Neues Datenschutzrecht ab 25.05.2018

Auf jeden, der personenbezogene Daten verarbeitet, kommt ab Ende Mai ein deutlich strengeres Datenschutzrecht zu.

Hierzu gibt es bisher keine Erfahrungswerte und wenig hilfreiche Quellen außerhalb des Gesetzestextes. Das Bundesinnenministerium hatte ursprünglich angekündigt, Handreichungen zu schaffen und zu veröffentlichen, um den Weg in die neue Materie zu erleichtern. Dies ist bis heute nicht erfolgt.

In dieser Situation soll der nachfolgende Text einen Einstieg in die zu erwartende Entwicklung bieten. Dies kann nur ein grober Überblick sein, der rechtliche Beratung im Einzelfall nicht ersetzen kann.

1.
Rechtslage:

Am 25.05.2018 wird die EU-Datenschutz-Grundverordnung (kurz DS-GVO) nach einer Übergangsphase wirksam. Sie bildet künftig den maßgeblichen datenschutzrechtlichen Rahmen in allen Mitgliedsstaaten der Europäischen Union.

Nach europäischem Recht handelt es sich dabei um eine Verordnung gemäß Art. 288 Abs. 2 AEUV. Einer derartigen Verordnung im Unionsrecht kommt allgemeine Geltung zu; derartige Verordnungen sind in allen ihren Teilen in der EU verbindlich und gelten unmittelbar in jedem Mitgliedsstaat. Anders als eine Richtlinie setzt die Verordnung damit unmittelbar geltendes Recht, das bereits ohne mitgliedsstaatliche Umsetzungsakte der jeweiligen Länderregierungen schon selbständige Rechte und Pflichten für einen bestimmten Personenkreis begründet.
Bei näherem Hinsehen hat diese europäische Datenschutzgrundverordnung allerdings einen Kompromiss geschaffen mit einer großen Zahl von sog. „Öffnungsklauseln“. So soll zwar im Grundsatz die Vereinheitlichung des Datenschutzrechts innerhalb der EU gewährleistet werden. Daneben gibt aber in einzelnen Bereichen das europäische Gesetz der deutschen Bundesregierung in Teilbereichen noch zulässige Handlungsspielräume.
Auf dieser Grundlage hat der deutsche Gesetzgeber im Juni 2017 ein neues Bundesdatenschutzgesetz erlassen, das zusätzlich zu dieser europäischen Richtlinie ebenfalls ab 25.05.2018 in Kraft ist.

2.
Gilt dies nur für Firmen oder auch Vereine?

Vereine und Verbände unterliegen diesen Bestimmungen ebenfalls. Sie müssen danach den Datenschutz jedenfalls ab 2018 besonders ernst nehmen und bis zum Inkrafttreten der gesetzlichen Bestimmungen sich vorbereitend mit dem Thema sorgfältig befassen.
Nach Art. 5 Abs. 2 DS-GVO muß der Verantwortliche (im Verein der Vorstand) die Einhaltung aller Regelungen nachweisen können. Es ist daher dringend davon abzuraten, zuerst einmal den Kopf in den Sand zu stecken.

3.
Was ändert sich ab 25. Mai 2018?
Die DS-GVO enthält umfangreiche Vorgaben für die rechtskonforme Verarbeitung von Daten, wie beispielsweise Dokumentations- und Nachweispflichten (Art. 30 DS-GVO), Lösch- und Benachrichtigungspflichten (Art. 16, 17), Melde-und Benachrichtigungspflichten bei Datenschutzverletzungen (Art. 33 ff) und die Gewährleistung der gesetzlich vorgeschriebenen Datensicherheit.

Darüberhinaus sind in den Art. 12 ff Informationspflichten vorgesehen mit dem Ziel, dass betroffene Personen vor der erstmaligen Verarbeitung ihrer personenbezogenen Daten unaufgefordert informiert werden.

