welches Opfer oder verantwortlich für die Verletzung des Datenschutzes ist, nach Art. 33 DSGVO sofort eine Meldung an die zuständige Datenschutzaufsichtsbehörde geben. Eine Ausnahme gibt es nur, wenn durch diese Meldung ein Risiko für Rechte oder Freiheiten von natürlichen Personen besteht. Die Meldung muss unmittelbar erfolgen – maximal 72 Stunden nach dem Verstoß gegen den Datenschutz.

Art. 34 DSGVO schreibt vor, dass neben der Datenschutzaufsichtsbehörde auch alle Betroffenen informiert werden müssen, dass der Datenschutz ihrer personenbezogenen Daten verletzt worden ist. Eine Ausnahme gibt es auch hier. Der Betroffene muss nur dann informiert werden, wenn:

- Die Daten nicht verschlüsselt sind und somit von unbefugten Dritten „verstanden" werden können
- Durch die Verletzung des Datenschutzes kein hohes Risiko für die natürliche Person besteht

Sofern die rechtlichen Ausnahmen nicht greifen und der Betroffene informiert werden muss, muss er inhaltlich über die Art der Verletzung des Datenschutzes informiert werden.

Datenschutz Folgeabschätzungen: Diese muss nach Art. 35 DSGVO gemacht werden, wenn:

- neue technische und organisatorische Maßnahmen getroffen werden, die dem Datenschutz dienen und so unmittelbar mit dem Datenschutz in Verbindung stehen
- ein besonders hohes Risiko aus datenschutzrechtlicher Sicht besteht

Diese Datenschutzfolgeabschätzung enthält eine systematisch und allumfassende Bewertung aller Maßnahmen, die aufgrund einer automatisierten Datenverarbeitung anfallen. Dies beinhaltet das Identifizieren aller möglichen Risiken und einer Abschätzung, wenn ein identifiziertes Risiko praktische Realität wird.

Zudem muss die Datenschutzfolgeabschätzung immer dann gemacht werden, wenn es sich um besondere personenbezogene Daten handelt. Dies sind bspw. Daten über strafrechtliche Verurteilungen oder begangene Straftaten. Auch Sicherheitsdienstleister, die für den Staat arbeiten, müssen die Folgeabschätzung durchführen, wenn sie systematisch und weiträumig öffentlich zugängliche Bereiche überwachen.

4. Zehn Änderungen für Marketing und Vertrieb

Die meisten aktuellen Whitepaper und Angebote rund um das Thema DSGVO betrachten das Thema Datenschutz und die sich ergebenden Änderungen oftmals aus einer organisatorischen Sicht sowie unter Gesichtspunkten der rechtlichen Folgenabschätzung. Wir geben Ihnen einen konkreten Überblick über die Änderungen in Ihrem Unternehmen bezogen auf Marketing und Vertrieb.

1 Gelten meine altern Verträge mit Partnern?

Bislang musste auf nationaler Ebene eine Vereinbarung zur Auftragsdatenverarbeitung mit Dienstleistern abgeschlossen werden, sobald eine Zugriffsmöglichkeit auf personenbezogene Daten nicht ausgeschlossen werden kann. Da die DSGVO als europäische Verordnung in allen Mitgliedstaaten Anwendung findet, steht sie über nationalen Regelungen. Das heißt, die Verträge müssen in dem Zuge alle zumindest überprüft werden.

Standardvertragsklauseln liegen hier noch nicht vor, da es noch keine allgemeingültige Rechtsprechung gibt, jedoch bieten frei zugängliche Muster Orientierung. Insbesondere Wartungsarbeiten an Systemen oder Servern sind hiervon betroffen. Ein Dienstleistungsvertrag legt die Art und den Umfang von Wartungsarbeiten fest, einschließlich der jeweiligen Auslöser von Wartungsaktivitäten. Zudem müssen Informationswege zur Bestellung, die Durchführung und Abrechnung der Wartung sowie die Protokollierung der Wartungsaktivitäten klar ausgezeichnet werden.

Eine Vertraulichkeitsvereinbarung ist unerlässlich und sollte alle Arten von Daten miteinschließen. Hierzu sollten Sie bereits jetzt ein Team bestimmen, dass die Aktualisierung der Verträge inhaltlich vorbereitet.

