Allgemeine Informationen zum Thema Datenschutz

Ab dem 25.05.2018 gilt innerhalb der gesamten Europäischen Union die Datenschutzgrundverordnung (DSGVO). Damit wird das bestehende Datenschutzrecht, wie etwa das aktuelle Bundesdatenschutzgesetz (BDSG), ersetzt. Ziel der DSGVO ist es, innerhalb der EU ein einheitliches Datenschutzrecht für alle Mitgliedstaaten zu schaffen. Am 25. Mai 2018 endet eine zweijährige Übergangsfrist – dann muss die Verordnung umgesetzt sein. Durch sogenannte Öffnungsklauseln können die einzelnen Mitgliedstaatenzusätzlich Ausführungsgesetze erlassen, durch welche die DSGVO konkretisiert wird. Hiervon hat Deutschland Gebrauch gemacht, sodass neben der DSGVO zusätzlich noch ein neues Bundesdatenschutzgesetz (BDSG) gelten wird. Die nachfolgende Darstellung soll Ihnen einen ersten Überblick und Hilfestellungen zu den neuen Regelungen geben. Den Verordnungstext ebenso wie eine Verlinkung auf das neue BDSG finden Sie z.B. unter *https://dsgvogesetz.de*.

Worum geht es bei der DSGVO eigentlich?

Um sich nicht nur über diese bürokratische Auflage zu ärgern, kann es hilfreich sein, sich die Hintergründe und die Intention des Gesetzgebers zu vergegenwärtigen. Neben der Schaffung eines einheitlichen Datenschutzrechts innerhalb der EU, geht es vor allem darum, den Datenschutz auf die aktuellen Entwicklungen zur Globalisierung und der damit einhergehenden Digitalisierung anzupassen und zu modernisieren. Ausgangspunkt ist letztlich der rasante Anstieg des Verkehrs personenbezogener Daten. Viele Unternehmen speichern gewaltige Datenmengen von Personen, die sie auswerten und weiter verkaufen oder intern nutzen, um Profile ihrer Kund/innen oder Mitarbeiter/innen anzulegen. Nicht nur Facebook, dessen Geschäftsmodell auf dem Sammeln und Auswerten von Daten beruht, arbeitet so. Auch viele andere Unternehmen haben erkannt, dass sich mit solchen Daten gezielter werben, verkaufen und beeinflussen lässt. Dagegen heißt es in der DSGVO: „Die Verarbeitung personenbezogener Daten sollte im Dienste der Menschheit stehen. Das Recht auf Schutz der personenbezogenen Daten ist kein uneingeschränktes Recht; es muss im Hinblick auf seine gesellschaftliche Funktion gesehen und unter Wahrung des Verhältnismäßigkeitsprinzips gegen andere Grundrechte abgewogen werden. “ Es geht also um den Schutz aller (unserer) personenbezogenen Daten. Im Zeitalter fast unbegrenzter Speichermöglichkeiten ein begrüßenswerter Anspruch. Man kann also die Regelung als sinnvollen Schutz für uns alle gegen „Datenkraken“ begreifen. Wenn man sich dieser Rechte bewusst ist, kann man auch besser auf ihre Einhaltung bestehen – und natürlich selbst mit gutem Beispiel vorangehen. Mit diesen hehren Zielen vor Augen fällt es schon viel leichter, sich auf die zunächst übertrieben wirkenden Vorgaben und Vorschriften einzulassen.

Datenschutz in der Praxis - Für welche Daten gilt die DSGVO?