Neu ist das so bezeichnete „ Recht auf Vergessenwerden“ als besondere Ausprägung der Löschpflichten in Art. 17 DS-GVO.

Ebenfalls neu ist beispielsweise auch ein Schmerzensgeldanspruch für Verbraucher oder aber auch betriebliche Arbeitnehmer im § 83 Abs. 2 Bundesdatenschutzgesetz. So könnte zukünftig eine betroffene Person Schadensersatz verlangen, der wegen eines Datenschutzverstoßes ein materieller oder immaterieller Schaden entstanden ist.

Nach dem neuen Bundesdatenschutzgesetz muss zudem ein Datenschutzbeauftragter bestellt werden, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung **personenbezogener** Daten beschäftigt sind.

Mögliche Sanktionen im Bereich des Datenschutzrechts haben sich auf den ersten Blick deutlich verschärft.

So regelt § 43 des neuen Bundesdatenschutzgesetzes folgendes:
Ordnungswidrig handelt, wer vorsätzlich oder fahrlässig
entgegen der Bestimmung des § 30 ein Auskunftsverlangen nicht richtig behandelt oder entgegen § 30 Abs. 2 Satz 1 einen Verbraucher nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig unterrichtet.
Die Ordnungswidrigkeit kann mit einer Geldbuße bis zu 50.000 € geahndet werden.

Nach § 42 Bundesdatenschutzgesetz könnte eine Geldstrafe oder sogar eine Freiheitsstrafe ausgesprochen werden, wenn wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen ohne Berechtigung einem Dritten übermittelt und hierbei gewerbsmäßig handelt.

In dieser Form ebenfalls neu ist eine generelle Informationspflicht zu Datenverarbeitungen in § 55 des neuen Bundesdatenschutzgesetzes:

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen,
2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung,

3. den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten
4. das Recht, die Bundesbeauftragte oder den Bundesbeauftragten anzurufen, und die Erreichbarkeit der oder des Bundesbeauftragten.

Achtung: Nach Art. 33 der neuen EU-Verordnung muss jeder Datenschutzverstoß in Zukunft innerhalb von maximal 72 Stunden bei der zuständigen Datenschutzbehörde gemeldet werden. (Mögliches Beispiel: es wird ein Vereinslaptop mit vertraulichen Mitgliederdatengestohlen).

4.
Wann ist die Verarbeitung von Daten nach aktuellem Recht ab Mai 2018 zulässig?

Im Datenschutzrecht galt bereits bisher und auch zukünftig das sog. Verbot mit Erlaubnisvorbehalt.

Dieser Rechtsbegriff bedeutet folgendes: Die Datenverarbeitung ist also generell verboten, solange sie nicht durch ein Gesetz ausdrücklich erlaubt ist oder der Betroffene ausdrücklich in die Verarbeitung eingewilligt hat. Dieser Grundsatz bleibt komplett erhalten, auch die EU-Datenschutzgrundverordnung hält an dem Verbot mit Erlaubnisvorbehalt fest.

Art. 6 ,hierzu auszugsweise wie folgt:

Rechtmäßigkeit der Verarbeitung

1. Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
   a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
   b) die Verarbeitung ist die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
   c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
   d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
   e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt,……

Artikel 7, Bedingungen für die Einwilligung:

Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen …..

Erste Frage: Liegt eine nachweisbare Einwilligung vor?
Wenn in früheren Zeiten eine Einwilligung eingeholt wurde, so wird diese den neuen Anforderungen des Datenschutzrechtes ab Mai 2018 im Regelfall nicht mehr genügen, so dass hierfür im Regelfall regelmäßig eine erneute Einwilligungserklärung erforderlich sein wird. Im Übrigen reicht auch nicht aus, eine sog. OPT-OUT-Erklärung (also eine voreingestellte Zustimmung z. B. mit einem voreingestellten Häkchen im Internet- ich stimme zu - dass dann ausdrücklich gelöscht werden müsste).