2 Was ändert sich in der Zusammenarbeit mit Partnern?

Bei der Auswahl von Dienstleistern und Partnern ist es wichtig, dass auch diese datenschutzkonform nach der neuen DSGVO aufgestellt sind. Dies umfasst Partner/Dienstleister, die direkt oder indirekt an der internen Auftrags-verarbeitung beteiligt sind, z.B. Lohnbuchhaltung in der Cloud, Managed Hosting, E-Mail-Marketing in der Cloud, CRM in der Cloud, Google Analytics, Schreibbüros, Übersetzungsdienste, Externe Call-Center, Anrufdienste usw. Wichtig für den Auftragnehmer ist, dass dieser nun auch haftet bei eigenem Verstoß gegen die DSGVO. Daraus ergeben sich neue Pflichten:

- Umfangreichere Dokumentationspflicht
- Führen von Verfahrensverzeichnissen
- Umsetzung technischer und organisatorischer Maßnahmen zur Datensicherheit
- Position des Datenschutzbeauftragten
- Zusammenarbeit mit Aufsichtsbehörde
- Meldepflicht bei Datenpanne
- Datentransfers in Drittland nur im Rahmen DSVGO
- Einhaltung der Mitarbeiterverschwiegenheit

Zudem müssen Sie auch darauf achten, dass die Mitarbeiter bei Partnern entsprechend geschult werden, wenn sie mit Daten zu tun haben. Denn sonst werden Vorgaben der Verordnung verletzt und es droht ein Bußgeld.

3 Welche Neuerungen ergeben sich für interne Organisationen?

Aus der DSGVO ergeben sich auch direkte Anforderungen an die Organisation eines Unternehmens. Beweggrund ist, dass die Gesetzgeber gewährleisten wollen, dass das Thema Datenschutz auch die gebührende Aufmerksamkeit erhält und organisatorisch keine Hemmnisse bestehen, die eine reibungslose Umsetzung der DSGVO behindern. Es muss prozessual gewährleistet sein, dass sämtliche Pflichten ordnungsgemäß terminlich erfüllt werden. Zum Beispiel müssen informationelle Anfragen von Nutzern innerhalb eines Monats bearbeitet werden. Bei Verzögerung müssen entsprechende Gründe genannt werden und bei Nicht-Tätigwerden müssen ebenso Gründe genannt sowie die Möglichkeit gegeben werden, Aufsichtsbeschwerde gegen einen selbst einzulegen.

Für die meisten Unternehmen ist es nicht neu, aber durch die DSGVO wird es zur Pflicht, einen Datenschutzbeauftragten zu benennen und entsprechend zu schulen und zu befähigen. Ebenfalls müssen sämtliche datenverarbeitende Mitarbeiter geschult werden, am besten vom Datenschutzbeauftragten. Davon betroffen ist
jedes Unternehmen mit mehr als zehn Mitarbeitern, die Daten verarbeiten. Grundsätzlich ist es zulässig auch einen externen Datenschutzbeauftragten zu benennen, denn einen eigenen zu finden ist oft nicht leicht, da dieser persönlich haftbar gemacht werden kann. Mitarbeiter sind ferner angehalten, sämtliche datenschutzrelevanten Vorfälle an den entsprechenden Beauftragten zu melden. Hierunter fallen z.B.:

- Beschwerden von Betroffenen (Mitarbeitern, Kunden)
- Einführung eines neuen Systems/Tools
- Einsatz eines neuen Dienstleisters
- Neue Werbemaßnahmen (z.B. Versand von Newsletter)
- Online-Marketing-Maßnahmen (Google AdWords, Conversion Tracking, etc.)
- Verkauf von Teilen des Unternehmens

4 Können Leads weiterhin so generiert werden wie bisher?

Grundsätzlich gilt, dass bezogen auf die Leadgenerierung bereits verhältnismäßig strenge Auflagen durch das TMG (Telemediengesetz), TKG (Telekommunikationsgesetz) und BDSG (Bundesdatenschutzgesetz) in Deutschland Geltung finden. Daten dürfen auch jetzt schon nur mit der persönlichen Einwilligung gespeichert werden. Zudem müssen Kunden darüber informiert werden, welche Daten zu welchem Zweck erhoben werden und wenn bspw. Daten an Drittländer übermittelt werden. Ein Hinweis auf die Beschwerdemöglichkeiten ist unerlässlich.

