OWM WHITEPAPER

Die EU-Datenschutz-Grundverordnung

Auswirkungen und Praxishinweise für Marketing und Werbung

in Kooperation mit DLA PIPER

Die Datenschutz-Grundverordnung

Auswirkungen und Praxishinweise für Marketing und Werbung

Stand: 27. Februar 2018

Inhaltsübersicht

1. Einleitung

1.1 Der Rechtsrahmen

Datenschutzrecht und Marketing bildeten schon immer ein Spannungsfeld. Der deutsche Gesetzgeber hat – europaweit einzigartig – im bisherigen Datenschutzrecht besonders detaillierte Beschränkungen für die Verarbeitung von Daten zu werblichen Zwecken vorgesehen.

Das deutsche Datenschutzrecht wird ab dem 25. Mai 2018 allerdings durch die **Datenschutz-Grundverordnung (DSGVO)** ersetzt. Diese gilt unmittelbar in allen EU-Mitgliedstaaten. Zusätzliche nationale datenschutzrechtliche Regelungen sind dann nur noch in Ausnahmefällen zulässig. Eine Ausnahme für nationale Beschränkungen speziell für die Verarbeitung von Daten für Werbung und Marketing ist dabei nicht vorgesehen. Konsequenterweise enthält daher auch das **neue Bundesdatenschutzgesetz** (BDSG-neu), welches das bisherige Bundesdatenschutzgesetz zum 25. Mai 2018 ablöst, keine spezifischen Regelungen für Werbung und Marketing mehr.

Beschränkungen für Marketing und Werbung ergeben sich allerdings zusätzlich aus wettbewerbsrechtlichen Vorgaben. Besonders hervorzuheben sind hierbei die Beschränkungen für Telefon- und E-Mail-Marketing in § 7 des Gesetzes gegen den unlauteren Wettbewerb (UWG). Diese beruhen im Kern auf Vorgaben aus der sogenannten e-Privacy-Richtlinie.

Der Gesetzgeber hat es leider versäumt, das Verhältnis von DSGVO und e-Privacy-Richtlinie eindeutig zu klären. Aus dem aktuell auf europäischer Ebene verhandelten **Entwurf** einer **e-Privacy-Verordnung** (die zukünftig ebenfalls EU-weit unmittelbar gelten soll) ergibt sich aber, dass Telefon- und E-Mail-Marketing nach dem Willen des EU-Gesetzgebers – wie schon im bisherigen deutschen Recht – grundsätzlich nur mit voriger Einwilligung möglich sein soll. Die Organisation Werbungtreibende im Markenverband (OWM) empfiehlt ihren Mitgliedern daher, die Vorgaben des § 7 UWG auch unter der DSGVO unbedingt weiter zu beachten.

1.2 Unser Whitepaper zur Datenschutz-Grundverordnung

Die DSGVO verändert die Rahmenbedingungen für Marketingmaßnahmen und Werbung. In unserem vorliegenden Whitepaper stellen wir Ihnen diese überblicksartig dar und geben Hinweise für die Praxis.

Dabei wird in Abschnitt 2 zunächst behandelt, wann die DSGVO Anwendung findet, bevor in Abschnitt 3 dargestellt wird, unter welchen Voraussetzungen personenbezogene Daten verarbeitet werden dürfen. Die letzten Monate haben gezeigt, dass unsere Mitglieder eine Vielzahl von Fragen zur DSGVO haben. Einen Teil dieser Fragen möchten wir Ihnen in Abschnitt 4 in kurzen und verständlichen Worten beantworten. Abschnitt 5 bietet dem interessierten Leser weiterführende Links auf Angebote, die zusätzliche Informationen zur Datenschutz-Grundverordnung enthalten. Im Anhang zu diesem Whitepaper finden Sie Auszüge aus den einschlägigen Gesetzen.

Bitte beachten Sie: Dieses Whitepaper kann nur einen ersten Überblick liefern. Sie ersetzt weder eine sorgfältige Vorbereitung auf die DSGVO noch eine rechtliche Prüfung der Verarbeitungsprozesse in Ihrem Unternehmen.

2. Wann gilt die Datenschutz-Grundverordnung?

Die DSGVO findet Anwendung auf Unternehmen, die ihren Sitz in der EU haben oder die Daten von EU-Bürgern verarbeiten. Entscheidend ist hierbei, dass personenbezogene Daten automatisiert verarbeitet werden. Dies ist bei Marketing nicht immer der Fall.

2.1 Wann liegen personenbezogene Daten vor?

Personenbezogene Daten sind Informationen, die sich auf eine „*identifizierte* oder *identifizierbare*" natürliche Person beziehen. Dies ist weit auszulegen. So hat der Europäische Gerichtshof zum Beispiel entschieden, dass IP-Adressen für Websitebetreiber schon allein dann Personenbezug aufweisen können, wenn diese die theoretische Möglichkeit haben, im Falle eines strafrechtlichen Ermittlungsverfahrens über ihr Akteneinsichtsrecht den Namen des Anschlussinhabers zu erfahren.

Werden bloß **anonyme Daten** verarbeitet, ist das Datenschutzrecht nicht anwendbar. Dabei ist im Einzelfall sorgfältig zu prüfen, ob Daten tatsächlich anonym sind. Dies ist grundsätzlich nur der Fall, wenn keine Mittel zur Verfügung stehen, die Daten einer natürlichen Person zuzuordnen. Auch angesichts der heute zur Verfügung stehenden technischen Möglichkeiten ist dies nur selten gegeben.

Wenn Daten so gespeichert sind, dass eine Identifizierung nur mit Hilfe von Zusatzinformationen möglich ist und diese Zusatzinformationen gesondert aufbewahrt werden, handelt es sich um **pseudonyme Daten**. Dies sind nach wie vor personenbezogene Daten. Eine solche „*Pseudonymisierung*" verringert allerdings die datenschutzrechtlichen Risiken und ist daher ein wichtiger Baustein bei der Einhaltung des Datenschutzes.

Praxisbeispiele

1. In dem Datensatz zu einer Person, der Werbung per E-Mail gesendet werden soll, sind Angaben wie Name, postalische Anschrift und Ort, E-Mailadresse und Telefonnummer hinterlegt.
   Es handelt sich um die Daten einer identifizierten Person und somit um personenbezogene Daten. Selbst die E-Mail-Adresse einer Person ohne weitere Angaben stellt ein personenbezogenes Datum dar.

2. In dem Datensatz zu einer Person, der für eine statistische Analyse abgelegt wird, sind der Name, die postalische Anschrift, E-Mailadresse und Telefonnummer durch Platzhalter ersetzt, lediglich der Ort und die gekaufte Warengruppe ist weiterhin im Klartext vorhanden.
   Es handelt sich um anonyme Daten, denn die ursprüngliche Person ist auch rein theoretisch nicht mehr zu identifizieren. Diese Bewertung kann anders ausfallen, wenn in dem Datensatz weitere Informationen enthalten sind, die noch immer einen Rückschluss auf eine Person zulassen (z. B. deren Bestellhistorie).

3. In einem Online-Shop wird personalisierte Werbung ausgespielt. Hierfür werden Kunden anhand von bisherigen Bestellungen und ihrem sonstigen Nutzungsverhalten in bestimmte Interessengruppen eingeteilt. Die Identifizierung der Kunden erfolgt über einen Identifier, der in einem Cookie auf dem Endgerät des Kunden abgelegt wird. Für die Werbeausspielung wird über eine Tabelle ermittelt, welche Interessen für diesen Identifier hinterlegt wurden.
   Der im Cookie gespeicherte Identifier ist ein Pseudonym. Auch der Abgleich

mit der Tabelle stellt eine pseudonyme Datenverarbeitung dar. Es handelt sich insofern um eine Verarbeitung personenbezogener Daten.

4. Ein Unternehmen kauft soziodemografische Informationen ein (z. B. zur Kaufkraft oder Altersgruppe).
   Die soziodemografischen Informationen sind grundsätzlich anonyme Daten. Sobald das Unternehmen diese Informationen allerdings einem bestimmten Kundendatensatz zuordnet (z. B. über die Anschrift), werden auch diese zu Informationen über eine identifizierte Person und damit zu personenbezogenen Daten.

2.2 Wann liegt eine Verarbeitung personenbezogener Daten vor?

Jeder Umgang mit personenbezogenen Daten stellt eine Verarbeitung im Sinne der DSGVO dar. Auch das Erheben von Daten – beispielsweise im Rahmen eines Kontaktformulars oder einer Bestellung – ist eine Verarbeitung von personenbezogenen Daten. Dasselbe gilt für sämtliche ggf. nachfolgenden Vorgänge wie etwa deren Analyse sowie Selektion und Nutzung für eine Werbeaussendung.