Immer wenn sogenannte personenbezogene Daten verarbeitet werden, sind auch die Vorgaben der DSGVO zu beachten. **Personenbezogene Daten** sind alle Informationen, die sich auf eine natürliche Person beziehen, die direkt oder indirekt identifiziert werden kann. Dies sind z.B. Name, Geburtsdatum, Geburtsort, Wohnort, Telefonnummer, Bankdaten, E-Mail- Adresse, Zeugnisse, Ausweisnummern, Eintrittsdatum in den Verein, IPAdressen, Kundendaten wie Bestellungen und Einkaufshistorie – also alle Daten, die eindeutig einer Person zugeordnet werden können und Auskünfte über diese enthalten. Unternehmensdaten sind dagegen nicht durch die Verordnung geschützt (z.B. Umsatzauswertungen von verschiedenen Lieferanten). Sogenannte **besondere personenbezogene Daten** werden noch wesentlich strenger geschützt. Dies sind Angaben zu rassischer oder ethnischer Herkunft, politische oder religiöse Ansichten und Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualität oder etwa auch biometrische Daten.

Beim Datenschutz geht es um jedwede Erhebung, Speicherung oder Verwendung dieser persönlichen Daten, unabhängig davon, ob dies mit oder ohne Hilfe automatisierter Verfahren erfolgt. Das Gesetz spricht hier einheitlich von „**Verarbeitung**“. Es spielt also keine Rolle, ob personenbezogene Daten elektronisch oder nur auf Papier festgehalten sind. Im Unternehmen betrifft dies alle Personen, mit denen das Unternehmen in einem Austausch steht, also Kunden, Lieferanten, Spender, Mitarbeitende und Interessierte.

Gilt die DSGVO auch für Vereine oder einen kleine Betriebe?

Verantwortlich für die Einhaltung der DSGVO ist jede 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 – also auch ein Verein und ein kleiner Betrieb, der z.B. personenbezogene Daten von Mitgliedern, etwa zur Beitragsverwaltung oder Daten von Mitarbeiter/innen im Rahmen der Lohnbuchhaltung verarbeitet. Innerhalb des Vereins ist der Vereinsvorstand und in einem Unternehmen, z.B. einer GmbH, die Geschäftsführung für die Einhaltung datenschutzrechtlicher Vorgaben zuständig.

Wann dürfen personenbezogene Daten verarbeitet werden?

Oberster Grundsatz des Datenschutzrechts ist das Verbotsprinzip: Die Verarbeitung und Speicherung personenbezogener Daten ist verboten – es sei denn, man hat gute Gründe bzw. eine rechtliche Grundlage dafür.

Rechtmäßige Verarbeitung personenbezogener Daten

Als Rechtsgrundlage für eine Datenverarbeitung ist z.B. die **Vertragserfüllung** zu nennen. Auch die Weitergabe von Daten an Dritte zur Erfüllung dieses Zwecks wäre somit abgedeckt. Das bedeutet zum Beispiel:

- Daten der Mitarbeitenden dürfen zum Zwecke der Lohnbuchhaltung verarbeitet werden. Diese und andere wichtige Daten in Personalakten sollten aber sicher aufbewahrt und vor dem Zugriff Dritter geschützt sein.

- Vereine dürfen persönliche Daten zu Spenden, Geburtstagen und Jubiläen veröffentlichen, sofern die Betroffenen dem nicht widersprechen.

- Esn können gesetzliche **Verpflichtungen zur Datenverarbeitung** bestehen, wie sie z.B. aus dem Steuerrecht für die Aufbewahrung von Abrechnungen oder Spendenbescheinigungen (Rechnungen und Spendenbescheinigungen müssen 10 Jahre aufbewahrt werden, geschäftliche Briefe/E-Mails sechs Jahre).