Diese Maßgaben werden sich durch die neue DSGVO nicht ändern. Neu sind jedoch die schärferen Kontrollen sowie die damit verbundenen Bußgelder. Unternehmen, die sich bislang nicht datenschutzkonform zeigen, z.B.
IP-Adressen nicht anonymisieren, sollten sich den drohenden Sanktionen bei Nichteinhaltung bewusst sein. Datenschutz und Transparenz wird zum Hygienefaktor bei den Nutzern und sollte viel-

5 Dürfen vorhandene Daten für E-Mail-Marketing (Newsletter) genutzt werden?

E-Mail-Marketing ist für Unternehmen eines der effektivsten Instrumente, um Kunden zu erreichen und nachhaltig zu binden. Grundsätzlich gilt hier bereits heute: Es ist nichts erlaubt, was nicht ausdrücklich genehmigt wurde. Da bei dieser Form des Marketings durch Kontaktdaten ein direkter Personenbezug hergestellt werden kann, werden Verstöße bereits jetzt schon entsprechend geahndet, etwa durch Abmahnungen. Rechtlich gilt der Versand eines Newsletters an Personen, die vorher keine Einwilligung zum Empfang erteilt haben, sogar als unzumutbare Belästigung und verstößt somit gegen das Wettbewerbsrecht § 7 Abs. 3 UWG. Das heißt, nicht nur Ihre Kunden, sondern auch Ihre Mitbewerber können Ansprüche bei Verstoß gegen diese Normen geltend machen.

Auch Messenger-Dienste werden rechtlich wie E-Mail-Marketing behandelt. Die einzige Ausnahme greift dann, wenn bereits eine Kundenbeziehung besteht und dem Adressaten Informationen im Kontext zu bereits abgesetzten Produkten/Dienstleistungen elektronisch zugesandt werden. D.h. konkret, die Werbung muss zum bereits gekauften Produkt passen und es darf vorher keine Abmeldung zugegangen sein. Auch hier gilt es zu beachten, dass Kunden stets auf die Möglichkeit zum Widerspruch hingewiesen werden.

Wollen Sie sich rechtssicher aufstellen, ist das Double-Opt-In-Verfahren das probate Mittel, um belegen zu können, dass eine Einwilligung des Kunden vorliegt. Hier muss der Empfänger einer Werbemail nach der Eintragung seiner E-Mail-Adresse und ggf. sonstiger Daten seine Einwilligung durch Anklicken eines Links in der Bestätigungsmail nochmals ausdrücklich bestätigen. Erfolgt keine Reaktion, gilt dies als Ablehnung.

Für sich genommen reguliert die DSGVO die Ausnahmeregelungen nicht so streng wie nationale Gesetze. Voraussetzung für den Versand von Mitteilungen ohne Einwilligung ist lediglich, dass ein „berechtigtes Interesse“ vorliegen muss. Näher ist dies jedoch nicht definiert. Auf Deutschland bezogen wird die DSGVO die nationale Gesetzgebung in dem Punkt nicht ersetzen, sondern nur ergänzen. Das heißt, die momentanen Regelungen bleiben in der jetzigen Form erhalten. Auch hier gilt es jedoch zu beachten, dass durch die stärkeren Kontrollen und höher ausfallenden Sanktionen ein Verstoß gegen geltendes Recht nicht ratsam ist.

In Konsequenz bedeutet dies, dass bereits generierte Daten auch unter der DSGVO entsprechend genutzt werden dürfen, sofern sie den jetzigen Standards entsprechen. Falls dies nicht der Fall ist, müssen diese spätestens bis zum 25.05.2018 nachweislich gelöscht werden.

