DIE EU-DATENSCHUTZ-GRUNDVERORDNUNG

Praxishilfen zur Implementierung der EU-DSGVO in Verbänden

Die EU erhält ein einheitliches Datenschutzgesetz. Obwohl die Datenschutz-Grundverordnung schon 2016 beschlossen wurde, wird sie erst ab dem 25. Mai 2018 angewendet. Im Verbändereport haben wir in den vergangenen zwei Jahren über die Anforderungen der EU-DSGVO berichtet und dargestellt, welche Änderungen diese für Verbände mit sich bringen. Der vorliegende Schwerpunkt zur EU-DSGVO fasst nochmals alle wichtigen Aspekte der neuen Verordnung zusammen und soll eine Praxishilfe für die Umsetzung im Verband

FAQ EU-DSGVO

RALF WICKERT
Rechtsanwalt und Fachanwalt
für Steuer- und Arbeitsrecht

Ralf Wickert ist Rechtsanwalt und berät seit vielen Jahren Verbände und Ihre Organisationseinheiten auch in datenschutzrechtlicher Hinsicht. Mit Blick auf die neue Datenschutz-Grundverordnung antwortet er hier auf die am häufigsten gestellten Fragen von Verbänden und Organisationen.

WARUM GIBT ES DIESE NEUE VERORDNUNG UND WAS WAR DER ANLASS DAFÜR?

Zwar gab es in Europa schon einen Vorläufer der Datenschutz-Grundverordnung, nämlich die europäische Datenschutz-Richtlinie. Diese wurde jedoch in vielen Mitgliedstaaten praktisch nicht umgesetzt, sodass ein ganz unterschiedliches Schutzniveau in Europa entstanden ist. Dies war Anlass für die Europäische Union, einen Mindeststandard im Datenschutz durch eine unmittelbar für alle Organisationen, gleich ob privat oder staatlich, geltende Verordnung einzuführen. Insbesondere die erheblichen technischen Veränderungen und die Nutzung elektronischer Medien führen dazu, dass immer tiefer in die Privatsphäre von Betroffenen eingegriffen werden kann. Man denke nur an das sogenannte Web-Tracking. Demzufolge muss der Gesetzgeber heute Spielregeln festsetzen, an die sich alle halten müssen.

ÄNDERT SICH DURCH DIE DATENSCHUTZ-GRUNDVERORDNUNG WIRKLICH SO VIEL FÜR VERBÄNDE ODER MÜSSEN SIE EIGENTLICH NUR KLEINERE MASSNAHMEN VORNEHMEN?

Deutschland gilt seit vielen Jahren als Vorreiter in datenschutzrechtlichen Fragen. Jedenfalls vom gesetzgeberischen Rahmen aus gesehen. Allerdings waren weder die Aufsichtsbehörden personell so ausgestattet, dass die Einhaltung des Datenschutzes auch wirklich kontrolliert werden konnte, noch gab es in den Unternehmen und Organisationen eine flächendeckende Umsetzung. Diejenigen Organisationen, die bislang datenschutzkonform gearbeitet haben, müssen ihr Datenschutz-Management insbesondere im Bereich der Transparenzregelungen etwa zur Erfüllung von Informationspflichten im Sinne der Art. 13 und 14 DSGVO ergänzen. Weiterhin gibt es in der Datenschutz-Grundverordnung auch neue Bereiche, so etwa die Datenschutz-Folgeabschätzung oder das Verzeichnis von Verarbeitungstätigkeiten. Vieles ist aber auch gleich geblieben, so etwa die wesentlichen Voraussetzungen für die Bestellung eines sogenannten betrieblichen Datenschutzbeauftragten.

UNTERFALLEN ALLE VERBÄNDE DEM DATENSCHUTZ ODER GIBT ES HIER AUSNAHMEN?

Das Datenschutzrecht ist rechtsformneutral, sodass alle Verbände hierunter fallen, unabhängig davon, ob sie etwa als rechtsfähiger oder nicht rechtsfähiger Verein organisiert sind. Jede rechtlich selbstständige Organisation ist ein eigener datenschutzrechtlicher Verantwortlicher. Hat etwa eine Verbandsorganisation neben dem Bundesverband auch Landesverbände, die eigenständig organisiert sind, so unterfallen diese selbstständig dem Datenschutzrecht. Gleiches gilt für eine Service-GmbH. Auch die öffentlich-rechtlichen Verbände, etwa die berufsständischen Kammern, fallen hierunter. Größenbedingte Ausnahmen gibt es nicht.

MUSS JEDER VERBAND EINEN DATENSCHUTZBEAUFTRAGTEN BESTELLEN?