Dabei muss allerdings zwischen den verschiedenen Beteiligten differenziert werden. Wer über die Zwecke und Mittel der Verarbeitung bestimmt, ist **Verantwortlicher**, wer Daten nur weisungsabhängig im Auftrag verarbeitet, sogenannter **Auftragsverarbeiter** (zur Auftragsverarbeitung siehe auch unter 3.6).

Praxisbeispiele

1. Ein Unternehmen mit zahlreichen Kundendaten bietet diese anderen Unternehmen zur werblichen Nutzung an. Ein Werbetreibender macht hiervon Gebrauch. Das Unternehmen selektiert seine Kundendaten nach den Vorgaben des Werbetreibenden und sendet den ausgewählten Adressaten entweder selbst oder mit Unterstützung eines Lettershops Mailings.
   In diesem Beispiel verarbeitet nur das Unternehmen als Verantwortlicher (und ggf. der Lettershop als dessen Auftragsverarbeiter) personenbezogene Daten, aber nicht der Werbetreibende. Dasselbe gilt, wenn der Werbetreibende lediglich Online-Werbeflächen einkauft, die Auswahl der Adressaten und Aussteuerung der Werbung aber Dritte übernehmen.

2. Wie Beispiel 1, aber der Werbetreibende möchte, dass nur Werbung an Neukunden versandt wird. Ein Lettershop erhält daher nicht nur die Liste der potentiellen Adressaten vom Unternehmen, sondern zusätzlich vom Werbetreibenden eine Liste mit dessen Bestandskunden zum Abgleich.
   In diesem Beispiel verarbeiten beide, das Unternehmen und der Werbetreibende, ihre jeweiligen Kundendaten als Verantwortliche. Der Lettershop führt den Abgleich der Listen im Auftrag beider durch und nutzt die „gewaschene" Adressatenliste im Auftrag des Unternehmens für die Werbeaussendungen.

3. Die Datenschutz-Grundverordnung und Werbung – Voraussetzungen für eine zulässige Verarbeitung

3.1 Die Grundsätze für die Verarbeitung personenbezogener Daten

Bei jeder Verarbeitung personenbezogener Daten müssen Verantwortliche die Datenschutzgrundsätze nach Art. 5 DSGVO beachten. Hierbei handelt es sich – vereinfacht dargestellt – um folgende Grundsätze:

- Rechtmäßigkeit (jede Verarbeitung bedarf einer Erlaubnis),

- Transparenz (betroffene Personen, also etwa Kunden und Interessenten, müssen detailliert über die Verarbeitung ihrer Daten informiert werden),

- Zweckbindung (die Daten dürfen nur für festgelegte, eindeutige Zwecke verarbeitet werden, jede Zweckänderung erfordert eine Prüfung, ob die weiteren Zwecke mit den ursprünglichen kompatibel sind),

- Datenminimierung (die Daten dürfen nur in einer dem Zweck angemessenen sowie im hierfür notwendigen Umfang verarbeitet werden, ggf. müssen sie z. B. pseudonymisiert, also unter einer Kennziffer gespeichert werden),

- Richtigkeit (die Daten müssen sachlich richtig sein, unrichtige Daten berichtigt oder gelöscht werden),

- Speicherbegrenzung (die Daten dürfen nur solange personenbezogen gespeichert werden, wie dies für die festgelegten Zwecke erforderlich ist) und

- Integrität und Vertraulichkeit (die Daten müssen unter Einsatz angemessener Sicherheitsmaßnahmen verarbeitet werden).

Verantwortliche sind für die Einhaltung der Datenschutzgrundsätze nicht nur verantwortlich, sondern müssen **die Einhaltung auch nachweisen** können (sogenannte **Rechenschaftspflicht**). Die Beachtung der Datenschutzgrundsätze ist somit bei jeder Verarbeitung personenbezogener Daten zu Zwecken der Werbung bzw. des Marketings von zentraler Bedeutung. Wir gehen daher in diesem Whitepaper auf ausgewählte Grundsätze näher ein.

3.2 Erlaubnis für die Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist nur rechtmäßig, wenn hierfür eine Erlaubnis nach DSGVO vorliegt.

Die Datenschutz-Grundverordnung enthält keine speziellen Erlaubnistatbestände für die Verarbeitung personenbezogener Daten zum Zwecke der Werbung. Die Rechtmäßigkeit einer solchen Verarbeitung ist daher an den allgemeinen, in Art. 6 Abs. 1 DSGVO niedergelegten Erlaubnissen zu messen. Personenbezogene Daten können demnach zu Zwecken der Werbung insbesondere auf Basis

- einer **Interessenabwägung** oder

- einer **Einwilligung** der betroffenen Person

verarbeitet werden.

3.2.1 Verarbeitung auf Basis einer Interessenabwägung – was ist zu berücksichtigen?

Die Verarbeitung personenbezogener Daten kann grundsätzlich auf eine **Interessenabwägung** gestützt werden. Danach ist eine Datenverarbeitung rechtmäßig, wenn sie zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen.

In den Erwägungsgründen der DSGVO wird positiv festgestellt, dass die Verarbeitung personenbezogener Daten zum Zwecke der **Direktwerbung ein berechtigtes Interesse** darstellen kann. Der Begriff des Direktmarketings erfasst hierbei sämtliche Datenverarbeitungsvorgänge zu diesem Zwecke – also etwa auch Maßnahmen im Vorfeld wie die Einordnung von Kunden in eine bestimmte Zielgruppe und die Selektion von Adressaten eines Mailings anhand deren Zielgruppenzugehörigkeit.

Bei der Verarbeitung von Daten auf Basis einer Interessenabwägung müssen die betroffenen Personen über **die konkreten berechtigten Interessen informiert** werden (zu den Informationspflichten siehe unter 3.3). Ihnen muss weiterhin ein **bedingungsloses Widerspruchsrecht** gewährt werden; auch hierüber sind sie zu informieren, und zwar bei jeder Kundenkommunikation (zum Widerspruchsrecht siehe näher unter 3.2).

Praxishinweis

Wenn Sie sich für Ihre Datenverarbeitung auf die **Interessenabwägung** berufen möchten, müssen die folgenden Prüfschritte durchgeführt werden:

- Liegt ein **berechtigtes Interesse** des Verantwortlichen oder eines Dritten vor?
- Ist die Verarbeitung zur Erreichung dieses Interesses **erforderlich**?
- Stehen **Interessen der betroffenen Personen** entgegen und überwiegen diese? Dies dürfte insbesondere bei Kindern der Fall sein (nach der DSGVO gelten alle nicht volljährigen Personen als Kinder). Unbedingt zu beachten sind Widersprüche (siehe auch 3.3).
- Sind die widerstreitenden Interessen **ausgewogen** berücksichtigt? Für überwiegende Interessen des werbenden Unternehmens dürfte u.a. sprechen, wenn auch **externe Sperrlisten** geprüft und berücksichtigt werden.

Ein wichtiger Aspekt im Rahmen der Interessenabwägung sind die **berechtigten Erwartungen** der betroffenen Personen: wenn diese mit einer entsprechenden Verarbeitung ihrer Daten rechnen mussten und über ihr Widerspruchsrecht informiert waren, hiervon aber keinen Gebrauch gemacht haben, spricht viel dafür, dass ihre Interessen nicht überwiegen.

Die Prüfung sollte schriftlich erfolgen und ausreichend detailliert **dokumentiert** werden.

Was ist danach konkret möglich? In jedem Fall sind solche Verarbeitungsvorgänge, die auch unter bisherigem Recht gestattet waren, möglich – also etwa adressierte Briefwerbung für eigene Werbezwecke oder auch in Form einer Empfehlungswerbung für Dritte, wenn

- **Bestandskunden** oder **Interessenten** angesprochen werden,
- sich die Werbung an Adressaten und deren **berufliche Tätigkeit** richtet und hierfür deren berufliche Kontaktdaten verwendet werden oder

- es sich um **Spendenwerbung einer steuerbegünstigen Organisation** handelt.

Zulässig auf Basis einer Interessenabwägung ist im Regelfall auch die **Selektion von Kundendaten für eigene oder fremde Werbezwecke** und die Übermittlung von **in Gruppen zusammengefassten Kundendaten** an Dritte für deren Werbezwecke.

Grundsätzlich dürfte die Interessenabwägung auch die **Erhebung von Daten aus öffentlichen Quellen** rechtfertigen. Die deutschen Datenschutzbehörden stehen der Anreicherung von Kundendatensätzen um Informationen aus den (öffentlichen) Profilen sozialer Netzwerke allerdings sehr kritisch gegenüber. Eine solche Anreicherung sollte daher stets sorgfältig geprüft werden.