6 Darf Google-Analytics genutzt werden wie bisher?

Der Einsatz von Google Analytics verbunden mit der Nutzung von Cookies ist aus datenschutzrechtlichen Gründen sehr heikel. Denn zum einen werden die gesammelten Daten mit den USA ausgetauscht. Datenschützer und Google haben hierfür jedoch entsprechende Vereinbarungen getroffen. Zum anderen werden mit der DSGVO die Bußgelder für Verstöße gegen Datenschutzregeln steigen. Auch hier muss man sich in Bezug auf die aktuell geltenden Normen versichern, dass diese rechtskonform umgesetzt werden. Diese werden mit Inkrafttreten der DSGVO in der jetzigen Form Gültigkeit behalten.

Für Google Analytics sind bereits folgende drei Punkte wichtig bzw. vorgeschrieben:

1. Aktivierung der DoNotTrack-Funktion per default
2. IP-Anonymisierung ebenfalls per default (muss manuell aktiviert werden)
3. Verweis auf Cookie-Nutzung entweder durch Google Analytics Add-On oder Opt-out-Cookie

7 Dürfen generierte Daten weiterhin für das Profiling genutzt werden?

Das Profiling wird im Gegensatz zum Tracking genauestens in Art. 4 Nr. 3 DSGVO thematisiert. Denn aus Sicht des Gesetzgebers geht das Profiling weit über das Tracking hinaus. Denn beim Profiling werden verschiedenste Daten gesammelt und einer Person zugeordnet, es entsteht ein Datenprofil. Es werden diverse Daten so verarbeitet, dass sie einem genauen Profil aggregiert zugeordnet werden können.

Durch Erwägungsgrund 60 DSGVO wird ersichtlich, dass das Profiling eine verarbeitende Handlung personenbezogener Daten ist, die die Lebenswirklichkeit des Nutzers tangiert. Da die Verarbeitung jedoch keinen rechtlichen Einfluss auf den Nutzer hat, darf dies vernachlässigt werden. Dem Nutzer werden bloß Anzeigen und Werbeinhalte geschaltet, der Einfluss auf das reale Leben ist somit marginal. Zudem wird der Betroffene des Profilings nicht in seiner Lebensweise und -qualität beeinträchtigt. Durch die fehlende rechtliche Beeinträchtigung findet Art. 22 DSGVO keine Anwendung.

Art. 6 Art. 1 f) findet aus den oben genannten Gründen Anwendung. Das heißt, dass Profiling grundsätzlich möglich ist. Jedoch muss von Seiten des Datenverarbeitenden genauestens abgewogen werden: überwiegt das eigene Interesse oder das Interesse des Betroffenen, dass die Daten über ihn in seiner Datenfreiheit, seinen Interessen oder sonstigen Gründen negativ beeinflussen.

Der Betroffene muss, wie bei anderen Online-Marketing-Maßnahmen auch, über das Profiling informiert werden. Besondere Bedeutung kommt dem Widerspruchsrecht zu. Denn das Widerspruchsrecht steht über allem. Bei allen Profiling-Maßnahmen muss der Betroffene darüber informiert werden, dass er jederzeit das Recht auf Widerspruch gegen die Maßnahme hat. Der Betroffene ist bei der ersten Kontaktaufnahme gesondert, verständlich und von anderen Informationen getrennt darüber zu informieren. Das Recht auf Widerspruch ist unentgeltlich zu leisten. Das Profiling bleibt also weiterhin erlaubt.

8 Was ändert sich in Bezug auf Tracking und der technischen Nutzung von Cookies?

Bis die DSGVO am 25. Mai 2018 Anwendung findet, ist das Tracking rechtlich genau definiert. Welche neuen Regeln nach dem Stichtag greifen werden, sind noch nicht genau geklärt, denn die DSGVO erwähnt das Tracking nicht explizit. Jedoch lässt sich über das Verarbeiten von Daten folgern, dass Art. 4 Abs. 2 DSGVO Anwendung findet. Der regelt, dass es einem Zweck bedarf, der das Tracking genehmigt. Hier kann das Werbeinteresse als Grund angeführt werden, der auch ausreichend ist, jedoch im Einzelfall geprüft werden muss. Ein Online-Shop, der Cookies einsetzt, um eine Verbesserung der User-Experience zu bewirken, wie z.B. durch eine Merklistenfunktion, hat weiterhin ein berechtigtes Interesse am Tracking. Bedingung für den Einsatz solcher Cookies ist jedoch stets die Anonymisierung und korrekte Verschlüsselung der Daten.