Das Konzept des betrieblichen Datenschutzbeauftragten ist einerseits in Art. 37 DSGVO und andererseits für die privatrechtlich organisierten Verbände in § 38 BDSG neu geregelt. Öffentlich-rechtliche Verbände benötigen immer einen Datenschutzbeauftragten (§ 5 Abs. 1 BDSG neu für die dem Bundesrecht unterfallenden öffentlich-rechtlichen Verbände). Nach § 38 BDSG neu ist ein betrieblicher Datenschutzbeauftragter zu bestellen, wenn mindestens zehn Personen (Achtung, der Begriff der Personen geht über den Begriff der Arbeitnehmer hinaus und umfasst etwa auch freie Mitarbeiter die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.) Damit ist jedenfalls bei einer Verbandsgeschäftsstelle in entsprechender Größe regelmäßig allein wegen dieser Vorschrift ein betrieblicher Datenschutzbeauftragter zu bestellen.

Bei kleineren Verbänden greift oftmals Art. 37 Abs. 1 lit. c DSGVO für die Bestellpflicht ein, wonach auch kleinere Verbände einen Datenschutzbeauftragten zu bestellen haben, wenn sie in einer gewissen Regelmäßigkeit besondere Kategorien personenbezogener Daten (insbesondere die Gewerkschaftszugehörigkeit und Gesundheitsdaten spielen bei Verbänden eine Rolle) automatisiert verarbeiten.

Verbände können wählen, ob sie einen internen Datenschutzbeauftragten oder einen externen Datenschutzbeauftragten benennen. Der interne Datenschutzbeauftragte genießt besonderen Kündigungsschutz gemäß § 38 Abs. 2 i. V. m. § 6 Abs. 4 BDSG neu. In jedem Falle sollten nur solche Personen als interne Datenschutzbeauftragte bestellt werden, die auch ein gewisses Interesse für den Datenschutz mit bringen, sodass eine fachliche Einarbeitung sichergestellt ist. Die häufig gestellte Frage, ob der IT-Leiter Datenschutzbeauftragter sein soll, würde ich glatt verneinen, da der zu Kontrollierende nicht zugleich der Kontrollierende sein sollte.

WIE GEHE ICH DENN ALS VERBAND VOR, WENN ICH MICH BISLANG MIT DEM THEMA DATENSCHUTZRECHT NOCH NICHT SO RICHTIG BESCHÄFTIGT HABE?

Zunächst einmal muss ich klären, welche personenbezogenen Daten ich überhaupt in welchen grundsätzlichen Verarbeitungsprozessen verarbeite. Personenbezogene Daten sind all diejenigen Daten, die einen Hinweis auf natürliche Personen geben, wie etwa die Adresse, das Alter oder Bankdaten. Das reine Foto auf einer Verbandswebsite ohne jeden Namenszusatz unterfällt dem Kunsturhebergesetz. Auch Wirtschaftsverbände verarbeiten selbstverständlich personenbezogene Daten, auch wenn die reine Mitgliederkartei selbst kein personenbezogener Datensatz ist, wenn nur Kapitalgesellschaften oder Personenhandelsgesellschaften Mitglied sind. Sobald man aber den Geschäftsführer zuspeichert, ist man bereits im Datenschutzrecht unterwegs.

Als Verband sollte man zunächst einmal alle klassischen Verbandsprozesse, in denen personenbezogene Daten verarbeitet werden, erfassen. Dies sind etwa die Mitgliederverwaltung, die Kommunikation mit Mitgliedern, die Erteilung von Rechtsberatung, die Durchführung von Seminaren oder auch die Personalverwaltung. Hat man diese Standardprozesse und die dabei verarbeiteten personenbezogenen Daten erfasst, muss man sich über die Rechtsgrundlage und damit über die Rechtmäßigkeit Gewissheit verschaffen. Dies ist in Art. 6 DSGVO geregelt. Nach dieser Norm darf derjenige personenbezogene Daten verarbeiten, der entweder über eine Einwilligung verfügt oder dies in Ausführung eines Vertrages tut (auch die Verbandsmitgliedschaft selbst ist ein Vertrag ebenso wie der Besuch eines Seminars), oder wenn das Gesetz dies selbst fordert (hier spielen z. B. Archivierungspflichten aus § 147 der Abgabenordnung eine zentrale Rolle). Daneben dürfen auch diejenigen Daten verarbeitet werden, die einem berechtigten Interesse des Verbandes unterfallen. Das berechtigte Interesse muss aber dann mit den Interessen der betroffenen Personen abgewogen werden. Klassischer Anwendungsbereich ist die Werbung, die von der Datenschutz-Grundverordnung selbst als berechtigtes Interesse bezeichnet wird. Hier kann also ein Verband bestimmte Kontaktdaten wie etwa die postalische Anschrift und den Namen für die Versendung von Werbematerial für Fortbildungsangebote nutzen. Andere Kontaktwege, wie etwa Mail-Kontakt oder Telefonanrufe, unterfallen hinsichtlich der Zulässigkeit § 7 UWG und müssen demgemäß an wettbewerbsrechtlichen Grundsätzen gemessen werden.

