# UNVERZAGT VON HAVE

**WHITEPAPER**

# DATENSCHUTZ GRUNDVERORDNUNG

Was ist aus datenschutzrechtlicher Sicht im Hinblick auf die zukünftige Datenschutz-Grundverordnung (DSVO) zu ändern?

**Dr. Frank Eickmeier**

# WHITEPAPER

Die Datenschutz-Grundverordnung, kurz „DSGVO“ tritt ab dem 25.05.2018 europaweit in Kraft. Die DSGVO ersetzt zugleich die bislang geltenden nationalen Datenschutzvorschriften, in Deutschland insbesondere das Bundesdatenschutzgesetz (BDSG) und das Telemediengesetz (TMG). Beide Gesetze bleiben nur noch als Rumpfgesetze in Kraft. Die wesentlichen datenschutzrechtlichen Fragestellungen werden sich zukünftig aus der DSGVO ergeben. Für die Onlineunternehmen ist darüber hinaus die sog. ePrivacy-Verordnung zu beachten, die seit Januar 2017 als Entwurf vorliegt.

## Was sind die wichtigsten Änderungen durch die DSGVO, die Unternehmen in der EU zukuntig berücksichtigen sollten:

### 1. NEUE DATENSCHUTZERKLÄRUNGEN, NEUE INFORMATIONSPFLICHTEN:

Die Art. 12 ff. DSGVO regeln neue Informationspflichten, die in weiten Teilen über die bisherigen Informationspflichten, die in einer Datenschutzerklärung abzubilden waren, hinausgehen. Falls noch nicht geschehen, müssen die Verfahrensverzeichnisse und/oder Datenschutzerklärungen um folgende Punkte ergänzt werden:

- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters;
- ggf. die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen sowie die Rechtsgrundlage für die Verarbeitung;
- wenn die Verarbeitung auf Art. 6 Abs. 1 f DSGVO beruht, die berechtigten Interessen, die von den Verantwortlichen oder einem Dritten verfolgt werden;
- ggf. die Empfänger oder Kategorien von Empfängern der personenbezogene Daten;
- ggf. die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln;
- die Dauer des Speicherung der Daten;

- Informationen über das Bestehen eines Rechts auf Auskunft, Berichtigung oder Löschung;

- Information darüber, ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist;

- das Vorhandensein von sog. „Profiling“ und in diesen Fällen aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

## 2. NEUE DEFINITION DER PERSONENBEZOGENEN DATEN - UND WAS HABEN COOKIE- ID´S DAMIT ZU TUN

Der Begriff der personenbezogenen Daten wurde in der DSGVO neu definiert. Prüfen Sie daher, welche Auswirkungen das auf Ihr Geschäftsmodell hat. Viele Daten, die früher als anonym galten, sind zukünftig Daten mit Personenbezug. „Personenbezogene Daten“ im Sinne der DSGVO sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu

- einer Kennung wie einem Namen,

- zu einer Kennnummer,

- zu Standortdaten,

- zu einer Online-Kennung oder

- zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Wichtig für die Onlinebranche ist insoweit ein durch die DSGVO eingeführter Paradigmenwechsel. Während es früher umstritten war, ob Online-Identifier wie Cookie ID´s, User ID´s, Mac Adressen u.ä. personenbezogene Daten waren, gelten sie nunmehr in der Regel als personenbezogen. Denn es handelt sich hierbei um eine „Online-Kennung“ im oben erwähnten Sinne. Die praktischen Auswirkungen sind erheblich. Denn wenn es sich bei Online ID´s um personenbezogene Daten handelt, dann bedarf jede Erhebung oder Nutzung dieser ID´s – etwa im Rahmen von Online-Werbung – der Einwilligung des Nutzers. Deshalb gelangt in diesen Fällen

der neue Art. 6 Abs. 1 f DSGVO zur Anwendung (siehe unten 3.), der zukünftig für die Onlinewerbebranche von kaum zu überschätzender Bedeutung werden dürfte.

## 3. NEUE REGELN FÜR ONLINEWERBUNG

Durch die DSGVO hat sich an dem Grundprinzip im Datenschutzrecht nichts geändert. Die Verarbeitung von personenbezogenen Daten ist nur zulässig, wenn eine Einwilligung der betroffenen Person vorliegt oder das Gesetz eine Datenverarbeitung gestattet. Neu sind aber die Erlaubnistatbestände im Art 6 DSGVO. Insbesondere **Art. 6 Abs. 1 f DSGVO** enthält eine für die Praxis weitreichende und zum Teil neue Regelung. Denn danach ist die Verarbeitung von personenbezogenen Daten auch ohne eine ausdrückliche Einwilligung zulässig, wenn die Verarbeitung zur Wahrung der „berechtigten Interessen“ des Verantwortlichen (des Werbetreibenden) oder eines Dritten (z.B. eines Kooperationspartners) erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Bei diesen berechtigten Interessen handelt es sich auch um die Interessen der Werbeindustrie. Diese sind also nicht von vornherein weniger wert, als die Interessen der Betroffenen, etwa die Besucher einer Website. Prüfen Sie daher dringend, welchen Einfluss die neuen Regeln zur Onlinewerbung für Ihr Unternehmen haben werden.

