Was muss ich wissen zur EU-Datenschutz Grundverordnung?

FAQ

www.bitkom.org

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Susanne Dehmel | Mitglied der Geschäftsleitung Vertrauen und Sicherheit
T 030 27576-223 | s.dehmel@bitkom.org

Satz & Layout

Sabrina Flemming | Bitkom

Titelbild

© artjazz – fotolia.com

Inhaltsverzeichnis

Einleitung

Die umfangreichen Vorschriften der Datenschutzgrundverordnung (DS-GVO) bereiten gerade kleinen und mittleren Unternehmen erstmal Anfangsschwierigkeiten. »Wo fängt man am besten mit der Umsetzung an?«, »welche Prozesse muss man im Unternehmen in Gang setzen?« und »wie sieht ein DS-GVO-konformes Datenschutzmanagement letztendlich aus?« sind nur eine wenige Fragen, die derzeit Kopfzerbrechen bereiten.

Jetzt ist aber keine Panik angesagt! Viele der datenschutzrechtlichen Konzepte und Prinzipien der DS-GVO sind im Großen und Ganzen nicht viel anders als auch bisher unter der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG), deren Vorschriften in Deutschland mit dem deutschen Bundesdatenschutzgesetz (BDSG) umgesetzt wurden. Wer sich im Unternehmen schon bisher um den Datenschutz gekümmert hat, sollte auch in Zukunft trotz der höheren Sanktionen nicht viel zu befürchten haben.

Dennoch ist es unumgänglich, seine Datenschutzpraxis zu überprüfen und das Datenschutzmanagement bis zum 25. Mai 2018 nach den Vorgaben der DS-GVO anzupassen und weiterzuentwickeln. Dabei gibt es keine Musterlösung, da jedes Unternehmen durch sein eigenes Geschäftsmodell auch unterschiedliche Datenverarbeitungsvorgänge durchführt. So werden beispielsweise für einen Anbieter einer Gesundheits-App die Vorschriften für Gesundheitsdaten im Vordergrund stehen, wohingegen ein Cloud-Anbieter sich mit den neuen Haftungsregeln genauer auseinandersetzen muss.

Diese FAQs haben das Ziel, den Einstieg in die Planung zur Umsetzung der DS-GVO zu erleichtern und Unternehmen auf die wesentlichen Veränderungen und teilweise Neuerungen aufmerksam zu machen. Sie sollen gerade kleinen und mittleren Unternehmen eine Checkliste an die Hand geben, um möglichst zielgerichtet innerhalb des Unternehmens die richtigen Prozesse in Gang zu setzen.

Wann tritt die EU-Datenschutz-Grundverordnung in Kraft?

Die EU-Datenschutz-Grundverordnung ist bereits am 25. Mai 2016, zwanzig Tage nach der Veröffentlichung im EU-Amtsblatt, **in Kraft getreten**. Nach der darin geregelten **Übergangsfrist** kommt sie allerdings erst zwei Jahre nach Inkrafttreten **zur Anwendung**. Das bedeutet, dass sie ab 25. Mai 2018 für alle gilt und deren Einhaltung durch die EU-Datenschutzaufsichtsbehörden und Gerichte überprüfbar ist.

Hinweis

Die zweijährige Übergangsfrist sollte von Unternehmen dringend zur Anpassung der Workflows/Prozesse genutzt werden, da EU-Datenschutzbehörden ab Geltung im Mai 2018 Sanktionen verhängen können, wenn die Vorgaben der DS-GVO nicht oder nicht ausreichend umgesetzt wurden.

Wie wirkt die EU-Datenschutzgrundverordnung in Deutschland?

Die für Unternehmen einschlägigen Regelungen des BDSG werden weitgehend durch die Regelungen der Verordnung ersetzt. Da es sich bei dem neuen Gesetz um eine europäische Verordnung handelt, gilt sie direkt in allen Mitgliedsstaaten und bedarf keines nationalen Umsetzungsgesetzes. Die nationalen Gesetzgeber werden lediglich neue Gesetze erlassen, um die nationalen Vorschriften, die durch die Verordnung ersetzt werden, aufzuheben. Die nationalen Gesetzgeber sind an einigen Stellen der Verordnung – sog. Öffnungsklauseln – ermächtigt, die Regelungen der Verordnung zu konkretisieren und zu ergänzen:

Beispiel Beschäftigtendatenschutz: Ein klassisches Beispiel ist der Beschäftigtendatenschutz. In Art. 88 Abs.1 DS-GVO ist eine Öffnungsklausel vorgesehen, nach der die Mitgliedsstaaten »spezifischere Vorschriften zur Gewährleistung der Rechte und Freiheiten hinsichtlich der Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext« vorsehen können. Diese Formulierung lässt weder eine Verschärfung noch Lockerung zu, sondern lediglich eine Konkretisierung der allgemeinen Vorschriften. Im Rahmen der ersten Anpassung des deutschen Rechts an die DS-GVO sind keine umfassenden neuen nationalen Regelungen zu erwarten, sondern lediglich eine dem **geltenden § 32 BDSG entsprechende Regelung**.

Hinweis

Auch Kollektivvereinbarungen wie die Betriebsvereinbarung zum Datenschutz im Arbeitsverhältnis bleiben gem. Art. 88 DS-GVO nach wie vor zulässig. Sie müssen jedoch zusätzlich die Vorgaben der DS-GVO beachten, was ggf. eine Überarbeitung der bisherigen Betriebsvereinbarungen erfordern kann. Zusätzlich werden auch die zahlreichen Urteile der deutschen Arbeitsgerichte nach wie vor eine wichtige Rolle bei datenschutzrechtlichen Vorgaben spielen.

Beispiel Einwilligung von Kindern unter 16 Jahren: Kinder genießen unter der DS-GVO einen besonderen Schutz. Das Mindestalter für Einwilligung von Kindern von 16 Jahren kann national auf 13 abgesenkt werden.

Hinweis

Ist ein Unternehmen in verschiedenen EU-Mitgliedsstaaten tätig, sollte es die in den einzelnen EU-Staaten festgelegten Altersgrenzen prüfen. Denken Sie daran, dass Sie nach der DS-GVO die Beweispflicht für die Einwilligung von Kindern oder ihrer Erziehungsberechtigten tragen. Es sollte sich also darüber Gedanken gemacht werden, wie man das Alter in Praxis verifizieren kann.

Beispiel Datenschutzbeauftragter: Nach bisherigen Aussagen zählt beim Thema Öffnungsklauseln vor allem die Beibehaltung der BDSG-Regelung zur **Bestellung eines betrieblichen Datenschutzbeauftragten (DSB) in Unternehmen mit mehr als neun Angestellten**, die über das hinausgeht, was die Verordnung als Mindeststandard vorgibt.