Bittet der Verband um die Einwilligung für eine bestimmte Datenverarbeitung, so ist man künftig nicht mehr an die Schriftlichkeit des alten Datenschutzrechts gebunden, sondern kann dies auch elektronisch (also per Mail) erbitten. Inhaltlich ändert sich bei der Einwilligung nur wenig, da auch nach dem neuen Recht die sogenannte informierte Einwilligungspflicht gilt, der Betroffene also wissen muss, was man mit den Daten beabsichtigt.

Fundraising TAG

STUTTGART

DONNERSTAG, 28. JUNI 2018
TAGUNGSZENTRUM BERNHÄUSER FORST

WISSEN, INSPIRATION UND SPANNENDE GESPRÄCHE

Hier treffen sich Engagierte aus Vereinen und Stiftungen, lernen gemeinsam Neues und tauschen sich fachlich aus. Melden auch Sie sich gleich an!

FACHWISSEN AUS DER AKTUELLEN PRAXIS

Referenten aus Non-Profit-Organisationen oder der Fundraising-Branche vermitteln praktisches, anwendungsorientiertes Wissen aus erster Hand.

KONTAKTE KNÜPFEN UND VERTIEFEN

Sponsoren und Aussteller kommen direkt mit interessierten Vertretern der NGOs ins Gespräch. Nutzen auch Sie diese Gelegenheit!

INFORMATIONEN UND ANMELDUNG
www.fundraisingtage.de

EINE VERANSTALTUNGSREIHE DES Fundraiser magazin

WELCHE TECHNISCHEN MASSNAHMEN MUSS EIN VERBAND ERGREIFEN?

Die Datenschutz-Grundverordnung hat keine Regelung, die § 9 BDSG in seiner heutigen Fassung entspricht. Inhaltlich dürfte jedoch der technische Maßnahmenkatalog nach neuem Recht nicht viel anders aussehen als nach altem Recht. Demgemäß müssen in einem technisch-organisatorischen Maßnahmenkonzept diejenigen Maßnahmen technischer und organisatorischer Art beschrieben werden, die der Verband zum Schutz personenbezogener Daten ergriffen hat. Dies sind etwa Zutrittsrechte zu Serveranlagen, die sich idealerweise ja in einem abgeschlossenen Raum befinden und Zugriffsrechte auf Dateien, wo der Passwortschutz eine Rolle spielt. Weiter spielen in diesem Zusammenhang Zugriffsrechte eine Rolle, also die Frage, welche Abteilung der Verbandsgeschäftsstelle zulässigerweise welche Daten benutzen darf. Bei der Verpflichtung zu einer Organisation der Weitergabekontrolle geht es um Verschlüsselungstechnik etwa bei E-Mail-Versendung. Im Rahmen der Verfügbarkeitskontrolle müssen die Maßnahmen dargestellt werden, die mit der Sicherung von Daten in Kopien und Back-up ergriffen wurden. Ein solches Maßnahmenkonzept kann nur in Zusammenarbeit mit der EDV-Abteilung bzw. dem EDV-Dienstleister erstellt werden und sollte auch dokumentiert werden.

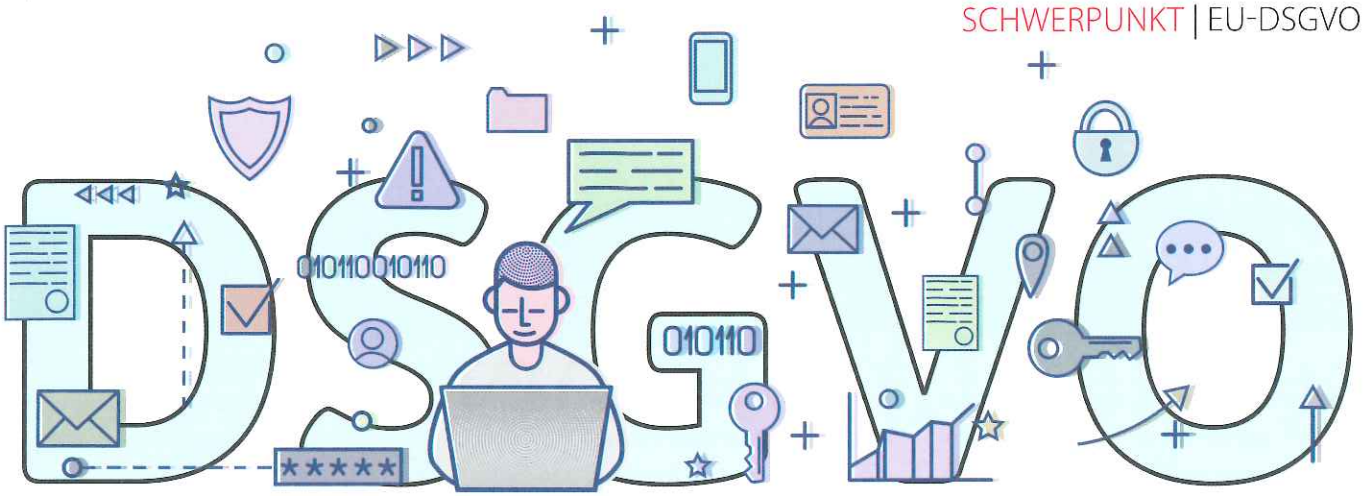
Solche Maßnahmen technischer Art müssen in einem gewissen Turnus überprüft werden, da die Datenschutz-Grundverordnung dem Umstand Rechnung trägt, dass sich technische Schutzvorrichtungen naturgemäß weiterentwickeln und demgemäß nicht statisch einmal praktisch für Jahre implementiert werden.