Nicht unkritisch ist hingegen die Übermittlung von umfangreichen Kundenprofilen an Dritte. Als Alternative stehen die Empfehlungswerbung und das Lettershop-Verfahren (siehe hierzu bereits die Praxisbeispiele unter 2.2) zur Verfügung. In beiden Fällen werden die Daten vom Verantwortlichen nur für fremde Werbezwecke genutzt, aber gerade nicht übermittelt.

Praxishinweis

Die Verarbeitung sogenannter besonderer Kategorien von Daten (z. B. Angaben zur Gesundheit, Religion oder sexuellen Orientierung) und zu strafrechtlichen Verurteilungen ist nur in engen Grenzen möglich. Im Regelfall gilt für solche **sensiblen Daten** ein **Verarbeitungsverbot**. Sensible Daten haben daher in der Werbung nichts zu suchen und sollten auch nicht für die Ermittlung von Zielgruppen verwendet werden.

Auch die Zusammenführung von Kundendaten im Rahmen einer **unternehmensübergreifenden CRM-Datenbank** einer Gruppe von Unternehmen kann unter Umständen auf die Interessenabwägung gestützt werden. In den Erwägungsgründen der DSGVO ist sogar positiv festgestellt, dass innerhalb einer Unternehmensgruppe ein **berechtigtes Interesse an einer Übermittlung von Kundendaten für interne Verwaltungszwecke** bestehen kann. Eine solche Datenbank wird in der Regel einer gemeinsamen Verantwortung der beteiligten Unternehmen unterliegen. In solchen Fällen muss ein sogenannter **Joint Controllership Vertrag** nach Art. 26 DSGVO geschlossen werden. Die betroffenen Kunden bzw. Interessenten müssen über die wesentlichen Inhalte des Vertrages informiert werden. Dazu zählt z. B., wer der Ansprechpartner für Auskünfte ist und wohin Widersprüche zu richten sind.

3.2.2 Verarbeitung auf Basis einer Einwilligung – wie ist diese auszugestalten?

Alternativ kann eine Verarbeitung für werbliche Zwecke auch auf Basis einer **Einwilligung** der betroffenen Personen erfolgen.

Die DSGVO definiert die Einwilligung als „*jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist*".

Die in dieser Regelung festgelegten Voraussetzungen sind kumulativ zu erfüllen. Besonderheiten sind beispielsweise auch mit Blick auf Kinder unter 16 Jahren zu beachten. Bei diesen muss die Einwilligung durch den Träger der elterlichen Verantwortung erfolgen.

3.2.2.1 Anforderungen an die Einwilligung

Bei Einholung einer Einwilligung sind stets die folgenden Grundsätze zu beachten:

- **Die Einwilligung muss freiwillig erfolgen**

  Der Einwilligende muss eine echte Wahl haben. Er darf sich daher weder in einer Abhängigkeitslage befinden noch überrumpelt werden. Eine Überrumpelung läge etwa vor, wenn ein besonderer Zeitmangel ausgenutzt würde. Die Einwilligung darf, damit sie freiwillig ist, auch nicht an eine Leistung gekoppelt werden – es darf also etwa bei einem Vertrag über eine Dienstleistung nicht eine Einwilligung abverlangt werden, die für die Erfüllung des Vertrages nicht erforderlich ist (zu diesem „Kopplungsverbot siehe auch die Antwort auf Frage 4.5). Um die Freiwilligkeit zu gewährleisten, müssen Betroffene unter Umständen getrennt in verschiedene Verarbeitungsvorgänge einwilligen können (Stichwort: Granulare Einwilligungen). So kann es zum Beispiel erforderlich werden, Betroffenen, die Werbung per E-Mail-Newsletter, aber nicht per Telefon wünschen, eine gesonderte Einwilligung zu ermöglichen.

- **Die Einwilligung muss für den konkreten Fall erfolgen**

  Es muss erkennbar sein, welche personenbezogenen Daten für welchen Zweck verarbeitet werden – “pauschale” Einwilligungen sind unwirksam. Wenn die Verarbeitung mehreren Zwecken dient, muss für jeden eine Einwilligung gegeben werden.

- **Die Einwilligung muss in Kenntnis der Sachlage erfolgen**

  Der Einwilligende muss die Einwilligung in Kenntnis der Sachlage abgeben, was insbesondere voraussetzt, dass er die Möglichkeit hatte, sich vom Inhalt der Erklärung in zumutbarer Weise Kenntnis zu verschaffen. Dies wäre unter anderem nicht gegeben, wenn eine sehr kleine Schriftart verwendet wird oder die Hinweise in einem längeren Text versteckt werden.

  Die entsprechende Erklärung muss ferner hinreichend transparent sein. Damit ist etwa eine klare und verständliche Sprache, aber auch die Vermeidung von Fachbegriffen gemeint. Dabei muss die betroffene Person nach Durchsicht der Einwilligungserklärung vor allem in der Lage sein, zu verstehen, wer seine Daten nutzen darf, welche Daten genutzt werden dürfen, zu welchem Zweck diese genutzt werden, ob diese Daten weitergeben werden und wenn ja, an wen und unter welchen Bedingungen, und wie lange seine Daten genutzt werden dürfen. Werden also Daten an Kooperationspartner weitergegeben, sind diese im Idealfall namentlich oder zumindest abstrakt zu benennen – dies greift allerdings dann nicht, wenn lediglich selber für Dritte geworben und folglich keine Daten weitergegeben werden.

- **Die Einwilligung muss unmissverständlich abgegeben werden**

Die Einwilligung kann zum einen schriftlich, in elektronischer Form oder auch mündlich erteilt werden (mündliche Einwilligungen stellen Verantwortliche mit Blick auf die Informationspflichten sowie die Beweislast jedoch vor besondere Herausforderungen). Zum anderen können Einwilligungen in Form einer "sonstigen eindeutigen Handlung" erfolgen, womit zum Beispiel die Aktivierung von Checkboxen im Rahmen von Formularen gemeint ist. In Betracht kommt auch die Nutzung von Schiebereglern. Wichtig ist, dass die Einwilligung nicht mittels einer bereits vorausgewählten Checkbox oder eines aktivierten Reglers eingeholt werden kann – in diesem Fall fehlt die „unmissverständliche Willensbekundung".

Eine „ausdrückliche" Einwilligung ist hingegen nur in besonderen Fällen erforderlich (u.a. bei der Einwilligung in die Verarbeitung besonderer Kategorien von Daten wie z. B. Gesundheitsdaten oder in den Transfer von Daten in unsichere Drittstaaten wie die USA ohne, dass hinreichende Garantien vorliegen). Im Bereich Werbung und Marketing dürfte eine ausdrückliche Einwilligung daher nur selten erforderlich sein.

Praxishinweis

Die Anforderungen an eine wirksame Einwilligung sind hoch. Bei einer unwirksamen Einwilligung kann auch nicht ohne weiteres auf eine gesetzliche Erlaubnis wie die Interessenabwägung zurückgegriffen werden. Soweit eine Verarbeitung eindeutig auch auf die Interessenabwägung gestützt werden kann, bietet es sich daher an, auf die Einwilligung zu verzichten.

3.2.2.2 Der Widerruf – so einfach wie die Einwilligung

Nach der DSGVO müssen Einwilligungen jederzeit mit Wirkung für die Zukunft widerrufen werden können. Hierauf muss vor Erteilung der Einwilligung hingewiesen werden.

Gleichzeitig muss der Widerruf *„so einfach wie die Erteilung der Einwilligung sein"*. Wurde eine Einwilligung z. B. online eingeholt, darf vom Betroffenen nicht verlangt werden, den Widerspruch per Brief zu erheben. Schon vor der Erteilung der Einwilligung sollten den Einwilligenden E-Mail-Adresse und ggf. auch Adresse bzw. Telefonnummer für den Widerruf mitgeteilt werden.

Wird die Einwilligung mündlich eingeholt, ist zumindest die Nennung einer Telefonnummer und einer E-Mail-Adresse zu empfehlen und der Kunde zu fragen, ob er weitere Kontaktmöglichkeiten wie eine postalische Adresse genannt haben möchte. Zusätzlich oder alternativ kann der Kunde auch auf eine Internetseite verwiesen werden, die weitere Informationen bereithält.