Wenn keine Einwilligung vorliegt bzw. die Mitgliedschaft schon so lange besteht, dass damals keine förmliche schriftliche Einwilligung eingeholt wurde, ist diese zwingend erforderlich?:

Zulässig kann eine Datenverarbeitung auch ohne schriftliche Einwilligung in Erfüllung eines Vertrags nach Artikel 6 Abs. 1 b) Datenschutzgrundverordnung sein. Danach ist die Verarbeitung personenbezogener Daten für eigene Geschäftszwecke zulässig, wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder Rechtsgeschäft ähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist.

Nach derzeitig überwiegender Meinung fällt unproblematisch unter diesen Vertragsbegriff auch ein durch den Betroffenen begründetes Mitgliedschaftsverhältnis mit einem Verein. Die Nutzung der Daten durch die satzungsmäßig berufenen Organe und sonstigen Funktionsträger erfolgt danach zulässig nach Maßgabe des § 6 Abs. 1 b DS-GVO. Der Vorstand eines Vereins ist dabei in Bezug auf die Verwaltung der Mitgliederdaten als Verantwortlicher zu qualifizieren.

Die Verarbeitung der betroffenen Daten muss aber erforderlich sein.
Aus einem vertragsähnlichen Verhältnis mit mitgliedschaftlicher Prägung heraus ist für den Verein als erforderlich anzunehmen, neben dem Namen seines Vertrags-partners auch eine Lieferanschrift für Schriftverkehr o. ä. zu ermitteln. Es wird dabei auch möglich und zulässig sein, die Bankverbindungsdaten zum Zweck der Zahlungsabwicklung zu erheben, wenn sich insoweit eine akzeptierte satzungs-mäßige Grundlage findet.

Das Kriterium der Erforderlichkeit ist daher sehr wohl zu bedenken und gibt im Übrigen auch Auskunft über die Dauer der zulässigen Datenspeicherung. (Quelle, die EU-Datenschutzgrundverordnung in der anwaltlichen Beratungspraxis, Kazemi, S. 140 f.)

Fraglich wird allerdings in Einzelfällen sein, wie sich das Verhältnis der Vereins-mitglieder untereinander darstellt. Zwar sind diese innerhalb der Vereinsstruktur mitgliedschaftlich organisiert, dennoch werden die Mitglieder, für den Fall, dass sie Einsichtsrechte in die Mitgliedsdaten des Vereins nehmen wollen, datenschutz-rechtlich als Dritte behandelt. Die mitgliedschaftliche Struktur innerhalb des Vereins führt also nicht dazu, dass die Vereinsmitglieder selbst als Teil des Verantwortlichen einzustufen wären. Hier wird wohl abzuwarten sein, wie die Rechtsprechung das neue Gesetz hierzu zukünftig auslegt.

5. Einige Vorschläge für erste Maßnahmen bis zum Inkrafttreten des neuen Datenschutzrechts Ende Mai:

- Vereine und Verbände sollten zunächst einmal die datenschutzrechtlichen Relevanzen und sensiblen Bereiche im eigenen Organisationsbereich ausloten. Dies sind einerseits die Mitgliederdaten und deren Nutzung, andererseits aber auch die Rechtsbeziehung zu Dritten, etwa im Bereich Kommunen als Eigentümer von Sportanlagen oder Sicherungsgesellschaften bzw. Reiseveranstalter im Zusammenhang mit dem Vereinsbetrieb.

- Hat man diese datenschutzrechtlich relevanten Bereiche gefiltert, muss geprüft werden, ob und in welchen Fällen tatsächlich Einwilligungserklärungen etwa der Mitglieder eingeholt werden müssen. Dies kann für bestimmte Standardprozesse bereits beim Eintritt in den Verein geschehen, muss jedenfalls aber weiter laufend überprüft werden. Problematisch ist dabei aber vor allem die Frage, ob auch bereits bei länger vorhandenen Mitgliederstrukturen Handlungsbedarf besteht.