KANN MAN DATEN EIGENTLICH EWIG VORHALTEN?

Aufgrund der technischen Entwicklung von Speichermedien ist es heute jedenfalls keine Kapazitätsfrage mehr, personenbezogene Daten praktisch ewig abzuspeichern. Dies geschieht frei nach dem Motto, dass man Daten ja immer wieder gebrauchen kann. Genau das will das Datenschutzrecht verhindern und verpflichtet die Verbände in Art. 17 DSGVO, ein sogenanntes Löschkonzept zu entwickeln. In diesem Löschkonzept müssen die Verbände die Maßnahmen beschreiben, wann sie welche Daten löschen. So kann man etwa sagen, dass Vertragsdaten nach Ablauf von Gewährleistungspflichten zu löschen sind, es sei denn, sie sind in ein Archiv zu überführen und müssen etwa in dieses übertragen werden. Das Archiv wäre eine andere Löschklasse. Ein solches Löschkonzept ist idealerweise eng mit der EDV-Abteilung abzustimmen, da es ja über die Software auch abgebildet werden, d. h. umgesetzt werden muss.

MAN LIEST SO VIEL ÜBER TRANSPARENZPFLICHTEN. WAS MUSS HIER AUS SICHT EINES VERBANDES GENAU GEMACHT WERDEN?

In der Tat gibt es hier ganz neue Anforderungen. Sah das bisherige Datenschutzrecht in § 34 BDSG „nur" vor, dass betroffene Personen Auskunft über die gespeicherten Daten beim Verband verlangen konnten – was in der Praxis nicht allzu häufig geschah –, so müssen künftig die Verbände von sich aus die Betroffenen informieren. Art. 13 und Art. 14 DSGVO verpflichten die Verbände dazu, bei Erhebung der Daten den Betroffenen selbst oder über Dritte zu informieren. So muss etwa bei Buchung eines Fortbildungsseminars, welches ein Verband durchführt, der Seminarteilnehmer auf der Eingangsbestätigung darüber informiert werden, welche zentralen Datenschutzprozesse beim Verband abgebildet werden. Die genauen Informationsinhalte sind in Art. 13 und Art. 14 DSGVO exakt beschrieben. Praktisch kann dies etwa dadurch geschehen, dass der Verband bei einer Onlinebestätigung per Link auf die Webseite weiterleitet, wo die entsprechenden Angaben gemacht sind. Auch dies sollte künftig in die Routineprozesse zusammen mit der EDV eingepflegt werden, da hier die Betroffenen ganz schnell merken, welche Verbände sich mit dem Datenschutz beschäftigen bzw. nicht.



IN DEN MEDIEN WIRD SO VIEL ÜBER DIE HOHEN BUSSGELDER BERICHTET. AUF WAS HAT MAN SICH DENN HIER ALS VERBAND EINZUSTELLEN?

In der Tat bekommt man es mit der Angst zu tun, wenn man das Gesetz liest. Art. 83 DSGVO beschreibt Bußgelder, die bis zu 20 Millionen Euro gehen können. Dies ist aber sicherlich nicht auf Verbände gemünzt und betrifft auch nicht den Normalfall. Auf der anderen Seite sind die Zeiten vorbei, wo mit Kleinst-Bußgeldern praktisch noch ein Anreiz dafür gegeben wurde, gegen das Datenschutzrecht durch Untätigkeit zu verstoßen, weil man nach drei Jahren unentdeckter Verstöße praktisch schon auf der Gewinnerseite war. Wenn die Ausgangsbußgelder so hoch sind, ist auch das Eingangsbußgeld höher als vorher. Da muss man kein Prophet sein. Wenn man dann noch weiß, dass die Aufsichtsbehörden personell aufrüsten, muss man auch mit einer Umsetzung des Bußgeldrahmens rechnen.