3.2.2.3 Ausgestaltung der Einwilligung

Praxishinweis

Einwilligungen unter Beachtung der Vorgaben der DSGVO könnten beispielsweise wie folgt aussehen:

Beispiel 1: **Einwilligung in Datenübermittlung an Kooperationspartner in der EU**

Einwilligung in Übermittlung von Daten

☐ *Ich bin damit einverstanden, dass [Firmenbezeichnung] meine bei der Registrierung erhobenen Daten (Name, E-Mail-Adresse, Geburtsdatum, …) und meine Bestelldaten (Datum der Bestellung, Bestellweg, Produktgruppe) regelmäßig an unsere Kooperationspartner [namentlich genannte Empfänger mit Anschrift] übermittelt. Unsere Kooperationspartner werden diese Daten nur für Briefwerbung zu eigenen Produkten verwenden. Diese Einwilligung kann uns gegenüber jederzeit mit Wirkung für die Zukunft widerrufen werden unter[datenschutz@firma.de].*

Beispiel 2: **Einwilligung in E-Mail-Marketing**

Einwilligung in E-Mail-Marketing

☐ *Ich bin damit einverstanden, dass [Firmenbezeichnung] mich per E-Mail regelmäßig über Aktionen und Angebote zu [konkreten Zweck beschreiben, z. B. "unseren Produkten aus dem Bereich Lebensmittel"] informiert. Diese Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden unter [datenschutz@firma.de].*

3.2.2.4 Einwilligungen von Kindern

Die DSGVO stuft alle Personen, die nicht volljährig sind, als Kinder ein. Besonderheiten gelten hierbei in Deutschland für Kinder unter 16 Jahren: Einwilligungen von Kindern unter 16, die im Rahmen von „Diensten der Informationsgesellschaft" – also z. B. auf Websites, in Apps oder sozialen Netzwerken – eingeholt werden, müssen von deren Eltern eingeholt werden oder diese zumindest zustimmen. In einem solchen Fall müssen Sie „*unter Berücksichtigung der verfügbaren Technik angemessene Anstrengungen unternehmen"* um sich zu vergewissern, dass die Einwilligung tatsächlich von den Eltern bzw. Sorgeberechtigten erteilt wurde. Welche Anforderungen im Einzelnen erfüllt sein müssen und ob es zum Beispiel ausreicht, eine E-Mail von einem anderen E-Mail-Account zu erhalten, ist noch nicht geklärt. Wenn Sie auf Nummer sicher gehen wollen, verzichten Sie bei Verarbeitungen, für die Sie eine Einwilligung benötigen, auf Daten von Personen unter 16.

3.2.2.5 Was ist sonst zu beachten?

Die **Beweislast** für das Vorliegen der Einwilligung und aller Voraussetzungen liegen bei Ihnen.

Wie der Nachweis der Einwilligung konkret zu erbringen ist, wird durch die DSGVO nicht festgelegt. Es ist aber ratsam, dass neben der Einwilligung auch die Tatsache dokumentiert wird, dass der Einwilligende vorab über sein Widerrufsrecht informiert worden ist (siehe hierzu auch unseren Formulierungsvorschlag oben unter 3.2.2.3).

Die Art der **Dokumentation** richtet sich grundsätzlich danach, wie die Einwilligung erteilt wird. Bei einer elektronischen Einwilligung sollten die exakte Zeit und die IP-Adresse protokolliert und gespeichert werden. Auch eine Kopie der erteilten Informationen sollte abgespeichert werden,

damit Sie im Streitfall darlegen können, worüber der Einwilligende von Ihnen konkret informiert worden ist.

Mündliche Einwilligungen stellen Verantwortliche mit Blick auf die Informationspflichten sowie die Beweislast vor besondere Herausforderungen. Hier sind zwingend feste Prozesse in Richtlinien für Telefonate zu implementieren. Telefonische Einwilligungen sollten einschließlich der erteilten Informationen über das Widerrufsrecht aufgezeichnet werden. Für diese Aufzeichnung muss allerdings vorab eine gesonderte Einwilligung eingeholt werden – ansonsten macht sich der Aufzeichnende strafbar.

3.3 Widerspruchsrecht gegen Direktmarketing

Die DSGVO gewährt ein bedingungsloses Widerspruchsrecht gegen Direktmarketing.

Übt eine Person ihr Widerspruchsrecht aus, dürfen die personenbezogenen Daten in dem Umfang, in dem diese Person von ihrem Widerspruchsrecht Gebrauch gemacht hat, nicht mehr verarbeitet werden. In Zweifelsfällen gilt: Fragen Sie nach. Solange die Sachlage unklar ist, sollten Sie von einem umfassenden Widerspruch ausgehen.

Das Widerspruchsrecht gilt nicht nur für das Direktmarketing selbst (also die Werbe-Mail an den Bestandskunden oder das postalische Mailing), sondern auch für sämtliche damit im Zusammenhang stehenden Verarbeitungsvorgänge. Geht ein entsprechender Widerspruch ein, muss die betroffene Person also nicht nur aus dem Werbe-Verteiler genommen, sondern auch die im Vorfeld erfolgte Zielgruppenzuordnung gelöscht werden.

Beworbene müssen spätestens bei der ersten Kontaktaufnahme auf dieses Widerspruchsrecht hingewiesen werden. Der Hinweis muss *„in einer verständlichen und von anderen Informationen getrennten Form"* erteilt werden. Aufgrund der zentralen Bedeutung des Widerspruchsrechts für die Verarbeitung von Daten auf Basis einer Interessenabwägung sollte diese Information darüber hinaus bei jeder Kundenkommunikation wiederholt werden.

Praxishinweis

Um zu gewährleisten, dass der Hinweis in einer von anderen Informationen getrennten Form erfolgt, könnte am Ende der Datenschutzhinweise ein **gesonderter Abschnitt „Informationen über Ihre Widerspruchsrechte"** aufgenommen werden. Dieser Abschnitt könnte wie folgt aussehen:

Informationen über Ihre Widerspruchsrechte

1. *Widerspruchsrecht gegen Direktmarketing*

Sie können jederzeit Widerspruch gegen die Verarbeitung Ihrer personenbezogenen Daten zu werblichen Zwecken einlegen („Werbewiderspruch"). Wir werden dann die Verarbeitung Ihrer Daten zu werblichen Zwecken einstellen. Bitte berücksichtigen Sie, dass es aus organisatorischen Gründen zu einer Überschneidung zwischen Ihrem Widerruf und der Nutzung Ihrer Daten im Rahmen einer bereits laufenden Kampagne kommen kann.

2. *Widerspruchsrecht aus persönlichen Gründen*

[….]

3. *Ausübung Ihrer Rechte*

Sie können Ihren Widerspruch per E-Mail an [E-Mail-Adresse] oder per Post an [Adresse] richten. Alternativ können Sie uns auch werktags in der Zeit zwischen [Uhrzeit] bis [Uhrzeit] Uhr unter der Telefonnummer [Telefonnummer] anrufen. Weitere Informationen enthalten unsere Datenschutzhinweise [Verweis auf Datenschutzhinweise einfügen].

Dieser Abschnitt sollte für die Leser von Datenschutzhinweisen auf den **ersten Blick erkennbar und im Online-Umfeld auch direkt anklickbar** sein. Bei in Ebenen angeordneten Datenschutzhinweisen gehören diese Informationen auf die erste Ebene.

3.4 Informationspflichten

Die DSGVO enthält umfassende Informationspflichten für Verantwortliche. Die Verordnung unterscheidet dabei zwischen Konstellationen, in denen die Daten bei der betroffenen Person erhoben werden, etwa im Rahmen einer Kundenbeziehung und solchen, in denen die Daten nicht bei den betroffenen Personen erhoben werden (sondern z. B. bei Adresshändlern). Hauptunterschied ist, dass für Daten, die nicht von den betroffenen Personen stammen, auch über die Datenarten und die Quelle der Daten informiert werden muss. Die Verordnung differenziert darüber hinaus zwischen Pflichtangaben und weiteren Angaben, die nur erforderlich sind um „*um eine faire und transparente Verarbeitung zu gewährleisten*". Diese Unterscheidung ist allerdings praxisfern und die europäische Art. 29 Datenschutzgruppe (ein Gremium, das die Europäische Kommission in Datenschutzfragen berät,) hat bereits verkündet, dass sie grundsätzlich erwartet, dass sämtliche Angaben gemacht werden.

Praxishinweise

1. Die Informationspflichten werden in der Regel über die **Online-Datenschutzbestimmungen** erfüllt. Wir empfehlen, bei deren Gestaltung auf die Empfehlungen der Art. 29 Datenschutzgruppe zu „Transparenz nach DSGVO" achten (siehe hierzu die Links unter Ziffer 5). Hierzu zählt eine Darstellung auf verschiedenen Ebenen.