Falls keine derartige Rechtsgrundlage existiert, kann die Datenverarbeitung auf die **Einwilligung** des Betroffenen stützen werden. Dies ist z. B. für die Zusendung eines Werbenewsletters oder die Weitergabe von Daten an Dritte (Sponsoren, Kooperationspartner oder ähnl.) erforderlich. Wichtig ist, dass eine Einwilligung immer freiwillig, informiert und transparent erfolgen muss. Dabei muss die Einwilligung jederzeit widerrufbar sein, worauf ebenfalls hingewiesen werden muss. Die einwilligende Person muss im Zeitpunkt der Einwilligung wissen, wozu sie einwilligt. Auch muss die Einwilligung nachweisbar sein, was bei einem Newsletter z.B. durch ein sog. Double-Opt-In-Verfahren gewährleistet werden kann (das bedeutet, dass der/die Nutzer/in nach der Anmeldung zum E-Mail-Newsletter anschließend noch durch eine Bestätigungsmail die Möglichkeit hat, die Anmeldung zu bestätigen). Per E-Mail versandte Newsletter können auch weiterhin an bereits bestehende Verteiler versandt werden, sofern die ursprüngliche Einwilligung bereits den oben genannten Vorgaben entsprochen haben. In jedem Falle müssen Einwilligungen aber – wie bisher auch schon – einen deutlichen Hinweis auf die Möglichkeit der Abbestellung des Newsletters enthalten.

Wenn Sie Daten von Mitarbeiter/innen, Kund/innen, Lieferanten etc. einholen, die über das hinausgehen, was für die übliche Geschäftstätigkeit, Auftragsabwicklung und Vertragseinhaltung benötigt wird, müssen Sie vorab die schriftliche Einwilligung der betroffenen Personen einholen. Im Umkehrschluss ist die übliche Geschäftstätigkeit nicht einwilligungspflichtig.

Weitere Grundsätze für die Datenverarbeitung

Datenverarbeitung muss immer **transparent**, d.h. nachvollziehbar erfolgen. Dies ist vor allem für die Sicherstellung der Betroffenenrechte wichtig und wird z.B. im Rahmen von Einwilligungen (siehe oben) und Datenschutzerklärung relevant.

Datenverarbeitung muss immer **zweckgebunden** sein und hat sich immer auf das notwendige Maß zu beschränken. Es gilt das Prinzip der Datenminimierung: Sensible Daten sollen in möglichst geringen Mengen erhoben und verarbeitet werden. Folglich ist neu zu prüfen, ob für o. g. Zweck das Geburtsdatum des Kunden notwendig ist.

Daneben gilt der **Grundsatz der Speicherbegrenzung**, d.h. Daten müssen frühes möglich nach dem Wegfall des Zwecks gelöscht bzw. gesperrt werden. Ist also die Notwendigkeit der Verarbeitung zur Zweckerreichung entfallen oder hat die betroffene Person ihre Einwilligung widerrufen und es besteht auch keine sonstige Rechtsgrundlage, sind die betreffenden Daten zu löschen. Die Löschpflicht stellt das sogenannte „Recht auf Vergessenwerden“ der Betroffenen sicher. Generell sind nicht mehr benötigte Daten zu löschen.

Schutz und Integrität: Weiterhin müssen personenbezogene Daten vom Verantwortlichen vor unbefugter und unrechtmäßiger Verarbeitung, Verlust oder Schädigung geschützt werden. Dies kann durch geeignete technische und organisatorische Maßnahmen gewährleistet werden, beispielsweise durch Vorgaben für Passwörter und Verschlüsselung oder eine entsprechende regelmäßige Datensicherung. Im Falle von Datenverlusten (z.B. durch Hacker- Angriffe, Diebstahl eines Datenträgers) müssen die Verantwortlichen im Unternehmen die Aufsichtsbehörde (Das sind die Landesämter/-beauftragten für Datenschutz) und ggf. die Betroffenen informieren. Es bestehen entsprechende Meldepflichten. Die DSGVO sieht zur Vorgabenerfüllung eine sogenannte **Rechenschaftspflicht** beim Verantwortlichen vor. Für Vereine und Unternehmen bedeutet dies, Sie müssen die Einhaltung der DSGVO jederzeit nachweisen können. Dies führt dazu, dass alle datenschutzrechtlich relevanten Vorgänge im Rahmen einer Dokumentation nachweisbar sein sollten.

Was muss getan werden?
Muss man einen Datenschutzbeauftragten bestellen?

