

Nach langen Verhandlungen erfolgte im Dezember 2015 die europäische Einigung auf eine **EU-Datenschutz-Grundverordnung (EU-DSGVO)**. Diese wird zu einer weitgehenden Vereinheitlichung europäischen Datenschutzrechtes führen. Während bislang durch nationale Gesetzgebungen auf Grundlage der EU-Datenschutzrichtlinie doch erhebliche Unterschiede bestanden, wird die Datenschutz-Grundverordnung direkt geltendes Recht in allen Mitgliedsstaaten sein. Geringe Unterschiede sind allenfalls durch die Möglichkeit sog. „Öffnungsklauseln“ zu erwarten. Öffnungsklauseln bieten nationalen Gesetzgebern die Möglichkeit, eigene nationale Regelungen zu erlassen.

Zeitplan der EU-Datenschutz-Grundverordnung

Bis zu der Anwendbarkeit sind noch einige Schritte erforderlich. Der Zeitplan sieht derzeit wie folgt aus:

- März 2016: offizielle deutsche Fassung der EU-DSGVO
- April 2016: Beratung des EU-Ministerrats, danach Abstimmung im Europäischen Parlament
- 25. Mai 2018: Anwendbarkeit der EU-Datenschutz-Grundverordnung

Ziele und Grundsätze

Die Ziele der EU-DSGVO sind der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten ([Art. 1 Abs. 2 DSGVO](#)) und der freie Verkehr personenbezogener Daten ([Art. 1 Abs. 3 DSGVO](#)).

Die vorangestellten Ziele sollen durch die in [Art. 5 DSGVO](#) festgelegten Grundsätze der Verarbeitung personenbezogener Daten erreicht werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

Die Datenschutz-Grundverordnung wird das europäische Datenschutzrecht nicht völlig umwälzen, weist aber eine Reihe von in der Praxis erheblichen Änderungen auf. Wir werden in einer Reihe von Fachbeiträgen die zu erwartenden Änderungen und Auswirkungen auf die Praxis darstellen. Folgende Beiträge sind erschienen:

Sachlicher Anwendungsbereich

Zunächst stellt sich immer die Frage, bin ich von der Datenschutz-Grundverordnung betroffen? Zur Beantwortung lohnt sich zunächst ein Blick in die Vorschrift zum sachlichen Anwendungsbereich. Diese klärt, bei welchem Sachverhalten die Datenschutz-Grundverordnung anzuwenden ist. Da die Norm relativ weit gefasst ist und nur wenige Ausnahmen bietet, erläutern wir die grundlegenden Begriffe des Art. 2 DSGVO und zeigen dessen Sonderbereiche auf.

[Sachlicher Anwendungsbereich: Die DSGVO gilt, wenn...](#)

Räumlicher Anwendungsbereich

Um abschließend zu klären, ob einen die Regelungen der Datenschutz-Grundverordnung treffen, muss zusätzlich auch der räumliche Anwendungsbereich beachtet werden. Also die Antwort auf die Frage, wo gilt die DSGVO? Hier ergibt sich im Vergleich zur Datenschutzrichtlinie 95/46/EG eine große Neuerung. Zukünftig gilt zusätzlich das Marktortprinzip. Werden personenbezogene Daten im Zusammenhang mit Angeboten von Waren oder Dienstleistungen in der europäischen Union verarbeitet, muss sich die verarbeitende Stelle an die Vorgaben der DSGVO halten. Dadurch fällt der Kreis der Betroffenen deutlich weiter aus.

[Räumlicher Anwendungsbereich: Wo gilt die DSGVO?](#)

Das sind Ihre Rechte

Die EU-Datenschutz-Grundverordnung bringt einige Neuerungen für das Datenschutzrecht mit sich. Diese betreffen nicht nur Unternehmen sondern auch den einzelnen Bürger. Zumindest dann, wenn es um die Rechte der Betroffenen einer Verarbeitung personenbezogener Daten geht. Mit dem 3. Kapitel der aktuellen Fassung der Datenschutz-Grundverordnung will der Gesetzgeber die Rechte der Betroffenen grundsätzlich stärken und weitet diese in manchen Bereichen (im Vergleich zur momentanen Rechtslage) sogar aus. Vor allem die neuen Transparenz- und Informationspflichten der Unternehmen führen zu einem deutlich stärkeren Schutz der Betroffenen, als die aktuell geltenden Regelungen des Bundesdatenschutzgesetzes.

[Neues EU-Datenschutzgesetz: Das sind Ihre Rechte](#)

Beschäftigtendatenschutz

Schon seit Jahren ist der Arbeitnehmerdatenschutz immer wieder im Gespräch der Öffentlichkeit. Bereits im Jahre 2010 stellte die Bundesregierung ein Gesetzesentwurf zum Beschäftigtendatenschutz vor. Nach jahrelangen Verhandlungen kam das Vorhaben aber Anfang 2013 zum Erliegen. Die Reform des Arbeitnehmerdatenschutzes wurde aufgrund der geplanten EU-DSGVO und einer Erweiterung des BDSG vorerst ausgesetzt. Im Jahre 2014 wurde das Thema wurde erneut im Koalitionsvertrag der Großen Koalition aufgegriffen, welcher vereinbarte, den Beschäftigtendatenschutz gesetzlich zu regeln. Das Thema Arbeitnehmerdatenschutzgesetz ist mit der kommenden Verabschiedung der Verordnung wieder aktuell. Doch welche Auswirkungen wird diese auf die Zukunft des deutschen Beschäftigtendatenschutzes haben?

[EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz](#)

Pflichten für Unternehmen

Die Datenschutz-Grundverordnung statuiert neben altbekannten Pflichten auch neue Anforderungen für Unternehmen im Bereich Datenschutz. Eine positive Neuerung ist z.B. die Pflicht zu verbraucher- und datenschutzfreundlichen Voreinstellungen bei elektronischen Geräten. Allerdings könnten andere Pflichten wiederum zu einem deutlichen Mehraufwand seitens der Unternehmen führen. Beispielsweise könnte die vorgesehene Pflicht zur Datenschutz-Folgenabschätzung sowie die sich daran evtl. anschließende Konsultation der zuständigen Aufsichtsbehörde zu einem vermehrten Maß an Bürokratie führen. Ob diese dann wirklich noch positive Auswirkungen für Verbraucher und Unternehmen hat, ist derzeit aber kaum abzusehen. Daher betrachten wir die kommenden Änderungen für Unternehmen einmal etwas genauer.

[Datenschutz-Grundverordnung: Pflichten für Unternehmen](#)

Internationale Datentransfers ins Ausland

Der Transfer von personenbezogenen Daten in Staaten außerhalb der EU/des EWA (sogenannten Drittstaaten) ist problematisch. Dies ist im Rahmen der Richtlinie 95/46/EG (Datenschutz-Richtlinie) der Fall und wird auch mit Inkrafttreten der Datenschutz-Grundverordnung so bleiben. Grund hierfür ist die Annahme, dass in Drittstaaten generell kein angemessenes Datenschutzniveau herrscht. Eine Ausnahme besteht dann, wenn die EU-Kommission für den betreffenden Staat ein solches festgestellt hat. Dementsprechend werden Datentransfers in Drittstaaten auch weiterhin nur zulässig sein, wenn zusätzliche Sicherheitsmechanismen dazu beitragen ein angemessenes Datenschutzniveau zu gewährleisten oder ein solches verbindlich festgestellt wurde.

[Grundverordnung: Internationale Datentransfers ins Ausland](#)

Neues zur Videoüberwachung

Mit der voraussichtlichen Anwendbarkeit der EU-DSGVO im Frühsommer 2018 ändert sich auch die Zulässigkeit einer Videoüberwachung. Eine explizite Regelung zur Zulässigkeit von Videoüberwachung ist dort nicht enthalten. Lediglich in dem Artikel zur Notwendigkeit einer sog. „Datenschutz-Folgenabschätzung“ wird das Thema Videoüberwachung erwähnt. Dies impliziert eine deutliche Veränderung zur bisherigen Rechtslage in Deutschland.

[EU-Datenschutz-Grundverordnung: Neues zur Videoüberwachung?](#)

10 Vorteile der EU-Datenschutz-Grundverordnung

Seit Anfang Februar steht die offizielle deutsche Übersetzung der EU-DSGVO zum Nachlesen bereit. Bereits jetzt lassen sich Vorteile benennen, welche die neue Verordnung für den Datenschutz und damit auch für die Betroffenen mit sich bringt. So z.B. die angestrebte Harmonisierung des Datenschutzrechts in Europa oder ein Konzernprivileg beim der Datenweitergabe innerhalb verbundener Unternehmen. Der nachstehende Artikel stellt 10 Vorteile vor.

[10 Vorteile der EU-Datenschutz-Grundverordnung](#)

Auftragsdatenverarbeitung

In Deutschland definiert sich die Auftragsdatenverarbeitung als durch einen Auftragnehmer auf Weisung eines Auftraggebers, bei dem die Verantwortung für die ordnungsgemäße Datenverarbeitung verbleibt. Ob eine Auftragsdatenverarbeitung in der Praxis vorliegt, richtet sich ausschließlich nach rechtlichen Vorgaben und kann nicht vertraglich festgelegt werden. Daher ist es wichtig deren Voraussetzungen zu kennen. In der Datenschutz-Grundverordnung werden diese nun erstmals europaweit einheitlich geregelt. Obwohl sich die neuen Regelungen inhaltlich an dem bekannten § 11 BDSG orientieren und diesen im Prinzip auf ein europäisches Level heben, sind einige Unterschiede zu beachten.

[Auftragsdatenverarbeitung und Datenschutz-Grundverordnung](#)

Wartungsarbeiten durch Dienstleister

Noch müssen Auftraggeber und Auftragnehmer eine Vereinbarung zur Auftragsdatenverarbeitung abschließen, auch wenn der Dienstleister lediglich mit der Prüfung oder Wartung automatisierter Verfahren (diverse Tools) oder von Datenverarbeitungsanlagen (z.B. Server) beauftragt wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Ob diese Regelungen mit der DSGVO weiterhin bestehen bleibt, ist umstritten. Daher stellen wir die einzelnen Positionen einmal genauer vor.

[Wartungsarbeiten – Ist das eine Auftragsverarbeitung nach der DSGVO?](#)

Websitebetreiber aufgepasst!

Website Betreiber müssen eine Vielzahl an Vorschriften beachten. Regelungen zur Website-Compliance finden sich u.a. in den §§ 11 ff. Telemediengesetz (TMG), insbesondere in § 13 TMG, der die Pflichten des Diensteanbieters vorgibt. Die Datenschutz-Grundverordnung wird zwangsläufig Auswirkungen auf die aktuellen Anforderungen an Website-Compliance haben. Da die EU-DSGVO als europäische Verordnung direkt in den Mitgliedstaaten anwendbar sein wird,

geht sie als europäisches Recht den nationalen Regelungen vor. Zwar bleiben viele gesetzliche Pflichten erstmal bestehen, andererseits sollte aber die Datenschutzerklärung mit den Vorgaben der EU-DSGVO abgestimmt werden.

[EU-Grundverordnung: Websitebetreiber aufgepasst!](#)

Bußgelder und Sanktionen

Die Landes- und Bundesdatenschutzbeauftragten werden gern als zahnlöse Tiger bezeichnet. Unter anderem auch wegen ihren eingeschränkten Sanktionsmöglichkeiten, die sie bei Datenschutzverstößen nach deutschem Recht haben. Die EU-Datenschutz-Grundverordnung aber enthält eigene Vorschriften zu Bußgeld- und Sanktionsmöglichkeiten. Dadurch sollen Unternehmen von Datenschutzverstößen abgehalten und das Bewusstsein dafür geschärft werden, dass Verstöße gegen die Verordnung zugleich Verletzungen der Grundrechtecharta der Europäischen Union sind. Wir geben deshalb einen Überblick über die Bußgelder und sonstige Sanktionen, die Sie bei Nichteinhaltung der Vorschriften treffen können.

[Datenschutz-Grundverordnung: Bußgelder und Sanktionen](#)

Die Rolle der Aufsichtsbehörden

Mit der neuen EU-Datenschutz-Grundverordnung (EU-DSGVO) ändert sich nicht nur die gesetzliche Ausgestaltung des Datenschutzrechts. Auch Aufgaben, Zuständigkeit und Befugnisse der Aufsichtsbehörden wurden teilweise überarbeitet. Daraus ergeben sich für die praktische Handhabung des Datenschutz ganz neue Chancen, aber auch Probleme.

[EU-Datenschutz-Grundverordnung – Die Rolle der Aufsichtsbehörden](#)

Anforderungen an eine Einwilligung

Die Einwilligung in die Verarbeitung seiner personenbezogenen Daten durch den Betroffenen ist seit jeher zentraler Bestandteil des Datenschutzrechts. Aufgrund des Grundrechts der informationellen Selbstbestimmung kann jeder Bürger für sich entscheiden, wer welche Informationen über ihn erhält. Aktuell sind die Voraussetzungen für eine rechtsgültige Einwilligung in die Verarbeitung personenbezogener Daten durch § 4a BDSG und für den Bereich der elektronischen Medien zusätzlich durch § 13 Abs. 2 Telemediengesetz (TMG). Durch die Einführung der Datenschutz-Grundverordnung werden diese Voraussetzungen ergänzt.

[Grundverordnung: Anforderungen an eine Einwilligung](#)

Datenschutz-Vertreter für Unternehmen

Bislang wenig beachtet wird durch die EU-DSGVO auch ein neues Rechtsinstitut eingeführt: der EU-Vertreter bzw. Vertreter in der Union. Seine Existenz hängt eng mit dem durch die EU-DSGVO neu eingeführten Marktortprinzip zusammen. Alle Unternehmen, die keine Niederlassung in der EU unterhalten, aber Personen in der Union Waren oder Dienstleistungen anbieten oder ihr Verhalten – z.B. durch „Tracking“ oder „Profiling“ – beobachten, müssen grundsätzlich einen EU-Vertreter bestellen. Dieser soll insbesondere als Anlaufstelle und Ansprechpartner für Aufsichtsbehörden und betroffene Personen dienen und stellt damit das Bindeglied zwischen diesen und dem in einem Drittland niedergelassenen datenverarbeitenden Unternehmen dar.

[EU-Grundverordnung: Datenschutz-Vertreter für Unternehmen](#)

Betrieblicher Datenschutzbeauftragter

Das Modell Datenschutzbeauftragter ist in Deutschland seit langem bekannt und viele Unternehmen müssen bereits jetzt einen Datenschutzbeauftragten bestellen. Mit Inkrafttreten der Datenschutz-Grundverordnung wird eine solche Pflicht auch erstmals europaweit für Unternehmen, deren Tätigkeit einer besonderen Kontrolle bedarf, eingeführt. Durch die Öffnungsklauseln können die Länder zwar nationale Sonderregelungen für die Bestellung eines betrieblichen Datenschutzbeauftragten schaffen. Nichtsdestotrotz gelten daneben die Anforderungen der Datenschutz-Grundverordnung, welche sich an einige Stellen vom Bundesdatenschutzgesetz unterscheiden und daher zwangsläufig eine Veränderung herbeiführen werden.

[Datenschutz-Grundverordnung – Datenschutzbeauftragter](#)

Datensicherheit

Mit der DSGVO ändern sich die Vorgaben zur Datensicherheit und somit auch die der technischen und organisatorischen Maßnahmen. Manche Begriffe werden durch die Verordnung noch abstrakter, als sie es bisher gewesen sind, einige Vorgehensweise ähneln der jetzigen Handhabung und wiederum andere Anforderungen, wie der Stand der Technik, Belastbarkeit oder data protection by default, sind neu. Auf Unternehmen kommt daher eine Menge Arbeit zu. Neue Verfahren müssen etabliert und Prozesse entsprechend der Verordnung angepasst werden.

[Datenschutz-Grundverordnung und Datensicherheit](#)

Informationspflichten

Die Datenschutz-Grundverordnung führt für Unternehmen und Verantwortlichen eine Reihe von neuen Informationspflichten ein. Dabei ändert sich im Vergleich zu den bisherigen Vorschriften des Telemedien- und Bundesdatenschutzgesetz einiges an den Anforderungen. Denn der europäische Gesetzgeber verfolgt das Ziel, dem Grundsatz der fairen und transparenten Datenverarbeitung gerecht zu werden. Die Betroffenen Nutzer sollen zukünftig besser in der Lage sein, eine Datenerhebung, -verarbeitung oder -nutzung, anhand den zur Verfügung gestellten Informationen, zu überprüfen.

[Neue Informationspflichten mit der Datenschutz-Grundverordnung](#)

Aufgaben des Datenschutzbeauftragten

Mit der Datenschutz-Grundverordnung erweitert sich der Aufgabenkreis des Datenschutzbeauftragten. Damit verbunden ist eine Aufwertung der Position im Unternehmen. Unter Umständen aber auch ein gesteigerter Haftungsumfang für Datenschutzverstöße des betreuten Unternehmen. Bis zur Anwendbarkeit der Datenschutz-Grundverordnung sollten Mitarbeiter und Datenschutzbeauftragte hinsichtlich der gesteigerten Bedeutung des Datenschutzes für Unternehmen sensibilisiert werden.

[Datenschutz-Grundverordnung: Aufgaben des Datenschutzbeauftragten](#)

Datenschutz-Folgenabschätzung

Dass es eine gute Idee ist, eine Abschätzung der Folgen vor dem Einsatz einer bestimmten Technologie durchzuführen, hat sich bereits in den 1960er Jahre in den Bereichen Gesundheit und Umwelt durchgesetzt. Mit der Datenschutz-Grundverordnung hat der europäische Gesetzgeber diese Überlegung aufgegriffen. Fortan sind Unternehmen unter bestimmten Voraussetzungen verpflichtet eine Datenschutz-Folgenabschätzung vorzunehmen. Diese ähnelt stark der aus dem

BDSG bekannten Vorabkontrolle. Aber der Text der DSGVO lässt weitgehend offen, wie und nach welchen Kriterien eine Datenschutz-Folgenabschätzung durchzuführen ist.

[Datenschutz-Folgenabschätzung: Was ist das überhaupt?](#)

Data Breach Notification

Schon heute müssen Unternehmen, unter bestimmten Voraussetzungen, Aufsichtsbehörde und Betroffenen eine Data Breach Notification zukommen lassen. Nämlich dann, wenn Unberechtigte vermutlich oder erwiesenermaßen Zugang zu „Risikodaten“ hatten. Eine weitere Voraussetzung ist, dass die Datenpanne zu einer schwerwiegenden Beeinträchtigung der Rechte oder schutzwürdigen Interessen des Betroffenen führen könnte. Die Datenschutz-Grundverordnung wird diese Anforderungen und etwaige Sanktionen noch deutlich verschärfen. Die Bedeutung der Data Breach Notification und deren Anzahl wird dadurch zwangsläufig steigen.

[Data Breach Notification: Datenpannen in der DSGVO](#)

Verzeichnis von Verarbeitungstätigkeiten

Mit der Datenschutz-Grundverordnung muss ein Unternehmen nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten von personenbezogenen Daten führen. Dies ist nur eine von mehreren, neuen Vorgaben zur Dokumentationspflicht. Bei der Einhaltung aller gesetzlichen Vorgaben wird das Verzeichnis aber eine tragende Rolle spielen. Denn es enthält eine Dokumentation und Übersicht über alle eingesetzten Verfahren, bei denen personenbezogene Daten verarbeitet werden.

[Verzeichnis von Verarbeitungstätigkeiten – Infos & Tipps zur Umsetzung](#)

Aufbau eines Datenschutzmanagementsystems

Neben dem angesprochenen Verzeichnis von Verarbeitungstätigkeiten finden sich in der Datenschutz-Grundverordnung eine Vielzahl von Normen, die eine Dokumentierung der getroffenen Datenschutzmaßnahmen fordern. Daneben schafft die DSGVO weitere Prozesse, die etabliert, und Aufgaben die wahrgenommen werden müssen. Bei dieser Vielzahl von Anforderungen kann man schnell mal den Überblick verlieren. Daher bietet sich ein Datenschutzmanagement an, um die Einhaltung aller Vorgaben systematisch zu planen, umzusetzen und laufend zu kontrollieren.

[Datenschutzmanagement nach der DSGVO – Leitfaden für die Praxis](#)

One Stop Shop

Bei grenzüberschreitender Datenverarbeitung gilt demnächst nach Art. 56 Abs. 1 DSGVO das One Stop Shop Prinzip. Demnach ist nur noch eine federführende Aufsichtsbehörde für die Beurteilung datenschutzrechtlicher Belange eines Unternehmens zuständig. Damit entfällt für internationale Unternehmen eine Menge Bürokratie. Dennoch gibt es auch bei dieser Regelung ein paar Problemfelder, die im Auge zu behalten sind.

[Datenschutz-Grundverordnung und der One Stop Shop](#)

Binding Corporate Rules

Binding Corporate Rules (BCR) sind ein von der Artikel-29-Datenschutzgruppe entwickelter Rahmen zum Umgang mit personenbezogene Daten auf dessen Grundlage Konzerne verbindliche Datenschutzrichtlinien erlassen können. Diese werden als ausreichende Datenschutzgarantie für

konzerninterne Datenübertragungen in unsichere Drittländer angesehen. Durch ihre Kodifikation in der DSGVO ergeben sich im Vergleich zur aktuellen Rechtslage einige Vorteile für Konzerne.

[Internationale Datentransfers: Binding Corporate Rules nach DSGVO](#)

Das Recht auf Vergessenwerden

Das Bundesdatenschutzgesetz enthält ein Recht auf Berichtigung, Sperrung und Löschung. Dieses Recht auf Löschung wird in der Datenschutz-Grundverordnung um das Recht auf Vergessenwerden erweitert. Dadurch ändern sich die gesetzlichen Anforderungen zwar nicht grundlegend, dennoch sind einige Unterschiede zu beachten. So enthält die Verordnung beispielsweise zusätzliche Pflichten für Unternehmen und schränkt die Ausnahmetatbestände der Löschpflicht ein.

[Das Recht auf Vergessenwerden bzw. die Löschungspflicht nach DSGVO](#)

Grundsätze für die Verarbeitung personenbezogener Daten

Die Datenschutz-Grundverordnung verpflichtet Verantwortliche gewisse, allgemeine Grundsätze bei der Verarbeitung personenbezogener Daten einzuhalten. Zudem muss dies dokumentiert werden. Die Grundsätze stellen die Spielregeln dar, welche bei jeglicher Verarbeitung von personenbezogenen Daten zu beachten sind. Daher eignen sich diese auch als Auslegungshilfe für die restlichen Artikel der Datenschutz-Grundverordnung. Es ist daher von Vorteil, die einzelnen Vorgaben bei Inkrafttreten der DSGVO zu kennen.

[DSGVO: Grundsätze für die Verarbeitung personenbezogener Daten](#)

Datenschutz bei Marktforschung

Die Marktforschung beschäftigt mit sich Themen wie beispielsweise Konsumgewohnheiten, demographischen Entwicklungen und Mediennutzung. Um aussagekräftige Ergebnisse zu liefern, werden oft eine Vielzahl von personenbezogenen Daten bei identifizierbaren Personen erhoben und ausgewertet. Bei der Verarbeitung von personenbezogenen Daten sind immer die datenschutzrechtlichen Vorgaben zu beachten. Bisher kam der Markt- und Meinungsforschung dabei durch den § 30a BDSG eine privilegierte Stellung zu. Diese wird aber mit der Datenschutz-Grundverordnung und dem neuen BDSG ersatzlos gestrichen.

[Datenschutz bei Marktforschung – Was ändert die DSGVO?](#)

Rechtmäßigkeit der Datenverarbeitung

Einer der ersten Grundsätze für die Verarbeitung personenbezogener Daten in der Datenschutz-Grundverordnung ist die Rechtmäßigkeit der Verarbeitung. Dafür muss mindestens eine von sechs gesetzlich geregelten Bedingungen erfüllt sein. Welche das sind und wie sich deren Tatbestände von denen des BDSG unterscheiden, erklärt dieser Beitrag.

[Datenschutz-Grundverordnung: Rechtmäßigkeit der Datenverarbeitung](#)

Besondere Kategorien personenbezogener Daten

Auch die DSGVO kennt besondere Kategorien personenbezogener Daten, welche einen erhöhten Schutzbedarf aufweisen. Diese werden in Art. 4 und 9 DSGVO aufgelistet und entsprechen weitgehend den aus dem BDSG bekannten besonderen Arten personenbezogener Daten. Hinzukommen biometrische sowie genetische Daten. Die DSGVO bringt in dieser Hinsicht wenig Neues. Aber ein paar Ungewissheiten bleiben, gerade bei der Erforderlichkeit der Durchführung

einer Datenschutz-Folgenabschätzung.

[Besondere Kategorien personenbezogener Daten nach der DSGVO](#)

Datenverarbeitung von Kindern und Jugendlichen

Der Kinder- und Jugendschutz nimmt in der EU-Datenschutz-Grundverordnung (DSGVO) eine wichtige Rolle ein. So findet sich in der Verordnung z.B. erstmals eine ausdrückliche gesetzliche Regelung zu Anforderungen an die Rechtmäßigkeit der Einwilligung von Kindern. Ebenso beziehen sich zahlreiche weitere Normen und Erwägungsgründe explizit auf Kinder und Jugendliche. Nachfolgend geben wir einen Überblick über die gesetzlichen Vorgaben, welche künftig von Diensten eingehalten werden müssen, die gleichsam Kindern und Erwachsenen offenstehen.