2. Bei einer Verarbeitung von Daten auf Basis einer **Interessenabwägung** muss über die **konkreten berechtigten Interessen** informiert werden (z. B. „Wir haben ein berechtigtes Interesse, eigene Kundendaten nach Zielgruppen zu segmentieren und zielgruppenspezifisch postalische Mailings zu versenden").

3. Bei der Erhebung von Daten bei Dritten (z. B. Adresshändler, Auskunftei) sowie aus öffentlich zugänglichen Quellen (z. B. Internet) muss auch über **Datenkategorien und Quellen** informiert werden.

4. Es muss **dokumentiert** werden, dass die betroffene Person eine bestimmte Fassung der Datenschutzbestimmungen zur Kenntnis genommen hat (etwa im Rahmen des Bestellprozesses); dies ist im Kundenkonto zu speichern.

5. Bei der Erhebung von Daten von Dritten oder sonstigen Quellen, die in den Datenschutzbestimmungen noch nicht genannt waren, muss eine **Benachrichtigung** erfolgen, und zwar spätestens innerhalb eines Monats und jedenfalls im Rahmen der ersten Kommunikation (z. B. einem Mailing).

6. Auch **Zweckänderungen führen zu einer Benachrichtigungspflicht**. Die deutschen Datenschutzbehörden sehen dabei bereits neue Kategorien von Empfängern (z. B. Kooperationspartner, die erstmals Adressdaten von eigenen Kunden erhalten) als Zweckänderung an.

3.5 Rechte der betroffenen Personen

Die DSGVO gewährt betroffenen Personen neben den bereits bekannten Rechten auf Auskunft, Berichtigung und Löschung von Daten sowie dem Widerspruchsrecht noch weitere Rechte. Neu hinzukommt z. B. das Recht auf Datenübertragbarkeit. Einschränkungen zu Betroffenenrechten enthält das BDSG-neu, wobei diese aus unserer Sicht im Bereich Werbung und Marketing keine große Relevanz entfalten werden.

Antworten auf typische Fragestellungen im Zusammenhang mit Betroffenenrechten finden Sie in Abschnitt 4.

3.6 Verträge mit Dienstleistern – Auftragsverarbeitungen

Im Bereich Werbung und Marketing werden regelmäßig zahlreiche Tätigkeiten auf Dritte ausgelagert – etwa der Versand von E-Mail-Newslettern oder Briefwerbung oder Telefonmarketing durch Callcenter. Solche Dienstleister sollten von Ihnen regelmäßig als sogenannte Auftragsverarbeiter tätig werden – denn nur dann benötigen Sie für die Weitergabe der Daten keine Erlaubnis nach der DSGVO (da diese Auftragsverarbeiter nicht als Dritte gelten).

Verträge, die noch nicht mit Blick auf die Datenschutz-Grundverordnung entworfen wurden, sind im Hinblick auf die Anforderungen nach DSGVO kritisch zu überprüfen. Für Auftragsverarbeitungen sind eine Vielzahl von Regelungen aufzunehmen, die detailliert in Art. 28 Abs. 3 DSGVO aufgeführt sind. Viele davon waren auch schon nach BDSG nötig (z. B. Angaben zu Gegenstand, Dauer, Art und Zweck der Verarbeitung, zu den Kategorien von betroffenen Personen bzw. Daten sowie zur Löschung und Rückgabe von Daten). Neu sind insbesondere **Anforderungen an die Einschaltung neuer Subunternehmer**: Wenn ein Verantwortlicher dem Auftragsverarbeiter allgemein erlaubt, Subunternehmer einzuschalten, muss er über Änderungen vorab so zeitig informiert werden, dass er widersprechen kann.

Von zentraler Bedeutung ist, dass der Auftragsverarbeiter nur nach Ihren Weisungen handeln und keine Entscheidungsfreiheit bezüglich der Zwecke und Mittel der Verarbeitung haben darf. Die Weisungen müssen unbedingt **detailliert und dokumentiert** werden.

In jedem Fall müssen zusätzlich an die Risiken der jeweiligen Verarbeitungssituation angepasste **technische und organisatorische Maßnahmen zum Schutz der Datensicherheit** vereinbart werden. Der Auftraggeber ist verantwortlich dafür, dass diese angemessen sind und muss deren Umsetzung auch kontrollieren.

Praxishinweis

Die Gesellschaft für Datenschutz und Datensicherheit e. V. stellt einen mit Blick auf die Datenschutz-Grundverordnung entworfenen Vertrag für eine Auftragsverarbeitung zur Verfügung:
https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo.

Auch die Bayerische Datenschutzbehörde hat eine Formulierungshilfe für eine Vertrag über eine Auftragsverarbeitung ins Netz gestellt: https://www.lda.bayern.de/media/muster_adv.pdf.

Diese Dokumente können für kleinere Projekte, die zwischen Auftragnehmer und Auftraggeber ausgeglichen gestaltet werden sollen, verwendet werden. Anpassungen für das konkrete Projekt sind aber unumgänglich.

Zukünftig werden sich Unternehmen noch von offiziellen Zertifizierungsstellen zertifizieren lassen können. Diese Zertifizierung soll den Nachweis erleichtern, dass die Vorgaben der DSGVO eingehalten sind.

Praxishinweis

Zertifizierungen mildern die Rechenschaftspflicht von Unternehmen ab und können bußgeldmindernd wirken. Auftragsverarbeiter, die eine Zertifizierung nach DSGVO vorweisen können, sollten daher bevorzugt werden.

3.7 Folgen von Verstößen – hohe Bußgelder und Verbandsklagen drohen

Verstöße gegen die DSGVO können erhebliche Bußgelder nach sich ziehen. Der Bußgeldrahmen steigt auf bis zu 20 Millionen EUR oder – falls höher – 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres. Dieser Bußgeldrahmen greift z. B. bei einer Nutzung von Kundendaten für Mailings ohne hinreichende Erlaubnis oder die Nichtbeachtung eines Widerspruchs gegen Direktmarketing. Alleine schon aus diesem Grund sollte die Beachtung der DSGVO auch bei Ihnen eine zentrale Rolle spielen.

Für bestimmte Datenschutzverstöße – darunter auch die unzulässige gewerbsmäßige Übermittlung personenbezogener Daten an Dritte – sieht das BDSG-neu darüber hinaus sogar **Freiheits- bzw. Geldstrafen** für die handelnden Personen vor.

Hinzukommt, dass der deutsche Gesetzgeber von der Möglichkeit Gebrauch gemacht hat, ein Verbandsklagerecht einzuführen: Verbraucherschutzverbände können auf **Unterlassung** klagen, wenn Unternehmen personenbezogene Daten von Verbrauchern zu Zwecken der Werbung, der Markt- und Meinungsforschung, des Betreibens einer Auskunftei, des Erstellens von Persönlichkeits- und Nutzungsprofilen, des Adresshandels, des sonstigen Datenhandels oder zu vergleichbaren kommerziellen Zwecken rechtswidrig verarbeiten. Darüber hinaus steht ihnen ein Beseitigungsanspruch zu – rechtswidrige Datenbestände müssen hiernach sogar gelöscht werden. Daneben haben Verbände auch die generelle Möglichkeit, Unterlassungsklagen gegen aus ihrer Sicht unzulässige AGB anzustrengen.

Bußgeldmildernd wirken können neben Zertifizierungen (siehe hierzu oben unter 3.6) auch die **Einhaltung sogenannter genehmigter Verhaltensregeln**. Diese sollen insbesondere kleineren und mittleren Unternehmen helfen, die DSGVO einzuhalten. Sobald entsprechende Verhaltensregeln für den Bereich Werbung bzw. Marketing entwickelt und von den Aufsichtsbehörden genehmigt wurden, sollten diese von Verantwortlichen und Auftragsverarbeitern beachtet werden. Dies gilt erst recht, wenn die Kommission solche Regeln für allgemein gültig erklären sollte.

4. Häufig gestellte Fragen zur Datenschutz-Grundverordnung und Werbung

Die Organisation Werbungtreibende im Markenverband wird von ihren Mitgliedern regelmäßig zu verschiedenen Fragen zum Thema DSGVO und Werbung kontaktiert. Wir haben für Sie besonders häufig auftretende Fragen nebst kurzen Antworten hierauf im Folgenden zusammengestellt:

Einwilligung

4.1 Brauche ich für Marketing jetzt immer eine Einwilligung?

Marketing ohne Einwilligung ist grundsätzlich auch auf Basis der gesetzlichen Erlaubnis einer Interessenabwägung möglich (siehe hierzu näher unter 3.2.1). Dies gilt insbesondere für die Nutzung eigener Kunden- bzw. Interessendaten für postalische Mailings. Zu beachten ist dabei aber, dass nach den lauterkeitsrechtlichen Grundsätzen z. B. für E-Mail-Marketing oder Telefonmarketing auch weiterhin eine Einwilligung erforderlich sein kann.