Ein Datenschutzbeauftragter muss dann nicht von Gesetzes wegen bestellt werden, wenn weniger als 10 Personen innerhalb der Organisation regelmäßigen Umgang mit personenbezogenen Daten haben. Wenn Sie mehrere Niederlassungen unterhalten, könnte es jedoch grundsätzlich Sinn machen, eine Person zu benennen, die für alle

Datenschutz-Themen verantwortlich sein soll. Diese/r Datenschutzbeauftragte kann dann, evtl. sogar mit einem kleinen Team, die relevanten Prozesse des Unternehmens und die jeweils aktuelle Gesetzeslage im Blick behalten. Durchschnittlich große Betriebe brauchen also in der Regel keinen Datenschutzbeauftragten.

Muss man ein Verzeichnis von Verarbeitungstätigkeiten führen?

Um den Rechenschaftspflichten nachzukommen, müssen Verantwortliche ein sogenanntes „Verzeichnis von Verarbeitungstätigkeiten“ führen. Die DSGVO sieht zwar eine Ausnahme von dieser Verpflichtung für Organisationen/Unternehmen mit weniger als 250 Beschäftigten vor, jedoch soll dies nur dann gelten, wenn die Verarbeitung nur „gelegentlich“ erfolgt oder kein Risiko für die Rechte und Freiheiten von Betroffenen birgt. Sobald die Lohnabrechnung über einen externen Dienstleister oder die Veröffentlichung von Mitarbeiterfotos auf der eigenen Website stattfindet, liegt keine Ausnahme vor – so sieht es zumindest die Datenschutzaufsicht in Bayern und Niedersachsen. Insofern wäre ein Verzeichnis der Verarbeitungstätigkeiten im Unternehmen zu führen, was jedoch einfach und überschaubar gestaltet sein kann. Eine sehr übersichtliche Vorlage für ein Musterverzeichnis, an der man sich gut orientieren kann, stellt z.B. das Bayrische Landesamt für Datenschutz zur Verfügung:
https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf

Muss man Mitarbeiter/innen zur Vertraulichkeit verpflichten?

Bei der Aufnahme ihrer Tätigkeit sollten Beschäftigte, die mit personenbezogenen Daten umgehen, informiert und dahingehend verpflichtet werden, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DSGVO zu erfolgen hat. Ein kostenfreies Muster, das in entsprechende Arbeitsverträge eingefügt werden sollte, stellt z.B. die Gesellschaft für Datenschutz und Datensicherheit zur Verfügung.

Wann sind Daten zu löschen?

Sobald keine gesetzliche Grundlage (z. B. steuerliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese von Gesetzes wegen zu löschen. Bei Mitgliedsdaten in Vereinen wäre dies beispielsweise erst nach deren Ausscheiden der Fall. Bei Mitarbeiter/innen nach Beendigung des Arbeitsverhältnisses, wobei hier noch die Ausschlussfristen im Arbeitsvertrag berücksichtigt werden müssten, also der Zeitpunkt bis zu dem der/die Mitarbeiter/in noch

arbeitsrechtliche Ansprüche vor Gericht geltend machen kann. Nach Abschluss eines Bewerbungsverfahrens müssen die Daten der abgelehnten Bewerber/innen gelöscht werden, sofern es keine schriftliche Einwilligung des/der Bewerber/in gibt. Zu Löschen wären Daten auch dann, wenn ein/e Kund/in oder das Mitglied eines Vereins seine Einwilligung zur Datenverarbeitung widerruft. Dies gilt jedoch – wie bereits dargestellt – nicht, wenn die Datenverarbeitung zur Erfüllung einer anderen rechtlichen Verpflichtung erfolgt. Generell sollten alle Unternehmen darauf achten, dass sie keine unnötigen personenbezogenen Daten schriftlich festhalten oder speichern. Nicht mehr benötigte persönliche Daten müssen gelöscht bzw. vernichtet werden.