Bei der Bußgeldhöhe spielt sicherlich die Art des Verstoßes eine Rolle. So sind etwa nicht gemeldete Datenpannen sicherlich eher bußgeldrelevant als eine einmalige Verletzung einer Informationspflicht. Datenpannen können etwa abhandengekommene Laptops oder Handys betreffen und müssen in der Regel der Aufsichtsbehörde gemeldet werden. Hiervon kann man nur absehen, wenn praktisch keine Risiken für die Betroffenen, deren Daten auf dem Gerät gespeichert wurden, ersichtlich sind. Dies dürfte aber in der Praxis eher die Ausnahme sein. In manchen Fällen, also denjenigen, wo hohe Risiken für die Betroffenen bestehen, muss auch diesen gegenüber die Datenpanne offengelegt werden. Das Problem bei den Datenpannen ist, dass die Leitung der Geschäftsstelle erst einmal selbst Kenntnis von der Datenpanne haben muss, da eine nachvollziehbare Neigung der Mitarbeiter besteht, solche Pannen, die ja auf eigene fahrlässige Pflichtverletzung hindeuten, zu verschweigen. Hier sollte man eine klare Richtlinie erlassen, die die Mitarbeiter dazu verpflichtet, solche Pannen zu benennen, und ihnen auch erst einmal erklärt, was eigentlich eine Datenpanne ist.

Insgesamt wird sich die Höhe des Bußgeldes nach Art. 83 Abs. 1 DSGVO daran orientieren, wie der Verband sich überhaupt mit dem Thema Datenschutz auseinandergesetzt hat. Hat der Verband die notwendigen datenschützenden Maßnahmen ergriffen und passiert dann trotzdem etwas, so wird dies bei der Bemessung etwaiger Bußgelder schon kraft Gesetzes berücksichtigt. Umgekehrt gilt, dass der Verband, der das Datenschutzrecht ignoriert, letztlich bei den Bußgeldern mit drakonischen Strafen zu rechnen hat.

WAS GILT EIGENTLICH BEI DER HANDY- UND LAPTOPNUTZUNG?

Handys und Laptops sind fast eine Art Statussymbol von Arbeitnehmern. Da Verbände Dienstleistungsorganisationen sind, kommen solche Geräte dort in erheblichem Umfang zum Einsatz. Hier müssen klare Spielregeln gelten. So kann es nicht sein, dass Arbeitnehmer der Verbandsgeschäftsstelle einfach solche Geräte nutzen, wie sie es wollen. Der Klassiker ist etwa die Nutzung von Whatsapp, die aus datenschutzrechtlicher Sicht ein echtes Problem ist, da solche Messenger-Dienste praktisch das gesamte Handy auslesen und in die USA, also ein Drittland, was dazu noch kein organisiertes Datenschutzrecht besitzt, übermittelt. Würde dies etwa bei einer Gewerkschaft geschehen und wäre die Mitgliederkartei auf dem Handy, so hätte man ein echtes Problem. Dies sollte alles in einer Richtlinie geregelt werden, in der dann auch etwa die Zulässigkeit der privaten Nutzung von dienstlichen E-Mail-Accounts vorgegeben werden sollte. Gestattet der Arbeitgeber, also der Verband, eine solche Nutzung, so wird er zum Diensteanbieter und darf praktisch in seinen eigenen Account nicht mehr hineinschauen. Er würde sich dann sogar strafbar machen. Dies sind alles Dinge des Arbeitnehmerdatenschutzes, die man tunlichst vorher regeln sollte, um hier klare und transparente Spielregeln zu schaffen.

Wie sollte ein Verband bei der Implementierung der DSGVO vorgehen?

ANALYSE DES IST-ZUSTANDES

Welche personenbezogenen Daten werden verarbeitet?
- Gibt es besondere Kategorien personenbezogener Daten (Art. 9 DSGVO), die im Verband verarbeitet werden?
- In welchen Prozessen werden diese Daten verarbeitet? (z. B. Mitgliederverwaltung, Fortbildung, Presseverteiler, Werbeaktivitäten)
- Mit welcher EDV wird gearbeitet (Software, Endgeräte, Cloud)?
- Hat oder benötigt der Verband einen betrieblichen Datenschutzbeauftragten?

Untersuchung der Rechtmäßigkeit der Datenverarbeitung
- Benötigt der Verband Einwilligungserklärungen?
- Welche Verarbeitungen erfolgen in Erfüllung von Verträgen (Mitgliedschaftsvertrag, Fortbildungsseminarvertrag)?
- Welchen Archivierungspflichten bzw. sonstigen gesetzlichen Pflichten zur Datenverarbeitung unterliegt der Verband?
- Kann sich der Verband auf berechtigte Interessen im Sinne von Art. 6 Abs. lit. f. DSGVO berufen? (z. B. Werbung für Verbandsleistungen)

Analyse der technisch-organisatorischen Maßnahmen
- Welche technischen Schutzmaßnahmen gibt es? (Passwörter, Verschlüsselungen etc.)
- Welche organisatorischen Maßnahmen gibt es? (z. B. Wer greift auf welche Daten zurück?)
- Diese Maßnahmen müssen in ein Konzept überführt werden.