## 4. NEUE REGELN FÜR DIE EINWILLIGUNG VON KINDERN

Art. 8 DSGVO bestimmt zukünftig, dass die Einwilligung eines Kindes nur wirksam ist, wenn das Kind das 16. Lebensjahr vollendet hat. Hat das Kind noch nicht das 16. Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern durch die Eltern die Zustimmung erteilt wird.

## 5. NEU: PROFILING – UND WARUM NUTZERPROFILE KEIN PROFILING SIND

Neu ist in der DSGVO der Begriff des „Profilings“. Jede Person sollte nah dem Willen des Gesetzgebers das Recht haben, keiner Entscheidung zur Bewertung von sie betreffenden persönlichen Aspekten unterworfen zu werden, die ausschließlich auf einer automatisierten Verarbeitung beruht und die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, wie

die automatische Ablehnung eines Online-Kreditantrags oder Online-Einstellungsverfahren ohne jegliches menschliche Eingreifen.

Zu einer derartigen Verarbeitung zählt auch das sog. „Profiling“, das in jeglicher Form automatisierter Verarbeitung personenbezogener Daten unter Bewertung der persönlichen Aspekte in Bezug auf eine natürliche Person besteht, insbesondere zur Analyse oder Prognose von Aspekten bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person.

Dies gilt allerdings nur, soweit dies *rechtliche Wirkung* für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Im Klartext heißt das, dass jede Form von Nutzerprofilen im Rahmen der Onlinewerbung *nicht* darunter fallen. Denn diese haben in der Regel keine „rechtlichen Wirkungen“.

## 6. NEUE REGELN ZUR AUFTRAGSVERARBEITUNG

Es wird neue Regeln zur Auftragsdatenverarbeitung geben, die zukünftig schlicht „Auftragsverarbeitung“ heißen wird. Zwar gelten viele Grundsätze die in Deutschland seit langem bekannt sind auch zukünftig weiter. Es wird aber einige Änderungen geben, die eine Anpassung der „Auftragsverarbeitungsverträge“ erforderlich machen werden.

Die nach dem BDSG privilegierte Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (§ 3 Abs. 8 Satz 3 und § 11 BDSG), wonach der per Auftrag eingesetzte Dienstleister nicht Dritter ist, sondern sozusagen ein „Innenverhältnis“ ohne Prüfschranken für eine Datenübermittlung gesetzlich bestimmt wird, findet sich in vergleichbarer Weise auch in der DSGVO wieder. Denn nach Art. 4 Nr. 10 DSGVO ist ein Auftragsverarbeiter nicht Dritter. Neu ist aber, dass die DSGVO keine Beschränkung der Privilegierung der Auftragsverarbeitung auf den EU-/EWR-Raum enthält, wie sich dies bisher aus der Eingrenzung in § 3 Abs. 8 Satz 3 BDSG ergab.

Allerdings legt die DSGVO den Auftragsverarbeitern künftig mehr Verantwortung und mehr Pflichten auf. Die zentrale Vorschrift für Auftragsverarbeiter in der DSGVO ist zukünftig Art. 28 DSGVO. Dort wird in Absatz 1 zunächst die *Prüfung* der Geeignetheit eines Auftragsverarbeiters eingefordert. Der Verantwortliche darf nach dieser Bestimmung nur Auftragsverarbeiter einsetzen, die hinreichend Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz haben.

Wie bisher muss mit dem Auftragsverarbeiter im Regelfall ein Vertrag über die Auftragsverarbeitung geschlossen werden, der schriftlich oder, und das ist neu, auch in *elektronischer* Form geschlossen sein kann.

Für alle Auftragsverarbeiter besteht zukünftig die *neue Pflicht*, ein Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO für alle Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung führen. Diese müssen der Aufsichtsbehörde auf Anfrage, z. B. bei Kontrollen, zur Verfügung gestellt werden.

Neu ist zukünftig auch der Begriff „gemeinsamen Verantwortlichen“ (Joint controller). Legen nach Art. 26 DSGVO zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel zur Verarbeitung fest, so sind sie „gemeinsam Verantwortliche“. Sie legen dann in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten nachkommt.

## 7. DATENSCHUTZRECHTLICHE VOREINSTELLUNGEN, ART. 25 DSGVO

Neu ist die Verpflichtung zukünftig bei allen Unternehmen, datenschutz-freundliche Voreinstellungen vorzunehmen. Es besteht gemäß Art. 25 DSGVO zukünftig die Pflicht, geeignete technische und organisatorische Maßnahmen vorzunehmen, die sicherstellen, dass durch die Voreinstellung grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, auch wirklich verarbeitet werden. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Solche Maßnahmen müssen insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden.

Überprüfen Sie daher, ob Ihre IT diese Anforderungen zukünftig erfüllt.

## 8. ÜBERARBEITEN SIE IHRE VERFAHRENSVERZEICHNISSE – ABER: NICHT MEHR JEDER BRAUCHT DAS VERZEICHNIS

Art. 30 DSGVO legt neue Anforderungen für ein Verfahrensverzeichnis fest, dass zukünftig „Verzeichnis aller Verarbeitungstätigkeiten“ heißen wird. Nach Art. 30 DSGVO muss jeder Verantwortliche ein sog. „Verzeichnis aller Verarbeitungstätigkeiten“ führen, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält zukünftig folgende Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation;
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

Das Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann. Der Verantwortliche (oder der Auftragsverarbeiter, für den diese Regeln auch weitestgehend gelten) stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

Die genannten Pflichten gelten aber nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, es sei denn,

- die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen,

- **die Verarbeitung erfolgt nicht nur gelegentlich** oder

- es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art. 9 Abs. 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10.

Für die **Onlinebranche** bedeutet dies, da gerade hier viele Unternehmen eine Datenverarbeitung nicht nur „gelegentlich“ durchführen, sondern das geradezu der Hauptzweck der geschäftlichen Tätigkeit ist, die Unternehmen von der Pflicht zur Erstellung des Verzeichnisses in der Regel nicht freigestellt sind. Jedes Unternehmen, das also im Bereich der Onlinewerbung mit Themen wie Targeting, Nutzerprofilen, Cookie-IDs u. ä. befasst ist, ist deshalb nach wie vor zur Erstellung eines entsprechenden Verzeichnisses von Verarbeitungstätigkeiten verpflichtet.

## 9. NEU: DIE SOG. DATENSCHUTZ-FOLGENABSCHÄTZUNG

Neu eingeführt wurde die sog. Datenschutz-Folgenabschätzung, Art. 35 DSGVO. Hat nach dieser Vorschrift eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich „ein hohes Risiko“ für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche – also das Unternehmen - vorab „eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch“. Dabei ist der Rat des Datenschutzbeauftragten einzuholen (Art. 35 Abs.2 DSGVO).

Diese Datenschutz-Folgenabschätzung ist insbesondere in folgenden Fällen erforderlich:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die **Rechtswirkung** gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche;

Die Aufsichtsbehörden werden zudem zukünftig eine Liste der Verarbeitungsvorgänge erstellen, für die immer eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese.

Für die **Onlinebranche** enthält die oben erwähnte erste Voraussetzung eine wichtige Einschränkung. Denn danach bedarf eine automatisierte Verarbeitung von Daten – die in der Onlinebranche häufig vorkommt – nur dann einer Datenschutz-Folgenabschätzung, wenn diese **Rechtswirkung** gegenüber natürlichen Personen entfaltet. Die Auslieferung von programmatischer Werbung auf der Basis von möglicherweise erstellten Nutzerprofilen entfaltet aber in der Regel keine Rechtswirkung. In vielen Fällen der Onlinewerbung wird es deshalb nicht erforderlich sein, eine solche Datenschutzfolgenabschätzung vorzunehmen. Umso wichtiger ist es aber für das eigene Unternehmen festzustellen, ob diese Voraussetzung erfüllt ist oder nicht.

Ist aber eine Folgenabschätzung erforderlich, dann sollte sie zumindest folgendes enthalten (Art. 35  Abs. 7 DSGVO):

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

## 10. RECHT AUF LÖSCHUNG (RECHT AUF VERGESSENWERDEN), ART. 17 DSGVO

Art. 17 DSGVO hat ein neues Recht, das sog. „Recht auf Vergessenwerden“ eingeführt. Geblieben sind aber die üblichen Rechte auf Löschung der eigenen personenbezogenen Daten.
Insoweit bestimmt Art. 17 Abs. 1 DSGVO zunächst, dass jeder Betroffene das Recht

hat, von dem jeweils Verantwortlichen zu verlangen, das ihn betreffende personenbezogene Daten unverzüglich gelöscht werden, sofern einer der nachfolgenden Gründe zutrifft:

- Die personenbezogenen Daten sind für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig.
- Die betroffene Person widerruft ihre Einwilligung.
- Die betroffene Person legt Widerspruch gegen die Verarbeitung ein und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor.
- Die personenbezogenen Daten wurden unrechtmäßig verarbeitet.
- Die Löschung der personenbezogenen Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich.

## 11. RECHT AUF DATENÜBERTAGBARKEIT

Neu ist auch das Recht auf Datenübertragbarkeit, Art. 20 DSGVO. Jede betroffene Person hat danach das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen – zum Beispiel Facebook - bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Ferner hat sie das Recht, diese Daten einem anderen Verantwortlichen (zum Beispiel Google +) ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

## 12. NEUE BENACHRICHTIGUNGSPFLICHT BEI DATENPANNEN

Wie schon bisher in § 42 a BDSG geregelt, besteht nach wie vor eine Informationspflicht bei unrechtmäßiger Kenntniserlangung bestimmter personenbezogener Daten.

Gem. Art. 33 DSGVO ist jeder Verantwortliche verpflichtet, im Falle einer Verletzung des Schutzes personenbezogener Daten unverzüglich – und das ist neu – möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese bei der zuständigen Aufsichtsbehörde zu melden. Dies gilt nur dann nicht, wenn die Verletzung voraussichtlich nicht zu einem Risiko „für die Rechte und Freiheiten natürlicher Personen“ führt. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72

Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen. Neu ist auch die in Abs. 5 geregelte Verpflichtung, wonach der Verantwortliche verpflichtet ist, sämtliche Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen von Art. 33 DSGVO ermöglichen.

Jede Meldung muss folgende Informationen enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

## 13. SICHERHEIT DER DATENVERARBEITUNG

Die DSGVO verpflichtet auch zukünftig jeden Verantwortlichen dazu, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Datenschutzrisiko angemessenes Schutzniveau zu gewährleisten. Diese Maßnahmen haben unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu erfolgen. Diese Maßnahmen können u. a. folgendes einschließen:

- Eine Pseudonymisierung und Verschlüsselung personenbezogener Daten.

- Die Fähigkeit, die Vertraulichkeit Integrität und Verfügbarkeit von Daten sicherzustellen.

- Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und Zugang zu

Ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherstellen zu können.

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Überprüfen Sie daher Ihre heute schon bestehenden technischen und organisatorischen Maßnahmen (die sog. TOM´s) und stellen Sie sicher, dass zukünftig eine regelmäßige Überprüfung und die damit einhergehende Dokumentation für die Zukunft sichergestellt wird.

## 14. NEUE AUFGABEN UND PFLICHTEN DES DATENSCHUTZBEAUFTRAGTEN

Auch zukünftig wird es in Deutschland erforderlich sein, einen Datenschutzbeauftragten zu bestellen. Denn in Deutschland wir die Bestellpflicht eines Datenschutzbeauftragten abweichend zur DSGVO geregelt, und zwar in dem sog. Allgemeinen Bundesdatenschutzgesetz (ABDSG). Demnach muss ein Datenschutzbeauftragter bestellt werden, wenn mindestens 10 Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Auch der verschärfte Kündigungsschutz gilt, wie schon heute im BDSG geregelt, unverändert auch nach Geltung der DSGVO fort. Neu ist, dass Art. 37 Abs. 7 DSGVO vorsieht, dass der „Verantwortliche oder Auftragsverarbeiter“ die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und diese Daten der Aufsichtsbehörde mitteilt.

Für die Verletzung dieser Pflichten kann nach der DSGVO zukünftig gem. § 83 Abs. 4 ein Bußgeld verhängt werden, und zwar in Höhe bis zu 10 Mio. Euro oder 2% des weltweiten Jahresumsatzes, je nachdem welcher Betrag höher ist.

## 15. NEUE BUSSGELDER UND SANKTIONEN

Der heutige Bußgeldrahmen des BDSG beläuft sich noch je nach Schwere des Verstoßes auf bis zu 50.000,00 Euro bzw. 300.000,00 Euro. Die DSGVO bringt hier in Art. 83 ff. weitreichende Verschärfungen. Der neue Bußgeldrahmen der DSGVO beläuft sich je nach Schwere des Verstoßes auf Geldbußen bis zu 10. Mio. Euro oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes, je nachdem, welcher der Beträge höher ist. Bei Verstößen gegen die Bestimmungen der Art. 5, 6, 7 und 9 – also insbesondere bei der Verarbeitung von personenbezogenen

Daten – steigt der Bußgeldrahmen auf bis zu 20 Mio. Euro oder im Falle eines Unternehmens von bis zu 4 % seiner gesamten weltweit erzielten Jahresumsatzes.

## 16. HAFTUNGSERSTRECKUNG AUF AUSLÄNDSCHE UNTERNEHMEN

Die Haftung nach der DSGVO trifft zukünftig auch vermehrt ausländische Unternehmen, selbst wenn diese keine eigene Filiale in einem Mitgliedsstaat der europäischen Union unterhalten. Gem. Art. 3 DSGVO reicht es aus, das ausländische Unternehmen entweder betroffenen Personen in der EU Waren oder Dienstleistungen anbieten oder – und das dürfte für die Onlinemarketingbranche wichtig sein – dass diese Unternehmen das Verhalten betroffener Personen „beobachten“, soweit ihr Verhalten in der EU erfolgt. Unternehmen der Onlinemarketingbranche, die also Techniken insbesondere zur Nachverfolgung von Internetaktivitäten, wie z. B. bei Tracking, Profiling und Targeting einsetzen, haften nach den Bestimmungen der DSGVO selbst wenn sie keine eigene Filiale in der EU besitzen.

## 17. ERWEITERTE DOKUMENTATIONS- UND NACHWEISPFLICHTEN

Die Datenschutzgrundverordnung sieht für Verantwortliche und Auftrags-verarbeiter in vielen Fällen deutlich erweiterte Dokumentationspflichten vor. So schreibt Art. 5 Abs. 2 DSGVO vor, dass der für die Verarbeitung verantwortliche nachweisen können muss, dass er die in Art. 5 Abs. 1 DSGVO geregelten Datenschutzgrundsätze einhält. Verstößt ein verantwortliches Unternehmen gegen diese Vorgabe, drohen Bußgelder wie oben erwähnt von bis zu 4 % des Umsatzes.

Nach Art. 24 Abs. 1 DSGVO muss der für die Verarbeitung verantwortliche über dies nachweisen können, dass er personenbezogene Daten in Übereinstimmung mit der DSGVO verarbeitet. Auftragsverarbeiter müssen den Verantwortlichen alle erforderlichen Informationen zur Verfügung stellen, damit der Verantwortliche nachweisen kann, dass er seine in den Art. 32 ff. DSGVO geregelten Pflichten erfüllt.

## 18. DATENSCHUTZMANAGEMENTSYSTEME

Die Anforderungen an die Unternehmen, an ihre Datenschutzorganisation und Datenschutzprozesse werden zukünftig stark steigen. Das liegt vor allem an dem sog. risikobasierten Datenschutz, der an vielen Stellen in der DSGVO etabliert wurde. Gerade die

Anforderungen der Art. 24 und 25 DSGVO sowie der stark gestiegene Bußgeldrahmen werden es deshalb zukünftig in vielen Fällen erforderlich machen, sog. Datenschutzmanagementsysteme zu entwickeln. Unter einem Datenschutzmanagementsystem versteht man die Gesamtheit aller dokumentierten und implementierten Regelungen, Prozesse und Maßnahmen, die dazu dienen, einen datenschutzkonformen Umgang mit personenbezogenen Daten im Unternehmen systematisch zu steuern.

**Dr. Frank Eickmeier**

Dr. Frank Eickmeier ist als Rechtsanwalt Partner bei der Kanzlei Unverzagt von Have in Hamburg tätig (www.unverzagtvonhave.com)

Weiterhin ist er Gründungsgesellschafter der ePrivacy GmbH (www.eprivacy.eu) und akkreditierter Gutachter beim unabhängigen Landeszentrum für Datenschutz in Kiel. In Hamburg ist er Mitglied des Fachausschusses für Urheber- und Medienrecht der Hansetischen Rechtsanwaltskammer. Als Speaker und Referent ist er regelmäßig auf großen Konferenzen zum Thema Onlinemarketing und Datenschutz anzutreffen. In seinem Blog: www.onlinemarketingrecht.de publiziert und kommentiert er neueste Entwicklungen.

## SPEZIALISIERUNG

- Onlinemarketingrecht
- Datenschutzrecht
- DSGVO (Datenschutzgrundverordnung)

eickmeier@unverzagtvonhave.com
+49.40.414000-34

LinkedIn XING

## EMPFEHLUNGEN

- The Legal 500 Deutschland – 2016
- „Focus Spezial – Deutschlands Top-Anwälte“

## MEMBER OF

- World **IT** Lawyers
- Bundesverband Digitale Wirtschaft (BVDW) e.V.