Um das wichtige Thema Tracking konkreter zu fassen, wird aktuell ergänzend die e-Privacy-Verordnung erarbeitet. Diese soll analog zur DSGVO verabschiedet werden. Bisher in Deutschland geltende Regelungen, in denen ein Opt-Out für Cookies ausreicht, werden in Zukunft im Hinblick auf die neue Verordnung nicht mehr datenschutz-konform sein. Dies bedeutet, bislang reichte es aus, wenn Nutzern die Möglichkeit gegeben wurde, dem Einsatz von Cookies zu widersprechen. In Zukunft muss der Nutzer dem Einsatz aktiv zustimmen. Opt-Out wird zu Opt-In. Diese Änderung hat Folgen für alle im Online-Marketing eingesetzten Werbe- und Analysetools wie Google Analytics, Facebook, LinkedIn, Hotjar etc.

Den Betroffenen muss ferner mitgeteilt werden, was der Zweck des Trackings ist, z.B. Analyse oder Werbemaßnahmen. Die generelle Erfassung anonymer Daten wie die Zahl der Websiteaufrufe, bleibt davon unberührt. Für Marketer sind diese Angaben jedoch wenig aussagekräftig, so dass Möglichkeiten gesucht werden müssen, möglichst viele Nutzer dazu zu bewegen, aktiv dem Einsatz von Cookies zuzustimmen.

Browserhersteller werden bereits jetzt in die Pflicht genommen. Diese müssen dafür Sorge tragen, dass bis zur Einführung der Verordnung Do-Not-Track-Signale in den Browsereinstellungen als automatisierter Widerspruch gewertet werden.

Doch auch als Websitebetreiber sollte man sich frühzeitig mit dem erlaubten Einsatz von Cookies auseinandersetzen, um auch in Zukunft wertvolle Daten generieren zu dürfen. Datenschutzkonform wäre z.B. ein Hinweis, der dem Nutzer gezielt die Wahl lässt, welche Cookies er zulässt, etwa lediglich Analyse-Cookies oder auch Cookies von anderen Plattformen. Verstößt man auch nichtwissend gegen die neuen Regelungen, werden ähnlich wie bei DSGVO auch bei der e-Privacy-Verordnung Bußgelder verhängt. Die Höhe der Bußgelder ist bei Verstößen noch nicht abschließend national geregelt. Es ist jedoch davon auszugehen, dass man sich bei der e-Privacy-Verordnung an den Regelungen der DSGVO orientieren wird.

9 Wo dürfen Daten gespeichert werden? Welche Besonderheiten gelten für die USA?

Daten dürfen nicht überall gespeichert werden, jedoch gibt es Ausnahmen. Zudem gibt es für einzelne Nationen Besonderheiten, die aus dem Umgang dieser Länder mit dem Datenschutz resultieren. So gibt es mit den USA ein Abkommen, das „Privacy Shield" heißt. Dieses Abkommen ist seit 2016 in Kraft. Für Server in den USA gilt: Es darf nur mit Unternehmen zusammengearbeitet werden, die auf der Liste stehen, ergo eine Zertifizierung erbracht haben. Das Abkommen bleibt auch bestehen, wenn die DSGVO greift. Sobald die Standardvertragsklauseln bestehen, werden diese je nach Formulierung und Inhalt das Privacy Shield in Frage stellen.

Es gilt weiterhin, dass Datentransfers von personenbezogenen Daten nicht gewollt sind. Denn die EU geht davon aus, dass das Datenschutzniveau in Drittstaaten nicht mit dem in der EU vergleichbar ist. Jedoch gibt es, wie im Privacy Shield, Ausnahmen, die für einzelne Ländern gelten, wenn die EU in dem entsprechenden Land einen ausreichenden Datenschutz festgestellt hat. Dann dürfen die Daten in das entsprechende Land transferiert werden.
Durch die DSGVO ändert sich insofern praktisch nichts. Genau wie bisher müssen Unternehmen, wenn sie Daten ins Ausland transferieren wollen, prüfen, ob das Land den Datenschutzanforderungen der EU entspricht.