4.2 Müssen sämtliche Einwilligungen neu eingeholt werden?

Grundsätzlich werden vor dem 25. Mai 2018 wirksam erteilte Einwilligungen mit Geltungsbeginn der DSGVO nicht unwirksam.

Voraussetzung für die Weitergeltung früherer Einwilligungen ist allerdings, dass diese sämtlichen Vorgaben der DSGVO entspricht – so legt es der Verordnungsgeber ausdrücklich in den Erwägungsgründen fest. War es nach bisheriger Rechtslage beispielsweise in bestimmten Fällen möglich, dass ein bereits vorangekreuztes Kästchen zur Einholung der Einwilligung ausreichte, ist dies nun nicht mehr möglich. Im Offline-Bereich war bisher auch nicht zwingend auf das Widerrufsrecht hinzuweisen. Eine nach DSGVO unwirksame Einwilligung ist ab dem 25. Mai 2018 nicht mehr gültig und muss daher neu eingeholt werden. Erklärungen, die bereits den strengen Anforderungen der Rechtsprechung für Einwilligungen in Marketing (E-Mail, Telefon, SMS) entsprechen (vergleiche etwa Urteile des Bundesgerichtshof vom 25.10.2012 – I ZR 169/10 (KG) und vom 14.03.2017 – VI ZR 721/15), werden in der Regel auch den Anforderungen der DSGVO genügen. In jedem Fall sollten die bisher erteilten Einwilligungen sorgfältig überprüft werden.

Generell wird davon ausgegangen, dass eine Einwilligung in angemessenen Abständen neu eingeholt werden muss. Beachten Sie hierzu auch unsere Antwort auf 4.3.

4.3 Wie lange gilt eine Einwilligung?

Grundsätzlich gilt, dass die Einwilligung in angemessenen Abständen neu eingeholt werden sollte und Einwilligende erneut auf ihre Rechte aufmerksam zu machen sind. Es ist vertretbar, dass dies entfällt, wenn die Einwilligung regelmäßig gebraucht wird und die betroffenen Personen dabei erneut auf ihre Rechte (Widerrufsmöglichkeit, sonstige Rechte) unter Verweis auf detaillierte Informationen zum Beispiel auf einer Internetseite hingewiesen werden.

4.4 Meine Marketingkollegen in anderen EU-Ländern holen Einwilligungen von Kindern schon ab 13 Jahren ein – warum darf ich dies nicht? Die DSGVO gilt doch für alle?

Die DSGVO erlaubt den Mitgliedsstaaten, die Altersgrenze, ab der Minderjährige selbst in die Verarbeitung ihrer Daten einwilligen können, auf 13 Jahre abzusen-

ken. Deutschland hat hiervon aber keinen Gebrauch gemacht – für Unternehmen mit Sitz in Deutschland bleibt es daher bei der Altersgrenze von 16 Jahren.

4.5 Ich möchte über eine App Einwilligungen in E-Mail-Marketing generieren: Jeder kann sich kostenlos für die App registrieren, muss dafür aber einen Newsletter abonnieren – geht dies?

Diese Frage ist noch nicht abschließend geklärt. Die DSGVO sieht vor, dass eine Einwilligung in die Verarbeitung unter Umständen nicht hinreichend freiwillig und damit unwirksam ist, wenn sie an einen Vertrag gekoppelt ist, für dessen Durchführung sie nicht erforderlich ist. Auch eine Einwilligung in E-Mail-Marketing, deren Erteilung Voraussetzung für eine Nutzung von Services ist (im Beispiel eine App, denkbar ist auch eine Kopplung der Einwilligung an eine Gewinnspielteilnahme), könnte daher grundsätzlich unter dieses „Kopplungsverbot" fallen.

Irritierend ist hierbei, dass für die Verarbeitung von Daten, die für die Durchführung eines Services erforderlich sind, eigentlich sowieso keine Einwilligung erforderlich ist – die Daten können vielmehr im Regelfall auf Basis der gesetzlichen Erlaubnis „Vertragsdurchführung" verarbeitet werden (ausgenommen Sonderfälle wie sensible Gesundheitsdaten).

Die deutschen Datenschutzbehörden haben daher auch einen Ausweg aufgezeigt für Geschäftsmodelle, bei denen die Nutzer wie im Beispiel für die App mit einer Zustimmung in die werbliche Nutzung ihrer Daten „bezahlen" sollen: Bei hinreichend klarer Vertragsgestaltung halten sie solche Geschäftsmodelle für grundsätzlich zulässig. Die gesetzliche Erlaubnis für die Verarbeitung der Daten soll in diesem Fall offenbar die Vertragsdurchführung sein, denn die Behörden sprechen davon, dass dann „keine Notwendigkeit mehr [bestehe] für eine Einwilligung" (siehe Kurzpapier Nr. 3 der Datenschutzkonferenz vom 29.06.2017, Seite 2). Ob sich diese Auffassung EU-weit durchsetzen wird ist allerdings noch unklar. Wenn Sie eine Kopplung planen, sollten Sie das geplante Konstrukt unbedingt vorab rechtlich prüfen und sich zu den Risiken beraten lassen.

4.6 Müssen vor dem 25. Mai 2018 für Werbung erhobene Daten gelöscht werden?

Auch nach bisherigem Recht war es unzulässig, Daten ohne bestimmten Zweck oder ohne hinreichende Erlaubnis (z. B. eine Einwilligung oder die Interessenabwägung) zu verarbeiten. Daten, die im Rahmen einer Kundenbeziehung nach bisherigem Recht wirksam erhoben wurden, können hierfür auch unter der DSGVO weiter verarbeitet und – unter Beachtung der besonderen Anforderungen der DSGVO – auch für werbliche Zwecke genutzt werden. Wichtig ist insbesondere, dass spätestens ab dem 25. Mai 2018 die Informationspflichten nach DSGVO beachtet werden.

Wurden Daten allerdings rechtswidrig erhoben, sind Unternehmen unter der DSGVO verpflichtet, diese zu löschen – auch ohne entsprechende Anfrage.

Profiling und Tracking

4.7 Ich habe gehört, dass die DSGVO Profiling verbietet. Darf ich jetzt überhaupt noch Zielgruppen für mein Marketing bilden?

Die DSGVO enthält tatsächlich ein Verbot für sogenannte „automatisierte Entscheidungen im Einzelfall einschließlich Profiling" (Art. 22 DSGVO). Dieses Verbot gilt aber nur für Konstellationen, in denen personenbezogene Daten verwendet werden, um ***bestimmte Aspekte einer Person zu analysieren oder vorherzusagen*** *(„*Profiling*") – und dies dann* ***eine Rechtswirkung hat oder zu ei-***

ner erheblichen Beeinträchtigun*g führt. Beispiele für ein solches Profiling mit Rechtswirkung ist z. B. ein Bonitätsscoring, wenn dies dazu führt, dass ein Online-Kreditantrag automatisiert abgelehnt wird, sobald der Scorewert eine bestimmte Schwelle unterschreitet. Die Zusammenstellung von Zielgruppen für Marketing stellt zwar ein Profiling im Sinne der DSGVO dar, nämlich eine Verwendung personenbezogener Daten um bestimmte Aspekte einer Person – namentlich deren persönliche Vorlieben und Interessen – zu bestimmen. Rechtliche Wirkungen oder sonstige erhebliche Beeinträchtigungen sind hiermit aber nicht verbunden. Werbliches Profiling fällt daher nicht unter dieses Verbot.*

4.8 Wie ist das Verhältnis zwischen DSGVO und e-Privacy-Verordnung?

Die e-Privacy-Verordnung liegt derzeit nur in einem Entwurfsstadium vor. Es ist damit zu rechnen, dass diese 2019 in Kraft treten wird. Sie gilt grundsätzlich parallel zur DSGVO, soll aber vor allem die Bereitstellung und Nutzung elektronischer Kommunikationsdienste präzisieren und ergänzen und enthält auch Regelungen für E-Mail-Marketing und Telefonwerbung. Soweit die e-Privacy-Verordnung hierfür allerdings eine Einwilligung vorschreibt, gelten für diese Einwilligung die Anforderungen nach DSGVO.

4.9 Ist unter der DSGVO personalisierte Werbung auf der Basis von Nutzertracking im Internet weiterhin möglich?

Die DSGVO enthält keine Regelungen speziell für Werbezwecke. Ob die aktuellen Regelungen zum Nutzertracking im Telemediengesetz (TMG) unter der DSGVO weiterhin Anwendung finden, ist umstritten. Wir meinen, dass dies nicht der Fall ist und das Nutzertracking grundsätzlich auf Basis einer Interessenabwägung durchgeführt werden kann. Wir gehen aber davon aus, dass die deutschen Datenschutzbehörden zumindest übergangsweise die Anforderungen des TMG weiter berücksichtigen werden, sollte Werbung im Internet auch weiterhin nur auf Basis pseudonymer Nutzungsprofile erfolgen. Die Profile müssen also unter einer ID geführt werden und dürfen nicht mit personenbezogenen Daten zusammengeführt werden. Personenbezogene bzw. ggf. personenbezogene Daten wie Benutzernamen, E-Mail-Adresse oder IP-Adressen haben daher auch zukünftig nichts in den Nutzungsprofilen zu suchen. Auch eine verlässliche und einfache Opt-Out-Möglichkeit muss weiterhin gegeben sein – schon zur Umsetzung des Widerspruchsrecht (siehe hierzu oben unter 3.3); idealerweise steht hierzu ein einfaches Tool zur Verfügung, dass den betroffenen Personen auch eine individuelle Auswahl zulässt (Stichwort: „Präferenzmanagement"). Und selbstverständlich müssen diese informiert werden.

Zusätzlich zur DSGVO soll nach den Plänen des europäischen Gesetzgebers die sogenannte e-Privacy-Verordnung in Kraft treten. Details hierzu finden Sie oben bei Frage 4.84.3. Sollte die e-Privacy-Verordnung in ihrer derzeit absehbaren Form tatsächlich verabschiedet werden, ist Cookie-basierte personalisierte Werbung auch in Deutschland nur noch mit Einwilligung des Nutzers möglich. Diese Einwilligung wird dabei nicht über ein einfaches Cookie-Banner eingeholt werden können, wie man es derzeit noch auf vielen Websites sieht. Vielmehr werden auch für diese Einwilligung die strengen Vorgaben der DSGVO gelten. Die Details sind umstritten und in der Diskussion. Die Entwicklung bleibt zu beobachten - wir halten Sie auf dem Laufenden.

Bitte beachten Sie zusätzlich, dass für Cookies in den meisten Ländern der EU schon jetzt ein Opt-In erforderlich ist. Hierfür sollten ab dem 25. Mai 2018 die Vorgaben der DSGVO für Einwilligungen beachtet werden.

4.10 In meiner Shop-App ist ein Trackingtool zur Analyse des Nutzungsverhaltens meiner Kunden integriert. Der Anbieter des Tools sitzt in den USA. Kann ich das Tool auch unter der DSGVO noch verwenden?

Ja – wenn Sie mit dem Anbieter einen hinreichenden Vertrag über eine Auftragsverarbeitung abgeschlossen und Sie für „geeignete Garantien" gesorgt haben, die sicherstellen, dass das Schutzniveau der EU nicht unterschritten wird. Dies ist z. B. der Fall, wenn der Dienstleister die EU-Standarddatenschutzklauseln für Auftragsverarbeiter unterzeichnet hat. Auch eine aktive Zertifizierung für das EU-US-Privacy Shield reicht derzeit noch aus. Da die Datenschutzbehörden diesem Mechanismus allerdings besonders kritisch gegenüberstehen, sind die EU-Klauseln vorzuziehen. Auf Anfrage müssen Sie Ihren Kunden mitteilen, wie der Dienstleister heißt, was er für Sie tut und wo er die Kundendaten speichert. Außerdem müssen Sie Kunden mitteilen, welchen Schutzmechanismus sie gewählt haben und entweder eine Kopie zur Verfügung stellen oder den Kunden zumindest sagen, wo diese eine solche Kopie erhalten können.

Löschung, Heraus- und Weitergabe

4.11 Ein Kunde wünscht die Löschung seiner sämtlichen Daten – was muss ich beachten?

Von Datenverarbeitung betroffenen Personen steht das Recht zu, unrichtige Daten korrigieren oder Daten löschen zu lassen, wenn diese für die Zwecke, für die sie erhoben wurden, nicht mehr benötigt werden. Selbstverständlich müssen Sie aber weder Daten löschen, die Sie noch zur Durchführung eines Vertrags (etwa Auslieferung einer Bestellung) benötigen oder die gesetzlichen Aufbewahrungsfristen (z. B. aus dem Steuerrecht) unterliegen. Auch wenn Sie mit jemandem noch über Ansprüche streiten (z. B. Gewährleistung), können Sie dessen Daten bis zur Klärung weiter aufbewahren. Über die weitere Speicherung und den Grund hierfür sollten Sie den Kunden allerdings informieren.

Eine solche Löschungsaufforderung kann grundsätzlich auch als Widerspruch gegen Werbung gemeint sein. Wenn es sich um einen Werbewiderspruch handelt, wäre die vollständige Löschung allerdings kontraproduktiv, da der Widersprechende möglicherweise neue Werbung erhält, wenn er nicht auf einer internen Sperrliste steht. Im Zweifel sollten Sie nachfragen und den Kunden über die Funktionsweise der Sperrliste aufklären.

Wenn Sie die Daten des Kunden an Kooperationspartner weitergeben haben, müssen Sie diese über die Löschung informieren. Empfehlenswert ist, dass Sie hierfür die notwendigen Prozessabläufe festlegen – wie also etwa mit entsprechenden Anfragen umzugehen ist, wie diese umgesetzt werden und wie die entsprechende Dokumentation erfolgen muss.

4.12 Ein Kunde hat mitgeteilt, dass er von seinem „Recht auf Vergessenwerden" Gebrauch macht. Was bedeutet dies?

*Es kann zum einen bedeuten, dass er die Löschung seiner Daten wünscht. Zum anderen kann es bedeuten, dass er möchte, dass Daten zu seiner Person, die von Ihnen öffentlich gemacht wurden (z. B. über ein Online-Portal) und die infolgedessen von Dritten übernommen oder verlinkt wurden, wieder aus dem Internet verschwinden. Klären Sie durch Nachfrage, was sein Begehren ist. Bei veröffentlichten Daten sind Sie verpflichtet, Dritte „*unter Berücksichtigung der verfügbaren Technologien und der Implementierungskosten*" darüber zu informieren, dass die Links bzw. Kopien zu löschen sind. Welche Anstrengungen Sie hierzu*

unternehmen müssen, ist leider noch nicht geklärt. Sie schulden aber in jedem Fall keinen Löschungserfolg. Prüfen Sie allerdings vor jeder Veröffentlichung von Daten sehr genau, ob dies nötig ist – denn ohne Veröffentlichung bestehen schon keine entsprechenden Informationspflichten gegenüber Dritten.

4.13 Ein Gewinnspielteilnehmer wünscht die Herausgabe seiner Daten – was muss ich beachten?

Die DSGVO führt ein neues Recht auf „Datenübertragbarkeit" ein. Hiernach müssen Sie Personen, deren Daten Sie verarbeiten, diese auf Anfrage in einem strukturierten, gängigen und maschinenlesbaren Format herausgeben können - hierfür kommt etwa eine CSV-Datei in Betracht. Von Ihnen kann sogar verlangt werden, dass Sie die Daten direkt einem benannten Dritten übertragen. Dieses Recht beschränkt sich aber auf Daten, die Ihnen die Person selbst zur Verfügung gestellt hat (also z. B. im Rahmen einer Registrierung). Daten, die Sie selbst erzeugt oder von Dritten bezogen haben (z. B. ein Kundenprofil oder Bonitätsdaten), sind nicht umfasst. Außerdem gilt das Recht nur für Daten, bei denen die Verarbeitung auf einer Einwilligung oder einem Vertrag beruht. Hintergrund ist, dass Personen der Wechsel zu anderen Plattformen ermöglicht werden soll, was vor allem wettbewerbspolitische Ziele verfolgt. Gleichwohl betrifft dieses Recht auch Daten, die Sie etwa im Rahmen eines Gewinnspiels (und somit zur Durchführung eines „Gewinnspielteilnahmevertrags") erhoben haben.

4.14 Ich möchte erstmals Kooperationspartnern Adressdaten meiner Kunden für deren Werbezwecke zur Verfügung stellen. In meinen Datenschutzbestimmungen steht hierzu bislang nichts. Geht dies trotzdem?

Ja. Sie müssen allerdings zunächst sicherstellen, dass die Weitergabe auf Basis einer Interessenabwägung zulässig ist und dies dokumentieren. Hierfür kommt es maßgeblich darauf an, in welchem Umfang Sie Daten weitergeben. Denken Sie außerdem daran, die betroffenen Personen binnen Monatsfrist zu benachrichtigen bzw. den Kooperationspartner vertraglich zu verpflichten, dies für Sie binnen dieser Frist und in deren erster Kommunikation zu übernehmen. Außerdem sollten Sie Ihre eigenen Datenschutzbestimmungen umgehend anpassen.

4.15 Ich habe anhand von Kontrolladressen festgestellt, dass ein Lettershop meine Kundendaten an einen Dritten verkauft hat, obwohl er diese nur für meine Mailings verwenden durfte – muss ich dies irgendwo melden?

Es handelt sich um eine unbefugte Übermittlung von Daten an einen Dritte und somit um eine sogenannte Verletzung des Schutzes personenbezogener Daten. Diese muss der zuständigen Datenschutzbehörde binnen 72 h gemeldet werden – ausgenommen, die Verletzung führt nicht zu einem Risiko für die betroffenen Personen. Wenn es sich nur um Namen und postalische Anschriften handelt, dürfte kein Risiko bestehen. Hat der Dienstleister hingegen auch detaillierte Nutzungsprofile verkauft, kann die Bewertung anders ausfallen. Im Zweifel sollte eine Meldung erfolgen, da bei einem Verstoß ein hohes Bußgeld anfallen kann. Manche Datenschutzbehörden stellen für diese Meldung ein Online-Formular bereit.

Sofern mit der Verletzung sogar ein hohes Risiko verbunden ist, müssen zusätzlich auch die betroffenen Personen unterrichtet werden, und zwar „unverzüglich". Ein solches hohes Risiko liegt etwa vor, wenn Passwörter oder Bank- bzw. Kreditkartendaten betroffen sind.

Ohne entsprechende Sensibilisierung der Mitarbeiter im Vorfeld und einen gut strukturierten Prozess zum Umgang mit Datenpannen dürften die Vorgaben nicht einhaltbar sein, insbesondere nicht die Meldung an die Behörde binnen 72 h.

Sonstiges

4.16 Was ist ein „Verzeichnis von Verarbeitungstätigkeiten" und brauchen wir dies auch für unsere Werbung?

Vereinfacht gesagt, beinhaltet dieses Verzeichnis eine Beschreibung sämtlicher im Unternehmen eingesetzter Verfahren zur Verarbeitung personenbezogener Daten. Diese einzelnen Verfahrensbeschreibungen müssen wesentliche Angaben zur Verarbeitung enthalten wie z. B. Zwecke der Verarbeitung, Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger. Erforderlich sind auch Angaben zu Speicher- bzw. Löschfristen, technischen und organisatorischen Maßnahmen zur Datensicherheit sowie Angaben zur Übermittlung von Daten in Länder außerhalb von EU bzw. EWR. Eine solche Beschreibung muss auch für die Verarbeitung von Daten zu werblichen Zwecken vorgenommen werden. Das entsprechende Verfahren könnte z. B. „CRM-Verfahren" lauten.

Die Pflicht zur Führung eines solchen „Verfahrensverzeichnisses" besteht bereits nach derzeitigem Recht für die meisten Unternehmen. Nach der Datenschutz-Grundverordnung besteht diese Pflicht zwar grundsätzlich nur noch, wenn Ihr Unternehmen mindestens 250 Mitarbeiter beschäftigt. Die Pflicht kann aber auch Unternehmen mit weniger als 250 Mitarbeitern treffen, wenn ein besonderes Risiko bei der Verarbeitung besteht, die Verarbeitung nicht nur gelegentlich erfolgt oder besonders sensible Daten verarbeitet werden. Die deutschen Datenschutzbehörden gehen davon aus, dass dies in der Regel der Fall ist und dementsprechend auch kleine Unternehmen ein Verzeichnis anlegen müssen.

Das Verfahrensverzeichnis ist darüber hinaus gerade für kleinere Unternehmen ein guter Ausgangspunkt, um seine Verarbeitungsvorgänge zu dokumentieren und den Dokumentationspflichten und der Rechenschaftspflicht nach DSGVO nachzukommen. Hierzu sollte neben den Pflichtangaben vor allem vermerkt werden, auf Basis welcher gesetzlichen Erlaubnis die Daten im Rahmen des konkreten Verfahrens verarbeitet werden.

Neu ist unter der DSGVO, dass zukünftig auch Auftragsverarbeiter ein solches Verzeichnis führen müssen.

4.17 Müssen wir einen Datenschutzbeauftragten bestellen?

*Ein Datenschutzbeauftragter muss nach der Datenschutz-Grundverordnung nur bestellt werden, wenn die Kerntätigkeit eines Unternehmens "*in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen*". Dies ist in der Regel aber nicht der Fall, wenn Sie bloß begleitend zum eigentlichen Geschäftszweck (z. B. Verkauf von eigenen Markenprodukten) solche personenbezogenen Daten zum Zwecke der Werbung verarbeiten.*

Das BDSG-neu schreibt darüber hinaus allerdings – vergleichbar zum bisherigen Recht – vor, dass ein Datenschutzbeauftragter zu bestellen ist, soweit in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. Ein "ständig" in diesem Sinne ist bereits dann gegeben, wenn die datenverarbeitende Tätigkeit nicht die Kernaufgabe des

jeweiligen Mitarbeiters ist. Wenn bei einem Unternehmen mit Sitz in Deutschland oder einer deutschen Niederlassung also mindestens zehn Personen am Computer arbeiten, muss bereits ein Datenschutzbeauftragter bestellt werden. Beachten Sie, dass die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und der Datenschutzbehörde mitgeteilt werden müssen. Angedacht ist, dass die deutschen Behörden Online-Meldung ermöglichen, noch ist dies aber nicht der Fall.

4.18 Wann muss eine Datenschutzfolgenabschätzung durchgeführt werden?

Eine Datenschutzfolgenabschätzung ist zwingend, wenn bei der Datenverarbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Ziel ist, dass die Risiken vor der Verarbeitung erkannt und vorbeugende Maßnahmen getroffen sowie dokumentiert werden. Bei der Verarbeitung ausschließlich im Rahmen von Vertragsbeziehungen erhobener Kundendaten bzw. Interessentendaten für eigene Werbung ist in der Regel davon auszugehen, dass kein hohes Risiko besteht. Anders kann dies sein, wenn umfassende Profile gebildet werden, die sehr genaue Rückschlüsse auf die Lebensumstände der betroffenen Personen erlauben, Kundendaten mit Daten aus sozialen Netzwerken angereichert werden oder Bewegungsprofile (z. B. aus einer App-Nutzung) verwendet werden.

Sie haben weitere Fragen, auf die Sie in diesem Whitepaper keine Antworten finden konnten? Wenden Sie sich gerne an unseren Legal-Help-Desk:

https://www.owm.de/index.php?id=16

5. Weiterführende Links

Nachfolgend finden Sie weiterführende Links rund um das Thema Datenschutz-Grundverordnung:

- Die DSGVO in der **offiziellen deutschen Version** finden Sie hier:

  http://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679&from=DE

- Die Bayerische Datenschutzbehörde hat **zahlreiche Papiere der deutschen Datenschutzbehörden zur DSGVO** auf folgender Seite zusammengestellt:

  https://www.lda.bayern.de/de/datenschutz_eu.html

- **Richtlinien der europäischen Art. 29 Datenschutzgruppe** zur DSGVO u. a. zu den Themen Einwilligung, Transparenz, Datenübertragbarkeit, Meldungen bei Datenpanne, Datenschutzbeauftragten und Datenschutzfolgenabschätzung finden sich unter folgendem Link:

  http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- **Whitepaper der Bundesbeauftragten für den Datenschutz** und die Informationsfreiheit zur DSGVO mit weiterführenden Informationen u. a. zum technisch und organisatorischen Datenschutz:

  https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.pdf%3F__blob%3DpublicationFile%26v%3D24

- Ebenfalls bei der Bayerischen Datenschutzbehörde finden Sie auch eine **Synopse zu den verschiedenen Fassungen der e-Privacy-Verordnung**:

  https://www.lda.bayern.de/media/eprivacy_synopse.pdf

- Die uns beratende Kanzlei DLA Piper UK LLP hat auf Ihrer Internetseite umfassende **Praxishinweise rund um die DSGVO** in englischer Sprache vorgesehen:

  https://www.dlapiper.com/de/germany/focus/eu-data-protection-regulation/home/

ORGANISATION WERBUNGTREIBENDE IM MARKENVERBAND (OWM)
Unter den Linden 42
10117 Berlin

Ansprechpartner: Lars Gibbe
Tel.: +49/30/20 61 68 28
E-Mail: l.gibbe@owm.de