Hinweis

Ein kleines Unternehmen bzw. Start-up mit weniger als 9 Angestellten sollte prüfen, ob es in die von Art. 37 Abs. 1 DS-GVO genannten Kategorien fällt und einen Datenschutzbeauftragten benötigt (mehr dazu siehe unten auf Seite 8).

Beispiel Verbandsklage: Mit dem am 17. Februar 2016 erlassenen Gesetz zur Verbesserung der zivilrechtlichen Durchsetzung von verbraucherschützenden Vorschriften des Datenschutzrechts hat Deutschland bereits die in Art. 80 Abs. 2 DS-GVO aufgeführte Öffnungsklausel genutzt. Das neue Gesetz räumt einer Vielzahl an Verbänden z. B. Verbraucherschutzorganisationen ein Klagerecht zur ‚abstrakten Durchsetzung', also ohne dass der Betroffene sich selbst beschwert, datenschutzrechtlicher Vorschriften ein. Bisher konnten Verbraucherschützer schon gegen Unternehmen vorgehen, wenn diese in den Allgemeinen Geschäftsbedingungen (AGB) gegen Datenschutzvorschriften verstießen. Diese Befugnis wird nun auch auf andere Vorschriften erweitert, nämlich dann, wenn Daten für Werbung, Markt- und Meinungsforschung, Auskunfteien, Profilbildung, Adresshandel oder »vergleichbare kommerzielle Zwecke« genutzt werden. In anderen Ländern, die kein Gesetz unter dieser Öffnungsklausel erlassen haben, können Verbraucherschutzverbände nur im Namen eines Betroffenen aktiv werden, wenn sie ein Mandat von ihm erhalten und in seinem Namen tätig werden.

Hinweis

Sie sollten in Zukunft in Deutschland also damit rechnen, dass auch Verbraucherschutzverbände Lösch-, Auskunfts- und Schadensersatzansprüche Betroffener einklagen können.

Die DS-GVO lässt dem Gesetzgeber in den Bereichen, die für die Unternehmen ausschlaggebend sind, ansonsten relativ wenig Spielraum für ergänzende Regelungen. In Deutschland ist die Verabschiedung eines entsprechenden Gesetzes für Frühsommer 2017 geplant. Da die meisten Regelungen für die Unternehmen in der Verordnung abschließend geregelt sind, **kann mit der Anpassung der Unternehmensprozesse bereits jetzt begonnen werden**.

Was ist weitestgehend gleich geblieben?

- Die Verordnung bewegt sich auf der materiell-rechtlichen Grundlage der geltenden EU-Richtlinie 95/46 und behält im Wesentlichen die grundsätzlichen **Datenschutz-Prinzipien** aus der Richtlinie bei.

  Beispiel: Datenschutzprinzipien wie »Zweckbindung«, »Datenminimierung« und »Transparenz« bleiben gleich.

  Hinweis

  Zwar bleiben die »allgemeinen« Grundsätze gleich, allerdings werden diese in strengeren Vorschriften »konkret umgesetzt«, z. B. bei der Weiterverarbeitung von Daten gem. Art. 6 Abs. 4 DS-GVO (Zweckbindung), durch die Verpflichtung zu »Privacy by Design« und »datenschutzrechtlichen Voreinstellungen« gem. Art. 25 DS-GVO (Datenminimierung) und den zusätzlichen Informationspflichten in Art. 13 und 14 DS-GVO (Transparenz).

- Der Umgang mit personenbezogenen Daten bleibt auch weiterhin **verboten, wenn** er **nicht** entweder durch einen **Erlaubnistatbestand** der DS-GVO oder sonstigen Rechtsvorschrift (z. B. Spezialgesetzgebung wie Telekommunikationsgesetz (TKG) oder Telemediengesetz (TMG)) erlaubt ist (Grundprinzip Verbot mit Erlaubnisvorbehalt). Die gängigen gesetzlichen Erlaubnistatbestände für die Verarbeitung bleiben erhalten.

  Hinweis

  Nicht alle Unternehmen werden bisher jeder Datenverarbeitung eine bestimmte Rechtsgrundlage zugeordnet haben. Unter der DS-GVO muss das Unternehmen neuerdings den Betroffenen in der Datenschutzerklärung darüber informieren, auf welche Rechtsgrundlage man die Datenverarbeitung stützt (siehe **Link zu Informations- und Auskunftspflichten**). Falls dies unter Art. 6 Abs. 1 lit. f DS-GVO erfolgt, müssen auch die berechtigten Interessen des Verantwortlichen aufgeführt werden. Sie sollten daher die Rechtsgrundlagen in Zusammenhang mit den unterschiedlichen Datenverarbeitungen dokumentieren. So können Sie auch schneller bei Auskunftsansprüchen von Betroffenen, Anfragen von Aufsichtsbehörden etc. reagieren. Behalten Sie auch im Kopf, dass an verschiede Rechtsgrundlagen unterschiedliche Rechte geknüpft sind. So kann die Einwilligung z. B. jederzeit widerrufen werden, wohingegen ein Widerspruch nur unter bestimmten Voraussetzungen erfolgen kann. Sie sollten sich also schon bei der Erhebung der Daten darüber Gedanken machen, welche Rechtsgrundlage für die jeweilige Datenverarbeitung geeignet ist.

- Die Verarbeitung **besonders sensibler Daten** unterliegt nach wie vor **besonderen Voraussetzungen**.

Hinweis

Für die Verarbeitung von sensiblen Daten gelten die in Art. 9 DS-GVO aufgeführten Voraussetzungen (siehe z. B. »explizite« Einwilligung).

- Die gängigen gesetzlichen **Rechtsinstrumente für die Übermittlung in Drittstaaten** bleiben weitestgehend erhalten und werden sogar noch erweitert.

Beispiel: Die DS-GVO hält für international tätige Unternehmen die gleichen Rechtsinstrumente zur Datenübermittlung in Drittstaaten wie schon die DS-RL bereit (u. a. Einwilligung, Vertrag, Standardvertragsklauseln, Binding Corporate Rules – und sogar noch weitere (Zertifizierung, Codes of Conduct).

Hinweis

Prüfen Sie immer erst, ob die EU-Kommission ↗ eine Angemessenheitsentscheidung für das jeweilige Land, in das Ihr Unternehmen Daten übermittelt, erlassen hat. Liegt eine solche Entscheidung nicht vor, müssen Sie den Datentransfer auf eines der in der Verordnung vorgesehenen Rechtsinstrumente stützen und den Betroffenen hierüber in der Datenschutzerklärung informieren.

Zukünftig kann deutschen Unternehmen auch das im Juli 2016 angenommene ↗ »Privacy Shield« als Rechtsgrundlage dienen, um an US-amerikanische Unternehmen, die sich dazu verpflichtet haben die Datenschutzgrundsätze in dem neuen Instrument einzuhalten, Daten zu übermitteln.

Bitkom: Mehr Informationen hierzu finden Sie in unserem Leitfaden »Übermittlung personenbezogener Daten – Inland, EU-Länder und Drittländer«.

- Zumindest in Deutschland bleibt der **betriebliche Datenschutzbeauftragte** für die meisten Unternehmen voraussichtlich unabdinglich.

Beispiel: Die DS-GVO schreibt einen betrieblichen DSB eigentlich nur in zwei Fällen vor, wenn entweder die Hauptaktivität des Unternehmens dem Umfang oder seinem Zweck nach die massenhafte, regelmäßige und systematische Beobachtung von Betroffenen erfordert (lit. b) oder deren Kerngeschäft in der massenhaften Verarbeitung sensibler Daten besteht (lit. c). In Deutschland wird sich durch die Beibehaltung der BDSG-Vorschrift an der bisherigen Praxis voraussichtlich jedoch nicht viel ändern.

Hinweis

Sind Sie ein kleines Unternehmen bzw. Start-up mit weniger als 9 Angestellten, sollten Sie prüfen, ob die Tätigkeit Ihres Unternehmens in die oben genannten Kategorien fällt. Falls ja, benötigen Sie trotz Schwellenwert einen betrieblichen Datenschutzbeauftragten. Konzerne können neuerdings auch nur einen DSB für die ganze Unternehmensgruppe (»Konzern-Datenschutzbeauftragter«) bestimmen, sofern dieser für jede Gesellschaft der Gruppe aus leicht erreichbar ist. Mehrfachbestellungen entfallen damit. Die genauen Anforderungen an einen solchen Konzern-DSB (z. B. hinsichtlich der Sprachanforderungen) sind derzeit noch unklar. Die Artikel-29-Gruppe plant eine Stellungnahme zum DSB in 2016 zu veröffentlichen (siehe Seite 20).

Was sind die wichtigsten Änderungen im Vergleich zum geltenden Recht?

- Der Anwendungsbereich der Verordnung wird auf alle Verarbeitungen ausgeweitet, die sich an EU-Bürger richten und personenbezogene Daten von EU-Bürgern verarbeiten.

Beispiel: Ein türkisches Unternehmen bietet EU-Bürgern Waren im Online-Shop an und verarbeitet dabei ihre personenbezogenen Daten. Auch bei geldfreien Internetangeboten wie Suchdiensten und sozialen Netzwerken findet die DS-GVO Anwendung.

Hinweis

Der Aufenthalt in der EU ist ausreichend, so dass z. B. auch Touristen oder »Gastarbeiter« den Schutz der DS-GVO erfahren, wenn in Deutschland ansässige Firmen ihre Daten verarbeiten.

- Es gibt einige neue Begriffsdefinitionen (Artikel 4).

Beispiele:

- Umfassender Verarbeitungsbegriff (Art. 4 Nr. 2) – Aufhebung der Dreiteilung (Erhebung, Verarbeitung, Übermittlung)
- Auftragsverarbeiter (Art. 4 Nr. 8) – keine Beschränkung mehr auf Auftragsverarbeitung im EWR
- Profiling (Art. 4 Nr. 4)
- Einwilligung (Art. 4 Nr. 11)
- Besondere Arten von Daten: So gibt es z. B. unter der DS-GVO neue Definitionen für »biometrische Daten« und »genetische Daten« (Art. 4 Nr. 12, 13). Unternehmen, die z. B. mit Verfahren wie Gesichtserkennung und Fingerabdruck arbeiten, sollten nicht nur die neuen Definition, sondern auch die damit verbundenen Vorschriften prüfen.

Hinweis

Eine gute ↗ Übersicht zu den Neuerungen und wesentlichen Änderungen bei den Definitionen stellt die Anwaltskanzlei Oppenhoff & Partner zur Verfügung.

- Die Verarbeitung zu anderen Zwecken als den ursprünglichen Erhebungszwecken ist anders geregelt als im BDSG – Weiterverarbeitung nur bei kompatiblen Zwecken zulässig (war auch in der Richtlinie schon so, aber im BDSG anders umgesetzt).

Beispiel Zweckänderung: Zwar bleibt der Grundsatz der Zweckbindung erhalten – der Wortlaut der allgemeinen Regelung für die Datenweiterverarbeitung ändert sich jedoch. Die Regelung zur Weiterverarbeitung für einen anderen Zweck als den, zu dem die Daten ursprünglich erhoben wurden, findet sich im BDSG in § 28 Abs. 2, während in der Verordnung Art. 6 Abs. 4 maßgeblich ist. Der Wortlaut des BDSG weicht von dem der Verordnung ab. Während die DS-GVO die Weiterverarbeitung nur zulässt, wenn sie **»mit dem ursprünglichen Zweck vereinbar ist«**, ist die Übermittlung und Nutzung für einen anderen Zweck nach § 28 Abs. 2 Nr. 1 zulässig, wenn es zur »Wahrung berechtigter Interessen« der verantwortlichen Stelle erforderlich ist und »kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.« Mit der Auslegung der Formulierung »mit dem ursprünglichen Zweck vereinbar« besteht in Deutschland daher wenig Erfahrung – obwohl er bereits in der EU-Datenschutzrichtlinie (DS-RL) enthalten war. Es bleibt daher abzuwarten, wie eng oder weit die Verarbeitungszwecke zukünftig formuliert werden können, um ein Mindestmaß an Flexibilität hinsichtlich der Art der Verarbeitung zuzulassen.

Hinweis

In Art. 6 Abs. 4 DS-GVO gibt die DS-GVO eine nicht-abschließende Liste von Kriterien vor, die Sie zur Kompatibilitätsprüfung heranziehen müssen. So kann sich z. B. die Pseudonymisierung personenbezogener Daten positiv auf eine Prüfung der Weiterverarbeitung der Daten auswirken.

- Die Anforderungen an die informierte, freiwillige Einwilligung wurden graduell erhöht.

Beispiel: Die Erteilung der Einwilligung erfordert eine freiwillige, spezifisch informierte und eindeutige Handlung – z. B. das Anklicken eines Kästchens auf einer Webseite und die Auswahl technischer Einstellungen bei Online-Diensten. Keine Einwilligung stellen laut Erwägungsgrund 32 zur DS-GVO ein stillschweigendes Einverständnis, standardmäßig angekreuzte Kästchen oder Untätigkeit des Betroffenen dar. Zudem fordert die DS-GVO, dass in verschiedene Datenverarbeitungsvorgänge jeweils gesondert eingewilligt werden muss. Andernfalls soll es an der Freiwilligkeit fehlen.

Hinweis

Nach der DS-GVO müssen Sie den Nachweis erbringen, dass eine effektive Einwilligung gegeben wurde. Die Einwilligung kann auch elektronisch abgegeben werden.

- Die Anforderungen an den Widerruf der Einwilligung wurden für den Betroffenen herabgesetzt.

Beispiel: Der Betroffene muss seine Einwilligung »jederzeit« und »ohne Begründung« widerrufen können. Der Widerruf der Einwilligung ist mindestens so einfach zu gestalten wie die Abgabe (Art. 7).

Hinweis

Sie sollten effektive Prozesse zum Widerruf der Einwilligung einführen. Gerade bei der Gestaltung von Webseiten, Apps und anderen digitalen Diensten sind die Vorschriften der DS-GVO zu beachten.

- Das Kopplungsverbot wurde verschärft.

Beispiel: Art. 7 Abs. 4 DS-GVO in Verbindung mit Erwägungsgrund 34 untersagt, dass der Abschluss eines Vertrags von der Erteilung einer Einwilligung abhängig gemacht wird, obwohl dies für die Durchführung des Vertrags nicht erforderlich ist (kein »take it or leave it«). Damit dehnt die DS-GVO die bestehende Regelung des § 28 Abs. 3b BDSG in Monopolsituationen deutlich aus. In der Praxis könnte diese bedeuten, dass Unternehmen ihre Dienstleistung einmal mit und einmal ohne Einwilligung anbieten müssen.

- Die Informations- und Auskunftspflichten wurden um weitere Angaben erweitert.

Beispiel: Sie müssen zukünftig dem Betroffenen eine Reihe an weiteren Informationen bereitstellen. Dazu gehören u.a. Informationen zu der Rechtsgrundlage, auf die Sie die Datenverarbeitung stützen und Angaben zur Dauer der Speicherung oder, falls dies nicht möglich ist, über die Kriterien zur Festlegung der Dauer. Zudem müssen Sie neuerdings vor jeder Weiterverarbeitung der Daten zu einem anderen Zweck den Betroffenen erneute Informationen nach Art. 13 und 14 DS-GVO bereitstellen.

- Es gibt eine neue Portabilitätsverpflichtung für Daten, die der Betroffene selbst zur Verfügung gestellt hat: Diese müssen in gängigem Format wieder zur Verfügung gestellt werden und ggf. auf Wunsch sogar direkt an Dritte übermittelt werden.

Hinweis

Sie sollten ab Mai 2018 in der Lage sein auf Anfrage personenbezogene Daten, die der Betroffene selbst bereitgestellt hat, in einem gängigen und elektronischen Format dem Betroffenen bereitzustellen. Je nachdem, welches Geschäftsmodell Sie verfolgen (soziale Netzwerke, Plattformen oder andere Dienstleistungen des Web 2.0), ist dies mehr oder weniger schwierig. Die europäischen Datenschutzbehörden (sogenannte Art. 29-Datenschutzgruppe (siehe unten)) hat angekündigt noch 2016 hierzu eine Stellungnahme abzugeben, an der Sie sich orientieren können.

- Die Löschpflicht wird erweitert (Hinweispflicht bei Weitergabe von Daten an Dritte).

Beispiel: Wenn Ihr Datenbestand nicht auf dem neusten Stand ist und Sie diese Informationen an Dritte weitergegeben haben, so ist es Ihre Pflicht diese Organisationen auf diese sachliche Unrichtigkeit hinzuweisen, sodass auch diese die falschen Daten korrigieren können.

Hinweis

Sie sollten dokumentieren welche personenbezogenen Daten Ihr Unternehmen verarbeitet, woher Sie diese Daten haben und an wen Sie die Daten weitergegeben. Andernfalls wird es schwierig dieser Vorgabe der DS-GVO nahzukommen. Sie sollten zusätzlich Ihr Löschverfahren im Unternehmen prüfen, sodass bei einem Löschanspruch die Daten schnell auffindbar sind und gelöscht werden können.

- Das Widerspruchsrecht wird erweitert.

Beispiel: Der Betroffene kann insbesondere Datenverarbeitungen zu Zwecken des Direktmarketings, einschließlich der Profilbildung für diese Zwecke, widersprechen.

Hinweis

Auf das Widerspruchsrecht ist der Betroffene »deutlich und getrennt« von jeglicher anderer Information hinzuweisen z. B. durch eine Hervorhebung des Widerspruchsrechts bei Datenschutzerklärungen.

- Die »Joint Controllership«, bei der zwei verantwortliche Stellen gemeinsam Daten mit jeweils vertraglich festgelegten Verantwortlichkeiten verarbeiten, war dem BDSG ebenfalls nicht bekannt (jedoch schon in der EU-Richtlinie enthalten).

Beispiel: Aus Art. 4 Abs. 7 DS-GVO ergibt sich zunächst, dass neben der alleinigen Verantwortung auch ein arbeitsteiliges Zusammenwirken möglich ist. Ohne ein solches Zusammenarbeiten kommen selbst kleinere und mittlere Unternehmen heute nur noch selten aus, denn es ermöglicht die Inanspruchnahme besonderer Kenntnisse und Erfahrungen und vermeidet unverhältnismäßige Investitionen. Dabei ist das Zusammenwirken nicht zahlenmäßig beschränkt: Art. 26 DS-GVO, die Kernbestimmung über gemeinsam Verantwortliche, nennt »zwei oder mehr Verantwortliche« und verzichtet damit sinnvollerweise auf eine Obergrenze. Von der gemeinsamen Verantwortung zu unterscheiden ist einerseits die alleinige Verantwortung einer Stelle, die die Entscheidungen über Zwecke und Mittel der Verarbeitung selbst und unabhängig von anderen Stellen trifft, und andererseits die Auftragsverarbeitung.

Hinweis

Die Artikel-29-Datenschutzgruppe setzte sich bereits 2010 mit dem Konzept des »Joint Controllers« auseinander (Art. 29-Datenschutzgruppe, WP 169 v. 16.2.2010). In diesem Papier wird auch ausführlich die Abgrenzung zwischen Auftragsverarbeitung und »Joint Controllership« erklärt.

Bitkom: Der Bitkom arbeitet derzeit an einer Übersicht zur Auftragsverarbeitung, die Erläuterungen zum gemeinsamen Verantwortlichen umfasst. Sie wird noch in diesem Jahr auf der Bitkom Webseite veröffentlicht werden.

- Die Pflichten im Auftragsverhältnis haben sich teilweise geändert. Der Auftragsverarbeiter wird für seinen Verantwortungsbereich stärker in die Pflicht genommen. Er hat eigene Dokumentationspflichten und haftet bei Datenpannen unter Umständen auch direkt gegenüber den Betroffenen.

Beispiel: Nach Art. 82 Abs. 1, 4 DS-GVO haftet im Gegensatz zur bisherigen Rechtslage nicht nur der für die Verarbeitung Verantwortliche, sondern auch der Auftragsverarbeiter gegenüber dem Betroffenen im Außenverhältnis gesamtschuldnerisch auf Schadensersatz. Alle Beteiligten der Verarbeitungskette haften also gegenüber dem Betroffenen voll, d. h. sie müssen im Außenverhältnis den kompletten Schaden ersetzen. Erfüllt ein Beteiligter den Anspruch des Betroffenen voll, so kann er über Art. 82 Abs. 5 DS-GVO Rückgriff bei den anderen Beteiligten entsprechend des Verantwortungsbeitrags im Innenverhältnis nehmen. Eine EU-Aufsichtsbehörde kann in Zukunft Bußgelder auch direkt gegen den Auftragsverarbeiter verhängen, wenn die Auftragsverarbeitung nicht den Vorgaben der DS-GVO entspricht, z. B. wenn der Dienstleister ohne Vertrag arbeitet.

Bitkom: Auch Datenverarbeiter müssen neuerdings eine schriftliche bzw. elektronische Dokumentation ihrer Verarbeitungstätigkeiten führen und auf Verlangen der Aufsichtsbehörde zur Verfügung stellen. Zur Hilfestellung eines Verfahrensverzeichnisses siehe Bitkom Publikation ↗ »Das Verfahrensverzeichnis« (Version 3.0). Stand März 2016.

Hinweis

Die Veröffentlichung »Verfahrensverzeichnis« bezieht sich bisher nur auf das Verfahrensverzeichnis des »Verantwortlichen« und nicht des »Auftragsverarbeiters«. Ein solches Verzeichnis muss also noch auf den Auftragsverarbeiter unter Berücksichtigung der DS-GVO-Vorgaben (Art.30 Abs. 2 DS-GVO) zugeschnitten werden. Der Bitkom arbeitet derzeit an einer Überarbeitung und Anpassung des Verfahrensverzeichnisses an die DS-GVO.

- Die Verordnung hat in Bezug auf die technisch-organisatorischen Maßnahmen einen stärker risikobasierten Ansatz, der eine Dokumentation der Risikoeinschätzung nötig macht.

Hinweis

Für die Festlegung der angemessenen technisch-organisatorischen Maßnahmen sind nach Art. 32 DS-GVO verschiedene Faktoren der Datenverarbeitung sowie die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu berücksichtigen. Um nachweisen zu können, dass man die technisch-organisatorischen Maßnahmen aufgrund einer solchen umfassenden Betrachtung ausgewählt hat, muss diese Prüfung bzw. ihr Ergebnis dokumentiert werden. Hierfür sollte ein möglichst effizienter Prozess gefunden werden. Der Bitkom arbeitet derzeit an einer Veröffentlichung zum risikobasierten Ansatz in den Art. 32-36 DS-GVO.

- Für besonders risikobehaftete Datenverarbeitungen wird die Durchführung einer Datenschutz-Folgenabschätzung vorgeschrieben. Dafür entfällt die Pflicht zur Meldung der Verfahren bei der Aufsichtsbehörde (Vorabkontrolle gem. §4d Abs. 5 BDSG).

Beispiel: Einer Datenschutzfolgeabschätzung sollte ein adäquates Risikomanagement vorausgehen. Sollten Sie bei der Risikoabschätzung der einzelnen Datenverarbeitung zu dem Ergebnis kommen, dass diese ein hohes Risiko für die Rechte und Freiheiten des Betroffenen darstellt, müssen Sie eine Datenschutz-Folgeabschätzung durchführen – insbesondere dann, wenn es um eine automatisierte Entscheidung für den Betroffenen geht, massenhaft sensible Daten verarbeitet werden oder systematisch öffentlich zugängliche Bereiche massenhaft beobachtet werden. Auch bei der Einführung neuer Technologien ist eine Datenschutzfolgeabschätzung notwendig. Sie sollten vorher in Verfahren festlegen, wer die Datenschutzfolgeabschätzung durchführt und welche anderen Stakeholder zusätzlich miteingebunden werden sollen.

Hinweis

Sie müssen die zuständige Aufsichtsbehörde miteinbeziehen, wenn Sie keine Maßnahmen treffen oder treffen können, um das hohe Risiko einer Datenverarbeitung einzudämmen (Konsultationspflicht). Nationale Aufsichtsbehörden können zudem Listen veröffentlichen, welche Verarbeitungen immer oder nie eine Datenschutzfolgeabschätzung benötigen.

Bitkom: Die europäischen Datenschutzbehörden (sogenannte Art. 29-Datenschutzgruppe [siehe Seite 19]) hat angekündigt noch 2016 hierzu eine Stellungnahme abzugeben, an der Sie sich orientieren können. Der Bitkom arbeitet derzeit auch an einer Veröffentlichung.

- Ausweitung der Meldepflicht bei Datenpannen an eine Aufsichtsbehörde auf jeden Vorfall, der ein »Risiko« für die Rechte und Pflichten der Betroffenen darstellt binnen 72 h. Zusätzlich muss auch der Betroffene unverzüglich über eine Datenpanne informiert werden, wenn sie »voraussichtlich« zu einem »hohen Risiko« führt.

Beispiel: Bislang war ein Unternehmen nach §42a BDSG zur Meldung von Datenschutzverstößen u. a. nur verpflichtet, wenn die Datenpanne besonders sensible Daten wie Gesundheits- oder Kontodaten betraf und nur bei schwerwiegenden Beeinträchtigungen für den Betroffenen.

Hinweis

Hierzu sollten Unternehmen interne Richtlinien und Verfahren zu entwickeln, die eine unverzügliche Meldung aller Datenschutzverstöße gewährleisten. Dabei sollten die (Mindest-) Anforderungen an den Inhalt einer solchen Meldung (siehe Art.33 Abs.3 DS-GVO) beachtet werden. Zusätzlich sind Unternehmen dazu verpflichtet, die Datenpannen zu dokumentieren.

Hinweis

Auch elektronische Telekommunikationsanbieter mussten bisher Datenschutzverstöße nach der e-Privacy Richtlinie (→ Umsetzung in § 109a TKG) an die Bundesnetzagentur und die Bundesdatenschutzbeauftragte melden. Mit der Einführung der DS-GVO kommt für solche Dienstleister also ein zweites Rechtsinstrument dazu, das ähnliche, aber nicht deckungsgleiche Anforderungen an Meldung von Datenpannen stellt. Die e-Privacy Richtlinie wird derzeit überarbeitet und an die DS-GVO angepasst. Es ist also gut möglich, dass die EU-Kommission diesbezügliche Vorschriften unter der e-Privacy Richtlinie aufhebt und Unternehmen nur noch ein Verfahren nach der DS-GVO umsetzen müssen.

- Die zuständige Aufsichtsbehörde für ein Unternehmen richtet sich europaweit nach dem Hauptsitz bzw. der Niederlassung, die generell über die Datenverarbeitung entscheidet.

Beispiel: Die Bestimmung des Hauptsitzes hängt insbesondere davon ab, wo die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten getroffen werden. Bei großen Unternehmen mit komplexer Struktur, die in unterschiedlichen Ländern Daten verarbeiten, ist zu prüfen, wo der Konzern die wichtigsten Entscheidungen bezüglich der Datenverarbeitung trifft.

Hinweis

Die nationale Aufsichtsbehörde, z. B. der hessische Datenschutzbeauftragte, bleibt für Sachverhalte zuständig, die ausschließlich die Niederlassung in Deutschland betreffen oder sich im Wesentlichen auf einen Deutschen Staatsbürger auswirken (»federführende Aufsichtsbehörde«). Sollte die Beschwerde aber nicht nur einen rein nationalen Bezug haben, z. B. sind durch die Datenverarbeitung auch Bürger anderer EU-Länder wie Frankreich betroffen, hat neben der federführenden Aufsichtsbehörde auch eine andere europäische Aufsichtsbehörde durch den Kooperations- und Kohärenzmechanismus (One-Stop-Shop) die Gelegenheit zur Stellungnahme. Können sich die verschiedenen Aufsichtsbehörden nicht auf ein Ergebnis einigen, kann der neu zu schaffende »Europäische Datenschutzausschuss« (siehe unten) als letzte Entscheidungsinstanz eine bindende Entscheidung treffen.

- Die möglichen Geldbußen für Verstöße wurden drastisch erhöht – auf bis zu 4 Prozent des weltweiten Umsatzes pro Verstoß.

Beispiel: Die in dem BDSG festgelegte Höchstgrenze von Bußgeldern lag bisher bei 300.000 Euro pro Verstoß und Geldbußen wurden eher moderat verhängt. Die neuen Vorschriften stützen sich auf den weltweit erzielten Jahresumsatz des vorangegangenen Geschäftsjahrs des Unternehmens. Der Begriff »Unternehmen« soll laut Erwägungsgrund 150 im Sinne der Artikel 101 und 102 AEUV verstanden werden. Diese beziehen sich auf wettbewerbs- bzw. kartellrechtliche Regeln. Daher wird die Vorschrift teilweise so verstanden, dass sich die Geldbuße nicht nur auf den weltweiten Umsatz der verantwortlichen Stelle, sondern der gesamten Unternehmensgruppe, zu der das Unternehmen gehört, beziehen soll. Aus dem Wortlaut selbst ist dies jedoch nicht zu entnehmen. Bei mehreren Verstößen können von Datenschutzaufsichtsbehörden auch Gesamtbußgelder verhängt werden, die über den festgesetzten Betrag für Einzelverstöße hinausgehen können.

Hinweis

Unternehmen, und insbesondere Konzerne, sollten das maximale Bußgeldrisiko auf der Grundlage ihres globalen Umsatzes bestimmen und dieses in die Compliance-Gefährdungsanalyse miteinbeziehen. Achten Sie darauf, dass alle Teile der Unternehmensgruppe in ein effektives Datenschutzmanagement miteinbezogen werden.

Hinweis

Durch ein koordiniertes Vorgehen der EU-Datenschutzaufsichtsbehörden können Datenschutzverstöße gerade bei grenzüberschreitenden Tätigkeiten eines Unternehmens leichter identifiziert und durchgesetzt werden. Bisher scheiterten viele Verfahren der deutschen Aufsichtsbehörden insbesondere an der Kompetenzzuständigkeit, die bisher nur bei einer einzigen Behörde lag.

Welche Prozesse und Dokumente muss ich in meinem Unternehmen überprüfen?

- Dokumentation der Datenverarbeitungsprozesse im Unternehmen (insbesondere Erweiterung der Dokumentationspflichten bei Auftragsverarbeitern, möglw. zusätzliche Dokumentationserfordernisse für Risk und Privacy Impact Assessment)
- Datenschutzerklärungen (Erweiterung der Informationspflichten)
- Einwilligungserklärungen (Verschärfung der formalen Vorgaben), Prozess für Widerruf der Einwilligung
- Anpassung der Betriebsvereinbarungen an DS-GVO
- Prozesse zur Umsetzung von Widersprüchen
- Vereinbarungen zur Auftragsverarbeitung (Haftungsregelung, Dokumentation)
- Prozess bei Datenpannen entsprechend der neuen Vorgaben überarbeiten
- Verfahren, um Daten in gängigem elektronischen Format übertragen zu können
- Durchführung von zielgruppengerechten Schulungen zu den Neuerungen der DS-GVO und den eigenen Prozessen
- Einführung von Risk Assessment zur Festlegung geeigneter technisch-organisatorischer Maßnahmen
- Einführung von Privacy Impact Assessment
- Monitoring nationaler Gesetzgebung und Fortbildung

Hinweis

Alle Punkte unterliegen einer erweiterten Rechenschaftspflicht: Die DS-GVO rückt die Verantwortlichkeit von Unternehmen in den Vordergrund und führt erstmalig die Rechenschaftspflicht als zentralen Grundsatz der Datenverarbeitung auf. Sie sollten ein effektives Datenschutzmanagement–System mit den oben aufgeführten Prozessen in Ihrem Unternehmen integrieren und vor allem die einzelnen Schritte dokumentieren, sodass Sie – auch gegenüber einer Aufsichtsbehörde – nachweisen können, dass Sie geeignete Strategien und Maßnahmen ergriffen haben. Eine unzureichende Dokumentation der datenschutzrechtlichen Umsetzung der DS-GVO kann sich maßgeblich auf die Höhe des Bußgeldtatbestands auswirken.

Mit welchem Aufwand muss ich für die Umstellung rechnen?

Der Aufwand wird von Unternehmen zu Unternehmen variieren – je nachdem wie viele relevante Datenverarbeitungsprozesse und Verträge zu prüfen sind und welche Relevanz geänderte Vorschriften für die Unternehmensprozesse haben. Er hängt auch davon ab, wie umfangreich und übersichtlich die bisherige Dokumentation der Datenverarbeitungsprozesse aussieht.

Im Folgenden sind einige Faktoren genannt, die Sie für die Aufwandsabschätzung zu Hilfe nehmen können:

- Anzahl der bereits dokumentierten Verfahren im Verfahrensverzeichnis – Anzahl der noch zu dokumentierenden Verfahren? Muss ein Verfahrensverzeichnis neu erstellt werden? Mit wie vielen Abteilungen ist zu sprechen?
- Zeit, die für Überarbeitung einer (mehrerer) Datenschutzerklärung(en) benötigt wird und Zeit für Überprüfung der X Verfahren, für die eine gesonderte Einwilligung benötigt wird
- Verhandlung mit dem Betriebsrat über Ergänzung / Änderung von Betriebsvereinbarung(en)?
- Anzahl ADV-Vereinbarungen x Zeit für Check + Zeit für ggf. Neuverhandlung mit Vertragspartner
- Überarbeitung des bisherigen Prozesses, Einbeziehung aller Beteiligten
- Schulungen der Mitarbeiter
- Rechenschaftspflicht führt zu mehr Dokumentationsaufwand

Welche Abteilungen im Unternehmen sollten über Änderungen informiert werden?

Neben dem betrieblichen Datenschutzbeauftragten sollten auch andere Stellen in Ihrem Unternehmen über die Änderungen in der DS-GVO informiert werden:

- **Geschäftsleitung:** Die Geschäftsleitung sollte über die veränderte datenschutzrechtliche Praxis in Ihrem Unternehmen Bescheid wissen.
- **Recht und Compliance:** Durch die DS-GVO müssen voraussichtlich eine Vielzahl an Verträgen angepasst werden. Ihre Compliance-Abteilung muss zudem bei der Gefährdungsanalyse Risiken für Datenschutzverstöße miteinbeziehen, die durch die hohen Bußgelder deutlich höher zu bewerten sind.
- **IT-Security:** Für das geforderte Risk Assessment zur Festlegung der technisch-organisatorischen Maßnahmen sollte man prüfen wie diese sinnvoll mit ohnehin bereits durchgeführten IT-Security Risikoassessments harmonieren oder sich ergänzen können.

- **Finanzen:** Durch die Anpassungsprozesse können Ihrem Unternehmen erhebliche Kosten entstehen, die von Ihrem Unternehmen berücksichtigt werden müssen.

- **Forschung und Entwicklung:** Vorschriften wie »Privacy by Design« und »datenschutzrechtliche Voreinstellungen« stellen u. a. auch Anforderungen an die Produktentwicklung- und Implementierung. Es sollten daher schon in frühem Projektstadium bei Produktentwicklungen auf die Einhaltung datenschutzrechtlicher Prinzipien geachtet werden.

- **Personalabteilung und Betriebsrat:** Bei der Nutzung von an die DS-GVO angepassten Betriebsvereinbarungen zur Regelung des Beschäftigtendatenschutzes sollten Sie die Mitbestimmungsrechte des Betriebsrates gem. §87 Abs.1 Nr.6 BetrVG im Blick haben. Außerdem werden Mitarbeiterschulungen nötig werden.

Wer gibt Hilfestellung bei der Auslegung?

- Die **Erwägungsgründe der DS-GVO** müssen zur Auslegung der Artikel mit herangezogen werden.

- **Artikel 29 Working Party:** Die Artikel-29-Datenschutzgruppe wurde im Rahmen der Richtlinie 95/46/EG eingerichtet und besteht hauptsächlich aus Vertretern der Datenschutzbehörden der EU-Mitgliedsstaaten. Die Gruppe hat eine beratende Funktion und veröffentlicht regelmäßig Informationen (Stellungnahmen, Interpretationsleitfäden, usw.) auf ihrer ↗ **Webseite**. Am 2. Februar 2016 stellte die Artikel-29-Gruppe ihren ↗ **Aktionsplan zur Umsetzung der DS-GVO** für 2016 vor.

- Eine der Hauptaufgaben der EU-Aufsichtsbehörden wird darin bestehen, den sogenannten **»Europäischen Datenschutzausschuss«** zu formen, der zukünftig mit eigener Rechtspersönlichkeit das zentrale Datenschutzgremium in Europa bildet und die Artikel-29-Gruppe damit ersetzt. Er setzt sich zusammen aus einem Präsidenten der jeweiligen nationalen Aufsichtsbehörde. Durch ihn wird zukünftig die verstärkte Koordinierung der Aufsichtsbehörden stattfinden (Kooperations- und Kohärenzmechanismus), z. B. bei Beschwerdeverfahren gegen Unternehmen, die europaweit tätig sind. Noch ist offen, wen Deutschland als Vertreter bestimmt.

- Zusätzlich wird die Artikel-29-Gruppe Praxishilfen für Unternehmen erstellen. Die ersten in 2016 bearbeiteten Themen werden die folgenden sein:

  - **Datenschutzfolgeabschätzung:** Die DS-GVO schreibt erstmalig Unternehmen vor, vor bestimmten Datenverarbeitungen eine Datenschutzfolgeabschätzung durchzuführen. Erste Ansätze wurden bereits in einigen Ländern z. B. von der französischen Aufsichtsbehörde CNIL in ↗ **Frankreich** und dem britischen ICO in ↗ **Großbritannien** entwickelt. Auch in der internationalen Standardisierung werden hier bereits erste Konzepte entwickelt (ISO DIS 29134 Management Standard Privacy Impact Assessment). Die Artikel-29-Gruppe wird wohl bisher bestehende Ansätze weiterentwickeln und an die Vorgaben der DS-GVO anpassen.

- **Recht auf Datenübertragbarkeit:** Das Recht auf Datenübertragbarkeit, wonach der Betroffene nicht nur das Recht hat, die Daten in einem gängigen Format zu erhalten, sondern auch das Recht, diese Daten an eine andere Stelle zu übermitteln, ist neu. Der ursprüngliche Grundgedanke war eine Datenübertragbarkeit von Inhalten, die in soziale Netzwerke oder andere Plattformen eingestellt wurden. Der Wortlaut ist jedoch so allgemein gehalten, dass es unklar ist, ob und wie dieses Recht auf andere Dienstleistungen des Web 2.0 Anwendung finden soll. Die Artikel-29-Gruppe wird wohl Hilfestellung bei der Interpretation geben.
- **Zertifizierung:** Der Auftragsverarbeiter kann seine Datenverarbeitungsvorgänge von einer akkreditierten Zulassungsstelle oder eine Aufsichtsbehörden zertifizieren lassen und gegenüber seinem Auftragsgeber den Nachweis für die Einhaltung seiner Pflichten nach DS-GVO zu erbringen.
- **Datenschutzbeauftragter:** Anders als in Deutschland gab es bisher in vielen Ländern keine Verpflichtung zur Bestellung eines betrieblichen DSB. Die Artikel-29-Gruppe hat wohl daher dieses Thema priorisiert. In Deutschland wurde bereits langjährige Expertise aufgebaut (siehe auch ↗ hier), auf die zurückgegriffen werden kann, da sich durch die DS-GVO nicht viel verändert hat.

Für die Jahre 2017 und 2018 werden neue Prioritäten von der Artikel-29-Gruppe festgelegt.

- **Der Europäische Datenschutzbeauftragte:** Der Europäische Datenschutzbeauftragte (eng. EDPS) ist die unabhängige Behörde auf EU-Ebene, deren Aufgabe es unter anderem ist einen kohärenten Datenschutz sicherzustellen. Auf seiner ↗ Webseite veröffentlicht der EDPS auch Informationen zur Grundverordnung. Er hat in seiner ↗ Strategie für 2015 – 2019 aufgeführt, welche Rolle er bei der DS-GVO übernehmen möchte. Zum einen wird das EDPS-Büro zukünftig das Sekretariat für den neuen Datenschutzausschuss übernehmen und eng mit den EU-Datenschutzbehörden (z. B. bei der Erstellung von Praxisleitfäden und Fortbildungen) zusammenarbeiten. Zusätzlich möchte der EDPS ein webbasiertes Repositorium für Datenschutzinfos aufbauen und sich bei der sektorspezifischen Gesetzgebung engagieren.

- **Aufsichtsbehörden auf deutscher Ebene:**
  - **Bundesbeauftragte für den Datenschutz und die Informationssicherheit:** Die Bundesbeauftragte hat eine Informationsbroschüre mit endgültigem Text zur künftigen Europäischen Datenschutz-Grundverordnung veröffentlicht. Die BfDI Info 6 zur Datenschutz-Grundverordnung ist ↗ hier abrufbar. Eine gute Übersicht »Datenschutz kompakt« ist ↗ hier abrufbar.
  - **Der Düsseldorfer Kreis:** Der Düsseldorfer Kreis ist der Arbeitskreis der unabhängigen deutschen Datenschutzbehörden des Bundes und der Länder und zuständig für deren Kommunikation, Kooperation und Koordinierung. Er ist in verschiedene Arbeitsgremien eingeteilt und veröffentlicht ↗ Datenschutzrichtlinien und Praxishilfen für bestimmte Themen.

- **Bayrische Datenschutzbehörde:** Das Bayrische Landesamt für Datenschutz veröffentlicht verschiedene kurze ↗ Papiere zur DS-GVO. Es wurden bisher Beiträge zu folgenden Themen veröffentlicht:
  - Videoüberwachung nach der DS-GVO – ein Ausblick (06.07.2016)
  - Art. 42 DS-GVO – Zertifizierung (22.06.2016)
  - Veröffentlichung zum Art. 32 DS-GVO – Sicherheit der Verarbeitung (10.6.2016)
  - Recht auf Löschung (»Vergessenwerden«) – Art. 17 DS-GVO (19.07.2016)
  - Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO (02.08.2016)
  - Besondere Kategorien personenbezogener Daten – Art. 9 DS-GVO (17.08.2016)
  - Sanktionen nach der DS-GVO – (01.09.2016)

- **Aufsichtsbehörden anderer EU-Länder:**
  - **Vereinigtes Königreich – ICO:** Trotz des Brexit wird der ICO auch in Zukunft eine wichtige Rolle beim Thema Datenschutz in Europa einnehmen. Der ICO hat bereits viele hilfreiche Beiträge für Unternehmen zur DS-GVO auf seiner ↗ Website veröffentlicht, u. a. eine ↗ 12-Schritte-Checkliste für Unternehmen sowie eine ↗ Übersicht zur DS-GVO. Er will in den nächsten 6 Monaten zusätzlich zu folgenden ↗ Themen etwas veröffentlichen: Datenschutzrechte, Verträge, Einwilligung und Codes of Conduct.
  - **Frankreich – CNIL:** Die französische Aufsichtsbehörde CNIL veröffentlichte bisher ↗ Leitlinien zur DS-GVO und führt bis zum 15. Juli 2016 eine ↗ Online-Konsultation zu den von der Artikel-29-Gruppe priorisierten Themen (siehe oben) durch.
  - **Spanien – AEPD:** Die spanische Aufsichtsbehörde hat ein Dokument zur ↗ Implementierung der DS-GVO am 29. Juni 2016 veröffentlicht. Die Empfehlungen schließen insbesondere die Themen Einwilligung, Informationspflichten, Datenschutzfolgeabschätzung, Zertifizierung, Datenschutzbeauftragter, Verhältnis zwischen verantwortlicher Stelle und Auftragsverarbeiter mit ein. Zusätzlich gibt es eine ↗ Checkliste für Unternehmen.
  - **Dänemark – Datatilsynet:** Auch die dänische Aufsichtsbehörde hat am 21. Juni 2016 ein erstes ↗ Q&A Dokument als Checkliste zur DS-GVO veröffentlicht, das Unternehmen erste Informationen zu Themen wie Einwilligung, Datenverarbeitung von Kindern und Datenschutzmeldungen gibt.
  - **Finnland – VAHTI:** Das finnische Ministerium für Finanzen und Cyber Security Management unterstützt finnische Unternehmen in der Umsetzungsphase der DS-GVO und veröffentlichte hierzu am 2. Juni 2016 ein umfangreiches ↗ Dokument.

- **Bitkom Leitfäden:**
  - **Auftragsdatenverarbeitung:**
    ↗ Mustervertragsanlage zur Auftragsdatenverarbeitung. Diese werden derzeit an die Anforderungen der DS-GVO angepasst.
  - **Dokumentationspflichten:**
    Leitfaden: ↗ Das Verfahrensverzeichnis BDSG – Ein Praxisleitfaden (Version 3.0).
    Stand März 2016.
  - **Internationaler Datentransfer:**
    - Leitfaden ↗ »Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer«
      Dieser Leitfaden wird demnächst an die Anforderungen der DS-GVO angepasst (Version 1.1.): Mit Infos zu den Auswirkungen des EuGH-Urteils zu Safe Harbor und der Anwendung von Standardvertragsklauseln.
    - ↗ Safe-Harbor-Urteil des EuGH und die Folgen. Fragen und Antworten.

- **Weitere Links:**
  - ↗ Übersicht DS-GVO mit Erwägungsgründen
  - BvD: Datenschutz-Grundverordnung (DS-GVO) als ↗ Website übersichtlich dargestellt
  - Oppenhoff & Partner: ↗ Synopse Übersicht BDSG / DS-GVO
  - Wybitul/Böhm: ↗ Das neue Datenschutzrecht (Juli 2016) – Folgen für Compliance und interne Ermittlungen

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 79 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, weitere 9 Prozent kommen aus Europa, 8 Prozent aus den USA. 4 Prozent stammen aus Asien, davon die meisten aus Japan. Bitkom fördert die digitale Transformation der deutschen Wirtschaft und setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org