10 Was passiert, wenn gegen die DSGVO verstoßen wird?

In Vergleich zu den Strafen und Bußgeldern, die bei Verstößen gegen die DSGVO auf Sie zukommen, fallen die Bußgelder bislang nach deutscher Rechtsprechung milde aus. Bei einer fehlenden Einwilligung hinsichtlich der E-Mail-Marketing-Maßnahmen z.B. drohen aktuell noch Bußgelder bis zu 300.000 Euro. Verstoßen Sie in Zukunft gegen die DSGVO, fallen Strafzahlungen bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres an. Bußgeldmindernde Faktoren wie ein prozessual effektiv eingebundenes Datenschutzmanagement fallen dann ins Gewicht. Zumal durch solche Maßnahmen die schnelle Reaktionsgeschwindigkeit in Fällen von Verstößen gewährleistet wird.

5. Unsere Empfehlung für Sie

Die Datenschutzgrundverordnung, die am 25. Mai 2018 in Kraft tritt, betrifft alle Unternehmen und hat Einfluss auf die gesamte Organisation in Hinblick auf Prozesse und Compliance. Jede Abteilung und jeder Mitarbeiter, der mit Daten in Berührung kommt, muss informiert und sensibilisiert werden. Dies kann und muss durch interne oder externe Schulungen umgesetzt werden.

Noch hat jedes Unternehmen Zeit, alle notwendigen Maßnahmen einzuleiten und umzusetzen, da jedoch unter Umständen organisatorische Änderungen implementiert werden müssen, sollte frühzeitig mit der Überprüfung der eigenen Richtlinien begonnen werden. Dies erledigen Sie nicht über Nacht oder in wenigen Wochen. Die Bußgelder bei Verstößen erhöhen sich ab dem Stichtag empfindlich, sofern Sie nicht rechtzeitig agiert haben.

Neben den organisatorischen Änderungen, wie z.B. der Erfordernis von internen oder externen Datenschutzbeauftragten, ergeben sich vor allem operativ für die Marketing-Abteilungen und Ihre Online-Präsenz neue Anforderungen, die es technisch und organisatorisch zu beachten gibt. Schon die Nichtbeachtung der neuen Regelungen in Bezug auf Cookies und Trackings stellen mögliche Wettbewerbsverstöße dar. Die bisherige Webanalyse und Datenverarbeitung ist in den meisten Fällen nicht mehr datenschutzkonform. Im Grunde müssen alle Online-Aktivitäten mitsamt allen Dienstleistern auf den Prüfstand gestellt werden.

Unsere Leistungen, die wir Ihnen in Hinblick auf die DSGVO bieten, umfassen die Prüfung Ihrer Organisation und Ihrer technischen Systemlandschaft. Sollten Sie gezwungen sein, Änderungen in Prozessen oder Ihrer Organisation vorzunehmen, so begleiten wir Sie – beratend als auch praktisch umsetzend.

In einen Check-up Ihrer technischen Datenschutzmaßnahmen prüfen wir, ob diese auf dem neuesten technischen Stand sind, so wie es die DSGVO fordert. Insbesondere Cookie-Einstellungen werden angepasst werden müssen, denn das bisher gängige Opt-In-Verfahren wird mit dem Stichtag nicht mehr ausreichend sein. Hierzu bieten wir Ihnen eine leicht zu implementierende Lösung, mit der Sie rechtlich geprüft datenschutzkonform online agieren.

Zudem können wir Sie neben einer Prüfung Ihrer internen Organisationsstruktur auch bei einer Prüfung Ihrer Dienstleister unterstützen, die an der Verarbeitung personenbezogener Daten direkt oder auch nur indirekt beteiligt sind. Denn Sie sind nach den neuen Regelungen dafür verantwortlich, dass die Auswahl der Dienstleister den Erfordernissen der DSGVO entspricht. Verstoßen Ihre Dienstleister gegen etwaige Anforderungen, müssen Verträge spätestens bis zum Stichtag aufgelöst werden.

Schreiben Sie uns eine Nachricht an Info@mpcg.de und wir stellen Ihnen in einem unverbindlichen Gespräch die Möglichkeiten eines Check-Ups vor.