ANSCHLIESSENDE MASSNAHMEN

Maßnahmen zum Datenschutz-Compliance
- Ein Datenpannen-Alarmplan muss existieren.
- Ein Löschkonzept muss regeln, wann welche personenbezogenen Daten gelöscht werden.
- Es muss geklärt werden, ob eine Datenschutz-Folgenabschätzung oder ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen sind.
- Haupt- und Ehrenamt sollten schriftlich auf den Datenschutz verpflichtet werden.

Alle Transparenzpflichten sind zu erfüllen
- Der Verband muss in die Lage versetzt werden, Auskunftsansprüche Betroffener zu erfüllen.
- Die Informationspflichten nach Art. 13 und 14 DSGVO werden in die Prozesse einzuführen sein (z. B. Erfüllung der Informationspflichten über Fernzugriff der Website).

Website des Verbandes und etwaige andere Online-Aktivitäten sollten „als Tor zum Internet" überprüft werden
- Überprüfung der Datenschutzerklärung auf der Website auch unter Darstellung etwaiger datenschutzrelevanter Programme (z. B. Google Analytics)
- Prüfung eines etwaigen Online-Shops

Dienstleister, die mit personenbezogenen Daten des Verbandes arbeiten, also sog. Auftragsverarbeiter, müssen identifiziert und gesetzeskonform behandelt werden
- Analyse der dortigen Datenschutzvorkehrungen
- Abschluss eines Auftragsverarbeitungsvertrages
- Organisation der Kontrolle dieser Dienstleister

Wesentliche Begriffsbestimmungen für die Anwendung der DSGVO*

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst sind. Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie die Auskunft darüber, welche sie betreffende personenbezogene Daten verarbeitet werden.

Zweckbindung

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Als nicht unvereinbar gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Zwecke oder für statistische Zwecke.

Datenminimierung

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherzustellen haben, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Richtigkeit

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

Speicherungsbegrenzung

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

Integrität und Vertraulichkeit

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

Personenbezogene Daten

Definitionsgemäß sind „personenbezogene Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person") beziehen. Der Begriff der personenbezogenen Daten ist allerdings sehr weit gefasst (Art. 4 Nr. 1 DSGVO) und umfasst beispielsweise Informationen wie Name, Adresse, Telefonnummer, Autokennzeichen oder aber auch die IP-Adresse einer Person. Ausreichend ist es, wenn die Informationen einer Person lediglich irgendwie zugeordnet und damit ein Personenbezug hergestellt werden kann. 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.

Die Grundsätze der DSGVO gelten nicht für „anonyme Informationen", d. h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Die Verordnung betrifft somit nicht die Verarbeitung anonymer Daten, dies gilt auch für statistische oder Forschungszwecke. Die DSGVO gilt nicht für die personenbezogenen Daten Verstorbener (Die EU-Mitgliedstaaten können jedoch Vorschriften für die Verarbeitung der personenbezogenen Daten Verstorbener vorsehen.) Soweit keine personenbezogenen Daten betroffen sind, ist die DSGVO nicht anzuwenden.

Besondere Kategorien personenbezogener Daten („Sensible Daten")

Dies sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit

hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

BEISPIELE
Biometrische Merkmale, Krankengeschichte

Gesundheitsdaten

Personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen, werden als „Gesundheitsdaten" definiert. Neben z. B. „Gesundheitsdaten" zählen nun auch ausdrücklich „genetische Daten" und „biometrische Daten" zu den „besonderen Kategorien personenbezogener Daten" (sensible Daten) und unterliegen damit strengeren Maßgaben.

Genetische Daten

„Genetische Daten" sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betroffenen natürlichen Person gewonnen wurden.

Biometrische Daten

„Biometrische Daten" sind mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen und verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder und daktyloskopische Daten.

Kinder

Für die Rechtmäßigkeit der Einwilligung eines Kindes bei einem Angebot von Diensten der Informationsgesellschaft legt die DSGVO eine Altersgrenze von 16 Jahren fest. Die EU-Mitgliedstaaten können niedrigere Altersgrenzen vorsehen, allerdings nicht unter das vollendete 13. Lebensjahr.

Verarbeitung

Unter dem Begriff „Verarbeitung" versteht die DSGVO jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang in Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

BEISPIELE
Erstellung einer Kundendatei, Aufnahme der Daten zur Erstellung einer Rechnung, Mitarbeiterdatenbank.

Automatisierte und nicht automatisierte Verarbeitung

Die DSGVO bezieht schließlich jede automatisierte Verarbeitung und jede nicht automatisierte Verarbeitung bei Speicherung in einem Dateisystem mit ein. Bei einer automatisierten Verarbeitung werden beispielsweise Computer, Smartphones, Kameras, Webcams, Dashcams, Scanner oder Kopierer erfasst. Jede Benutzung von Computer, Internet, E-Mail kann also zur Anwendbarkeit der DSGVO führen, wenn personenbezogene Daten betroffen sind. Eine nicht automatisierte Verarbeitung liegt insbesondere bei handschriftlichen Aufzeichnungen vor.

Dateisystem

Ein Dateisystem ist nach Art. 4 Nr. 6 DSGVO „(…) jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob die Sammlung, zentral, dezentral oder funktionalen oder geografischen Gesichtspunkten zugeordnet geführt wird. Damit sind etwa Akten, Aktensysteme oder Deckblätter erfasst."

Dass insbesondere bei handschriftlichen Aufzeichnungen noch ein weiterer Anwendungsbereich der DSGVO angestrebt wurde, verdeutlicht die Formulierung „gespeichert werden sollen" in Art. 2 Abs. 1 DSGVO. Hierbei reicht bereits die Absicht aus, dass personenbezogene Daten in ein Dateisystem aufgenommen werden.
Das kann auch eine Aktenverwaltung betreffen. Das Dateisystem kann automatisiert oder manuell geführt werden. Die Regelung ist technologieneutral.

BEISPIELE
Kundendatei (elektronisch oder in Papierform)

Verantwortlicher und Auftragsverarbeiter

„Verantwortlicher" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche bzw. die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

BEISPIELE
Der Unternehmer, der Kundendaten von natürlichen Personen zur Erstellung einer Rechnung an den Kunden erfasst, ist „Verantwortlicher". Der externe Buchhalter, der die Rechnungsdaten für die Bilanzerstellung von diesem Unternehmer erhält und verarbeitet, ist „Auftragsverarbeiter". Weitere Beispiele für den „Auftragsverarbeiter" sind das Rechenzentrum oder der Cloud-Anbieter.

Einwilligung

Als „Einwilligung" der betroffenen Person gilt jede freiwillig für den Einzelfall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit

der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig.

Pseudonymisierung

„Pseudonymisierung" ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden. Die Anwendung der Pseudonymisierung auf personenbezogene Daten kann die Risiken für die betroffenen Personen senken und die Verantwortlichen und die Auftragsverarbeiter bei der Einhaltung ihrer Datenschutzpflichten unterstützen. Durch die ausdrückliche Einführung der „Pseudonymisierung" in die DSGVO ist jedoch nicht beabsichtigt, andere Datenschutzmaßnahmen auszuschließen.

Binding Corporate Rules

Binding Corporate Rules (BCR) sind ein Rahmen zum Umgang mit personenbezogenen 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 einige Vorteile für Konzerne.

„One-Stop-Shop-Prinzip"

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 Bürokratie.

Erleichterter Datenaustausch in einer Unternehmensgruppe

Die DSGVO stellt weniger strenge Anforderungen an die Übermittlung personenbezogener Daten zwischen Verantwortlichen, die Teil einer Unternehmensgruppe sind. Art. 6 Abs. 1 (f) DSGVO differenziert anders als das BDSG nicht zwischen Datenverarbeitungen für eigene Zwecke und Datenverarbeitungen zur Wahrung berechtigter Interessen Dritter. Die Vorschrift erlaubt die Datenverarbeitung zur Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen. Erwägungsgrund 37 zur DSGVO stellt zudem klar, dass Verantwortliche, die Teil einer Unternehmensgruppe sind, ein berechtigtes Interesse haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke zu übermitteln. Dies soll ausdrücklich auch für die Verarbeitung personenbezogener Daten von Kunden und Beschäftigten gelten.

Externe Dienstleister

Auch externe Dienstleister, wie beispielsweise E-Mailing-Dienste, müssen nach der DSGVO arbeiten. Das muss vom Auftraggeber ggf. geprüft werden.

Auftragsdatenverarbeitung

„Auftragsverarbeiter" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag bzw. auf Weisung des Verantwortlichen bearbeitet (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, ihre Voraussetzungen zu kennen. In der DSGVO werden diese nun erstmals europaweit einheitlich geregelt.

***Dieser Beitrag ist dem Buch EU-Datenschutzgrundverordnung von Holger Mühlbauer mit freundlicher Genehmigung der Beuth Verlag GmbH, Berlin entnommen.**

Holger Mühlbauer

EU-DATENSCHUTZGRUNDVERORDNUNG

Praxiswissen für die Umsetzung im Unternehmen – Schnellübersichten

1. Auflage 2018, 100 Seiten, Beuth Verlag GmbH

ISBN 978-3-410-28353-9

Wer neue IT-Systeme implementiert, sollte Technologien nutzen, die den Schutz personenbezogener Daten in den Vordergrund stellen. Diese Publikation gibt einen praxisgerechten, schnellen Überblick.

Schritt für Schritt zum Datenschutzkonzept

Inklusive Mustervorlagen

HINWEIS

Dieser Überblick fasst die wesentlichen Punkte zur DSGVO für Verbände zusammen – ohne Anspruch auf Vollständigkeit. Bitte beachten Sie, dass daher nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang in dem einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet.