Informationen und Auskunftspflichten

Jede/r Verantwortliche muss den betroffenen Personen bereits zum Zeitpunkt der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zur Verfügung stellen. Ein Verein muss beispielsweise Informationen, die Auskunft darüber geben, wie mit erhobenen persönlichen Daten umgegangen wird, auf der Website als „Datenschutzerklärung“ und ggf. auch in der Satzung leicht zugänglich bereithalten. Für die Datenschutzerklärung auf der eigenen Website gibt es diverse Muster und Vorlagen. Es kommt allerdings immer darauf an, welche Dienste man konkret nutzt, so dass es keine einheitliche Standardvorlage geben kann. Einen kostenlosen Generator, der je nach genutzten Diensten eine fertige Datenschutzerklärung generiert, gibt es z.B. hier: *https://dsgvo-muster-datenschutzerklaerung.dg-datenschutz.de*
Je nachdem, welche Funktionen Sie auf der eigenen Website nutzen bzw. damit verknüpfen, müssen Sie Ihre Datenschutzerklärung individuell anpassen. Um alle benötigten Angaben machen zu können, braucht man möglicherweise die Unterstützung durch den Administrator der Website. Die Betroffenen (z.B. Kunden, Vereinsmitglieder, Mitarbeiter/innen) haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten. In einem solchen Fall muss der zum Beispiel ein Verein sicherstellen, dass dieses Auskunftsrecht innerhalb eines Monats bedient werden kann. Es muss unentgeltlich eine Kopie der gespeicherten personenbezogenen Daten bereitgestellt werden. Die Auskunft umfasst die Daten selbst (welche Daten?), die Quelle (woher stammen die Daten?), den Zweck (wozu die Daten gespeichert werden?) und ggf. Angaben zu einem externen Empfänger der Daten (wem werden die Daten weitergegeben?).

Einsatz von Dritten/Auftragsverarbeitern

Sobald Sie Dienstleistungen (z.B. von Gehaltsabrechnungsbüros, IT-Support- Firmen, Hosting-Anbietern, Werbeagenturen, Website-Betreibern, etc.) oder Analyse-

tools (z.B. Google Analytics, Matomo, etc.) in Anspruch nehmen, um personenbezogene Daten in Ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist eine Vereinbarung zur Auftragsverarbeitung erforderlich.

Sanktionen und Strafen

Bei Verstößen gegen die DSGVO können die Aufsichtsbehörden künftig deutlich höhere Bußgelder verhängen. Diese betragen bis zu 20 Mio. Euro oder mehr für größere Unternehmen, doch auch Vereine oder Handwerksunternehmen müssen bei ernsthaften Verstößen mit Bußgeldern in vier- oder fünfstelliger Höhe rechnen. Die Aufsichtsbehörden haben hier bei der Bemessung der Bußgelder einen eigenen Ermessensspielraum. Maßgeblich für eine Bußgeldbemessung sind etwa die Art und Schwere sowie die Dauer des Verstoßes. Aber auch z.B. die Zahl der Betroffenen oder die wirtschaftlichen Folgen. Die hohen Bußgeldrahmen sind dabei vor allem für große Konzerne wie Google, Facebook oder Amazon geschaffen worden und nicht, um Vereine oder kleine und mittelständische Unternehmen in ihrer Existenz zu treffen. Insofern besteht zwar grundsätzlich ein abstraktes Risiko, jedoch ist davon auszugehen, dass die hiesigen Aufsichtsbehörden, wie bisher auch, mit Augenmaß und kooperativ agieren werden und dass Bußgelder nicht ohne weiteres und auch nicht ohne Vorwarnung verhängt werden.

Haftungsausschluss

Die EGT Dreier & Partner darf im Rahmen seiner Tätigkeit keine Rechtsberatung durchführen. Es handelt sich bei dieser Informationsschrift um eine allgemeine Information zum Thema Datenschutz. Wir übernehmen keinerlei Gewähr für die Richtigkeit, Vollständigkeit oder Qualität der zur Verfügung gestellten Informationen und Vorlagen. Wir schließen jegliche Haftung für Schäden materieller oder immaterieller Art aus, die durch die Nutzung der zur Verfügung gestellten Daten oder durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden.