Mandantenbrief

Neues zum Datenschutzrecht

Handreichung zum Thema

EU-Datenschutzgrundverordnung und neues

Bundesdatenschutzgesetz

Allgemeine Hinweise
zu datenschutzrechtlichen Änderungen sowie
Empfehlungen zur Überprüfung des eigenen
Datenschutzkonzeptes

Einführung

Am 25. Mai 2018 treten die neue EU-Datenschutzgrundverordnung (DSGVO) sowie das insgesamt neu gefasste Bundesdatenschutzgesetz (BDSG neu) in Kraft. Beide Vorschriften sind unmittelbar in Deutschland anwendbar und müssen für die datenschutzrechtliche Beurteilung gemeinsam berücksichtigt werden.

Während die DSGVO einen Datenschutzstandard schafft, der unmittelbar in allen Mitgliedstaaten der EU gilt, enthält das neue BDSG wichtige Vorschriften zur Durchführung der DSGVO in Deutschland sowie diverse Konkretisierungen.

Im Folgenden erhalten Sie die wichtigsten Informationen, um beurteilen zu können, ob und inwiefern die neuen Vorschriften Anlass zur Überprüfung ihres Datenschutzkonzeptes geben. Dabei lassen sich die durchschnittlichen Anforderungen mit überschaubarem Aufwand selbstständig bewältigen. Da das neue Datenschutzrecht eine Reihe von standardisierten Informationspflichten und Prozeduren vorsieht, möchten wir Sie gerne in die Lage versetzen, hier möglichst eigenständig die vorgesehenen Vorkehrungen zu treffen und erlauben uns, zu diesem Zweck an den passenden Stellen mit Links auf kostenfreie Angebote im Internet hinzuweisen.

Wer wird durch das neue Datenschutzrecht verpflichtet?

Das neue Datenschutzrecht gilt für alle Personen und Unternehmen, die personenbezogene Daten in eigener Verantwortung verarbeiten und dies nicht nur zum privaten oder familiären Gebrauch tun.

Auch auf Vereine, Verbände, Stiftungen und sonstige Einrichtungen sowie freiberuflich Tätige, die regelmäßig personenbezogene Daten erheben und verarbeiten, ist das neue Datenschutzrecht anwendbar. Zuständig ist in der Regel der Vorstand oder die Geschäftsführung. Speziell für Vereine weisen wir gerne ohne rechtliche Gewähr auf diesen Praxisratgeber hin:

https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf

Welche Daten sind betroffen?

Die DSGVO gilt für fast jede Form der Verarbeitung personenbezogener Daten. Nicht nur die Eingabe und Speicherung auf dem PC fällt darunter, sondern auch ein nach bestimmten Kriterien geordnetes Karteikartensystem.

Personenbezogene Daten 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, die Ausdruck der physischen, psychischen, wirtschaftlichen, kulturellen, sozialen Identität dieser natürlichen Person sind, identifiziert werden kann (Art. 4 Nr. 1 DSGVO).

Beispiele sind: Name, Wohnort, Kontoverbindung, E-Mail-Adresse, Religionszugehörigkeit aber auch IP-Adressen oder Online-Kennungen.

Verarbeiten ist ein weit zu verstehender Begriff, der sämtliche Tätigkeiten mit personenbezogenen Daten umfasst: das Erheben der Daten (beschaffen und sammeln), Speichern, Ändern (einer E-Mail-Adresse), Nutzen (Abfragen), Übermitteln, Verknüpfen, Löschen.

- Für **besonders sensible Daten** gelten strengere Maßstäbe (Art. 9 Abs. 1 DSGVO). Darunter fällt die Verarbeitung von
    - Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,
    - genetischen oder biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person,
    - Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

  Die Verarbeitung dieser Daten darf nur unter bestimmten Voraussetzungen erfolgen, wie etwa bei einer entsprechenden ausdrücklichen Einwilligung der betroffenen Person (Art. 9 Abs. 2 lit. a DSGVO), oder wenn eine gesetzliche Erlaubnis besteht, wie beispielsweise im Rahmen einer therapeutischen Behandlung (Art. 9 Abs. 2 lit. h DSGVO i.V.m. § 22 Abs. 1 Nr. 1 lit. b BDSG), zur Erfüllung spezieller Pflichten aus dem Sozialrecht oder zur Wahrung von Rechtsansprüchen.

- Auch die Verwendung von **Cookies** auf Internetseiten fällt unter die DSGVO, unabhängig davon ob diese die IP-Adresse des Nutzers beinhalten oder nur pseudonymisierte Daten. Während nach der bisherigen Rechtslage für Cookies mit lediglich pseudonymisiertem Dateninhalt keine Einwilligung erforderlich war (Privilegierung nach § 15 Abs. 3 TMG), enthält die DSGVO eine solche Privilegierung nicht, so dass die Verarbeitung in Zukunft grundsätzlich auch einer Einwilligung bedarf. Allenfalls, wenn der Einsatz von Cookies zur „Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen“ (Art. 6 Abs. 1 Satz 1 lit. f DSGVO), könnte der Einsatz von Cookies ohne Einwilligung gerechtfertigt sein. Wann dies der Fall ist, lässt sich hingegen nicht pauschal beantworten und hängt von der in jedem Einzelfall vorzunehmenden Interessenabwägung ab. Als rechtssicherste Variante bietet sich in jedem Fall die Einholung einer Einwilligung an. Es ist allerdings darauf hinzuweisen, dass die in der nächsten Zeit zu erwartende EU-Verordnung zum Thema *ePrivacy* voraussichtlich bereits wiederum neue und speziellere Regelungen hierzu enthalten wird.
- Inwiefern **Fotos** unter den Begriff der personenbezogenen Daten und damit in den Anwendungsbereich der DSGVO fallen, ist noch völlig offen, und wird vermutlich erst im Laufe der nächsten Jahre durch entsprechende Gerichtsurteile geklärt werden. Unabhängig davon gilt jedoch gemäß § 22 KUG weiterhin der Grundsatz, dass Veröffentlichungen nur mit Einwilligung der betroffenen Person erfolgen dürfen und zwar unabhängig davon, ob es sich dabei ums Internet, das Intranet oder ein Informationsheft handelt.

Was muss gewährleistet sein?

Datensicherheit

Die DSGVO sieht vor, dass die Verantwortlichen geeignete technische und organisatorische Maßnahmen ergreifen, um ein dem Risiko angemessenes Schutzniveau der Daten zu gewährleisten. Die Maßnahmen hängen im Einzelfall vom Stand der Technik, den Implementierungskosten und der Art, dem Umfang, den Umständen und den Zwecken der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ab (Art. 32 DSGVO). Sie schließen unter anderem ein

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Außerdem müssen Schritte unternommen werden, um sicherzustellen, dass Mitarbeiter, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten.

Dokumentation der Datenverarbeitung

Das neue Datenschutzrecht schreibt die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten vor (Art. 30 DSGVO). Freigestellt sind davon lediglich Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen und nur gelegentlich personenbezogene Daten verarbeiten und auch nur, wenn darunter keine besonderen Datenkategorien wie Gesundheits- oder Religionsdaten sind. Dies dürfte jedoch auf die wenigsten Einrichtungen zutreffen, denn selbst Vereine verwalten die personenbezogenen Daten ihrer Mitglieder nicht nur gelegentlich sondern permanent und verarbeiten bei angestellten Mitarbeitern in der Regel auch Daten über Krankheitstage oder die Kirchensteuerpflicht, so dass eine Freistellung nicht unbedingt nahe liegt und zumindest im Hinblick auf mögliche Aufsichtsmaßnahmen einer eingehenden Überprüfung bedarf.

Das Verzeichnis dient dem Nachweis einer DSGVO-konformen Datenverarbeitung gegenüber der Aufsichtsbehörde. Es ist stets aktuell zu halten und muss mindestens die folgenden Bestandteile aufweisen

- Name und Kontaktdaten des Verantwortlichen
- Zwecke der Verarbeitung
- Datenkategorien (Adressdaten, Geburtsdaten, Bankverbindung, Steuermerkmale etc.)
- Beschreibung der Kategorien betroffener Personen (Mitarbeiter, Mitglieder, Schüler, Lieferanten)

- Kategorien von Empfängern von Daten einschließlich Empfänger in Drittstaaten (interne Empfänger, externe Empfänger, Sitz außerhalb EU z.B. bei Webmail-Diensten oder Cloud-Diensten)
- Vorgesehene Fristen zur Löschung
- Maßnahmen zur Datensicherheit

Für das Verzeichnis ist kein bestimmter Aufbau vorgeschrieben. Es muss in deutscher Sprache schriftlich oder elektronisch geführt werden. Da die Angaben aussagekräftig sein müssen, müssen sie umso detaillierter sein, je größer die Einrichtung, das Unternehmen oder der Verein ist. Ein umfassendes Verzeichnis enthält darüber hinaus eine Dokumentation über jede einzelne Datenverarbeitungstätigkeit, wie deren Rechtsgrundlage, die erteilte Einwilligung, Einhaltung der Informationspflichten etc.

Die folgenden Links verweisen auf Muster und Vorlagen für die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten. Gleichwohl können wir für die dort zu findenden Inhalte keine Richtigkeitsgewähr bieten.

https://www.bvdnet.de/muster-fuer-verzeichnisse-gemaess-art-30/

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_5.pdf

Bestellung eines Datenschutzbeauftragten?

Auch nach neuer Rechtslage sind Einrichtungen in Deutschland weiterhin verpflichtet, einen Datenschutzbeauftragten beispielsweise dann zu bestellen, wenn sie in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigen (Art. 37 Abs. 1 DSGVO, § 38 BDSG neu). Dabei handelt es sich um eine reine „pro-Kopf-Zahl“, so dass es weder auf die Stellung der Personen in der Einrichtung (Leitung oder Aushilfskraft) noch auf den Umfang ihrer Tätigkeit (50% Stelle) für die Frage ankommt, ob zehn Personen derart beschäftigt sind.

Verantwortung gegenüber betroffenen Personen

Betroffene Person ist jede natürliche Person, die durch personenbezogene Daten identifiziert werden kann oder identifizierbar wird. Ihr werden in der DSGVO umfassende Rechte eingeräumt. Neu ist vor allem das erweiterte Recht zu erfahren, was mit den eigenen Daten passiert. Darunter fällt u.a.:

- Das Recht bei Erhebung von personenbezogenen Daten über den Vorgang informiert zu werden, wobei gewisse Pflichtinformationen erfolgen müssen (Art. 13 Abs. 1 DSVO)
- Informationsrechte, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DSGVO)
- Das Recht von dem Verantwortlichen zu erfahren, ob personenbezogene Daten verarbeitet werden und wenn ja, mit welchen Zwecken, für welche Dauer mit welchen Empfängern u.v.m. (Art. 15 DSGVO)
- Das Recht auf Berichtigung der Daten (Art. 16 DSGVO)
- Das Recht auf Löschung der Daten (Art. 17 DSGVO)

- Das Recht, unter gewissen Voraussetzungen die Einschränkung der Verarbeitung der Daten zu verlangen (Art. 18 DSGVO)
- Das Recht, grundsätzlich jederzeit gegen die Verarbeitung sie selbst betreffender personenbezogener Daten Widerspruch einzulegen (Art. 21 Abs. 1 DSGVO), wobei hierauf bereits zum Zeitpunkt der ersten Kommunikation ausdrücklich und in einer verständlichen und von anderen Informationen getrennten Form hingewiesen werden muss (Art. 21 Abs. 4 DSGVO)
- Das Recht für den Fall der Verletzung des Schutzes personenbezogener Daten, die voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, unverzüglich benachrichtigt zu werden, soweit keine gesetzlichen Ausnahmen bestehen (Art. 34 Abs. 1 DSGVO)
- Diese Rechte können auch dann ggü. dem Verantwortlichen geltend gemacht werden, wenn sich dieser eines Auftragsverarbeiters bedient.

Generell gilt, dass die Verarbeitung personenbezogener Daten nur für die konkret festgelegten Zwecke (die vorab feststehen müssen) erfolgen darf, unabhängig davon, ob sie auf Basis einer Einwilligung, eines Vertrages oder einer Interessenabwägung beruht. Fallen diese Zwecke weg und bestehen keine sonstigen gesetzlichen Verpflichtungen zur Aufbewahrung, müssen die persönlichen Daten unaufgefordert gelöscht werden.

In Bezug auf sog. Mailing-Listen, bzw. Newsletter bedeutet das u.a., dass grundsätzlich nur für diesen Zweck erforderliche Daten verarbeitet werden dürfen, also nur die E-Mail-Adresse. Fällt der Zweck der Datenverarbeitung später Weg und gibt es keine anderweitige Rechtspflicht, die Daten weiterhin zu speichern, so müssen diese gelöscht werden. Insofern darf die Einwilligung in die Aufnahme einer Mailing-Liste auch nur von der Angabe der E-Mail-Adresse abhängig gemacht werden. Überdies können auch die bereits erwähnten Informationspflichten ggü. den Betroffenen eine Anpassung der Einwilligungserklärung erforderlich machen.

Verantwortung gegenüber Aufsichtsbehörden

Im Falle der Verletzung des Schutzes personenbezogener Daten besteht eine Meldepflicht gegenüber der zuständigen Aufsichtsbehörde. Die Frist für die Meldung kann unter Umständen 72 Stunden betragen (Art. 33 DSGVO), wobei die Meldung in jedem Fall besonderen gesetzlich bestimmten inhaltlichen Anforderungen genügen muss.

Zugleich besteht für den Fall der Datenschutzverletzung eine umfassende Dokumentationspflicht, die der Aufsichtsbehörde zur Überprüfung des Vorfalles dient.

Verantwortung beim Einsatz von Auftragsverarbeitern

Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften der DSGVO sowie des neuen BDSG zu sorgen (Art. 28 DSGVO, § 62 BDSG neu). Danach darf ein Verantwortlicher nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Maßnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der

Rechte der betroffenen Personen gewährleistet wird (§ 62 BDSG neu). Der Verantwortliche hat mit dem Auftragsverarbeiter einen bestenfalls schriftlichen Vertrag abzuschließen. Darin festzulegen sind der Gegenstand, Dauer, Art und Zweck der Verarbeitung, Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen.

Von dieser vertraglichen Gestaltung können beispielsweise Aufträge gegenüber Unternehmen betroffen sein, die den Webseiten-Auftritt pflegen oder die Lohnbuchhaltung durchführen.

Ohne Gewähr für deren inhaltliche Richtigkeit finden Sie Vertragsmuster zur Auftragsverarbeitung unter folgendem Link:

https://www.gdd.de/downloads/praxishilfen/GDD-Praxishilfe_DS-GVO_4.pdf

Was bedeutet das für die Datenschutzerklärung?

Die Informationspflichten gegenüber betroffenen Personen (Art. 13 und 14 DSGVO) in Bezug auf die internetbasierte Kommunikation hinsichtlich des Besuchs einer Internetseite lassen sich durch eine entsprechende Datenschutzerklärung erfüllen, die allerdings den neuen Regelungen angepasst werden sollte. Soweit erforderlich sollte die Datenschutzerklärung Informationen zu folgenden Themen beinhalten:

- Name und Kontaktdaten des für die Verarbeitung Verantwortlichen sowie eines betrieblichen Datenschutzbeauftragten (falls erforderlich und bestellt)
- Erhebung und Speicherung personenbezogener Daten sowie Art und Zweck von deren Verwendung
  - beim Besuch der Webseite
  - Bei der Anmeldung für den Newsletter
  - Bei Nutzung des Kontaktformulars
- Weitergabe von Daten
- Cookies
- Analyse-Tools
- Social Media Plug-ins
- Betroffenenrechte
- Widerspruchsrecht
- Datensicherheit
- Aktualität und Änderung der Datenschutzerklärung

Hilfen zur Erstellung einer Datenschutzerklärung – ohne Richtigkeitsgewähr – finden Sie hier:

https://www.e-recht24.de/muster-datenschutzerklaerung.html

https://www.activemind.de/datenschutz/datenschutzhinweis-generator/

Wie wird die Einhaltung des Datenschutzes kontrolliert?

Die für den Datenschutz zuständige Aufsichtsbehörde des jeweiligen Bundeslands kontrolliert die Einhaltung des Datenschutzrechts. Hierfür hat sie umfassende gesetzliche Befugnisse. Nicht nur können sie die Verantwortlichen anweisen, sämtliche Informationen bereitzustellen, die er-

forderlich sind, um die Einhaltung der Datenschutzvorschriften überprüfen zu können. Sie sind auch befugt unangekündigte Datenschutzprüfungen vor Ort durchzuführen.

Darüber hinaus befasst sich die Aufsichtsbehörde mit Beschwerden von Betroffenen im Hinblick auf etwaige Verstöße oder geht diesen von Amts wegen nach. Beschweren sich in Zukunft Kunden, Geschäftspartner oder Mitarbeiter bei der zuständigen Datenschutzbehörde, darf die Behörde nicht untätig bleiben und muss den Beschwerden nachgehen.

Was droht bei Verstößen?

Verstöße gegen Datenschutz können ernsthafte rechtliche Folgen nach sich ziehen. Die DSGVO hat die bisherigen Regelungen deutlich verschärft. Dies gilt sowohl im Hinblick auf denkbare Bußgelder als auch im Hinblick auf Schadensersatz einschließlich Schmerzensgeld. So sieht die DSGVO vor, dass Bußgelder bis zu 20 Millionen Euro oder bis zu 4% des Vorjahresumsatzes verhängt werden können.

Fazit

Das neue Datenschutzrecht gibt in vielen Fällen Anlass, die bisherige Datenschutzpraxis zu überprüfen, ggf. zu optimieren und an die neue Rechtslage anzupassen. Während Standard-Texte leicht mit Hilfe kostenloser Angebote aus dem Internet - soweit diese seriös, bewährt und aktuell sind – erstellt und bewältigt werden können, bedürfen komplexere Fragestellungen und Fragen zu einrichtungsspezifischen Datenschutzkonzepten einer Prüfung und Bearbeitung im Einzelfall. Hierzu beraten wir Sie gerne branchenbezogen und individuell.

Stuttgart, den 16.05.2018

Rechtsanwälte Keller & Kollegen

http://www.anwaltskanzlei-keller.de

Jan Matthias Hesse
Rechtsanwalt und
Fachanwalt für Medizinrecht

Bernhard Ludwig
Rechtsanwalt und Mediator
Gesellschaftsrecht
Verwaltungsrecht

Anna Fuchs-Keller
Rechtsanwältin und Mediatorin
Arbeitsrecht

Benjamin Böhm
Rechtsassessor