1 DEFINITION PERSONENBEZOGENER DATEN IM VERBAND

- Daten-Kategorien
- Besondere Daten-Kategorien („sensible Daten")

Mustervorlage: bit.ly/dsgvo-01

2 DATENSCHUTZBEAUFTRAGTEN/-VERANTWORTLICHEN BESTIMMEN

- Alle Verbände benötigen einen Datenschutzverantwortlichen
- Verbände mit mind. zehn Personen im Umgang mit personenbezogenen Daten (auch Nichtarbeitnehmer, z. B. ehrenamtliche Mitarbeiter) benötigen einen betrieblichen Datenschutzbeauftragten (DSB)
- Bei regelmäßiger Verarbeitung besonderer Kategorien personenbezogener Daten (z. B. Gesundheitsdaten, Gewerkschaftszugehörigkeit) wird betrieblicher DSB benötigt, u. U. ohne Berücksichtigung der Personenzahl
- Wahl zwischen einem internen/externen DSB

3 KLÄRUNG DER VERARBEITUNGSPROZESSE/-TÄTIGKEITEN UND VERARBEITER

- Mögliche Verarbeitungstätigkeiten im Verband:
  - Mitgliederverwaltung, -kommunikation
  - Website, Online-Medien, Pressearbeit
  - Erteilung Rechtsberatung
  - Durchführung von Veranstaltungen
  - Personalverwaltung etc.
- „Eigentum" und Verarbeitungsebenen beachten:
  - Bundesverband
  - Landesverband
  - Service-GmbH etc.

4 VORLIEGEN VON RECHTSGRUNDLAGE/RECHTMÄSSIGKEIT DER VERARBEITUNGSPROZESSE/-TÄTIGKEITEN

- Einwilligung
- Verträge (Mitgliedschaftsvertrag, Fortbildungsseminarvertrag)
- Berechtigte Interessen (Verbands-/Personensicht)

Download Mustervorlage: bit.ly/dsgvo-02

5 VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN ERSTELLEN

- Name und Kontaktdaten des Verantwortlichen
- Zweck der Verarbeitung
- Kategorien betroffener Personen und personenbezogener Daten
- Kategorien von Empfängern
- Löschfristen
- Technische und organisatorische Maßnahmen

Download Mustervorlage: bit.ly/dsgvo-03

6 TECHNISCHE UND ORGANISATORISCHE MASSNAHMEN ERARBEITEN

Sicherheitskonzept, Löschkonzept und Datenschutz-Folgeabschätzung

- Zugriffsrechte auf Dateien (Passwortschutz, Berechtigungen)
- Verschlüsselungstechnik bei Weitergabe von Daten
- Verfügbarkeitskontrolle (Sicherung von Daten)
- In Zusammenarbeit mit IT-Abteilung
- Regelmäßige Überprüfung auf Aktualität
- Organisatorische Maßnahmen (Personenzugriff)

Download Mustervorlage: bit.ly/dsgvo-04

7 VEREINBARUNGEN/VERTRÄGE MIT AUFTRAGSVERARBEITERN ABSCHLIESSEN

- Bei Weitergabe personenbezogener Daten (über-/untergeordnete Organisationen oder Dienstleister wie z. B. Steuerberater, Lettershops)

Download Mustervorlage: bit.ly/dsgvo-05

8 RICHTLINIEN/VEREINBARUNGEN FÜR HAUPT- UND EHRENAMTLICHE MITARBEITER ABSCHLIESSEN

- Klare Richtlinien/Vereinbarungen für Mitarbeiter bei der Arbeit mit:
  - Laptops
  - Handys/Smartphones
  - Messenger-Diensten (z. B. Whatsapp)

Download Mustervorlage: bit.ly/dsgvo-06

9 TRANSPARENZPFLICHTEN

- Informationspflicht bei Datenerhebung und Datenverarbeitung
- Auskunftspflicht auf Anfrage betroffener Personen

Download Mustervorlage: bit.ly/dsgvo-07

Alle Mustervorlagen finden Sie auch gesammelt unter folgendem Link als ZIP-Datei zum Download.
→ bit.ly/dsgvo-muster

12 DATENSCHUTZVERLETZUNGEN/BUSSGELDER

- Unverzügliche Meldung von Datenpannen an die Aufsichtsbehörden und Betroffenen
- Klare Richtlinien bei Datenpannen für Mitarbeiter

11 DATENSCHUTZERKLÄRUNG ÜBERARBEITEN

- Verantwortlicher
- Verarbeitungszwecke und Rechtsgrundlagen
- Speicherdauer
- Betroffenenrechte

10 BETROFFENENRECHTE WAHREN

- Informations- und Auskunftsrecht
- Berichtigung, Löschung und Einschränkung der Verarbeitung
- Datenübertragbarkeit
- Widerspruch gegen die Verarbeitung
- Automatisierte Einzelentscheidung