- Bitte prüfen Sie in Ihrem Verband oder Verein, ob **ein Datenschutzbeauftragter** zu bestellen ist.

- Nach dem neuen Recht sind zukünftig nach Art. 30 DS-GVO sogenannte **Verfahrensverzeichnisse** zu erstellen. Verantwortlich ist der Vorstand. Als jeweils ein gesondertes Verfahren gelten beispielsweise Dokumentenmanagementsysteme, Spezialsoftware, Buchhaltungssoftware, elektronische Diktierprogramme, spezielle Software zum Versenden und Verwaltung von emails, Adressdatenbanken, Software zur Terminverwaltung etc.

  Für diese Verzeichnisse ist keine bestimmte Form vorgeschrieben. Enthalten müssen sein:
  Der Name und die Kontaktdaten der Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
  die Zwecke der Datenverarbeitung
  die Art der Personen, deren Daten verarbeitet werden (z. B. Mitglieder, Angehörige, Beschäftigte, Vertragspartner)
  die Art der verarbeiteten Daten
  die möglichen Empfänger der Daten, denen die Daten offengelegt worden sind und offengelegt werden sollen
  die Übermittlung von Daten in die USA oder ein anderes Land außerhalb der EU (z. B. bei cloud-Diensten, möglicherweise auch bereits bei Whatsapp!)
  Löschlisten
  Maßnahmen der Datensicherheit nach Art. 32 DS-GVO

  Achtung: Das Thema Verfahrensverzeichnis ist sehr mühsam. So ist z. B. auch zu bedenken, dass zum Teil ja auch noch Smartphones, Laptops etc. genutzt

werden und insoweit ebenfalls möglicherweise relevante Programme auf den Endgeräten vorhanden sind.

- **Informationspflichten:**
  Betroffene, über die Daten gespeichert werden, müssen in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache „informiert werden“.

- Das neue Gesetz gibt ein „**Recht auf Vergessen** werden“. Danach besteht der Grundsatz, dass nicht mehr benötigte Daten unverzüglich gelöscht werden müssen. Dieser Begriff unverzüglich wird eingeschränkt durch etwa notwendige steuerrechtliche Vorgaben oder ähnliches. Jedenfalls aber sind etwaige notwendige Löschungen (z. B. Ende der Mitgliedschaft und eine gewisse Nachlaufzeit hierzu) zu regeln und zu dokumentieren.

- **Datensicherheit:**
  Artikel 32 europäische Datenschutzgrundverordnung verpflichtet die Datenverarbeiter zur Datensicherheit. Zu den in Betracht kommenden Fragestellungen zählt dabei auch die Überprüfung der zum Schutz des Datengeheimnisses notwendigen technischen und organisatorischen Maßnahmen

  Soweit möglich, sollte z. B. bei personenbezogenen Daten eine Verschlüsselung geprüft werden. Vertraulichkeit und Belastbarkeit der Systeme wird auf Dauer sicherzustellen sein. Bedenken Sie z. B. auch die Möglichkeit verschlüsselter Emails. Befinden sich personenbezogene Daten anderer auf einem Gerät mit Whats app, so können sich allein hieraus datenschutzrechtliche Probleme ergeben. Die Geräte mit personenbezogenen Daten des Vereins sollten ausreichend gesichert sein, dies sollte dokumentiert und überwacht sein. Vom Verein mit Datenverarbeitung beauftragte Dritte oder auch Mitglieder sind ebenso wie sonstige Funktionsträger des Vereins streng (und nachweisbar) auf das Datengeheimnis zu verpflichten. Dies scheint vor allem bei kleineren Vereinen notwendig, um die Vereinsdaten etwa bei Einsatz privater Computer effektiv zu schützen.

  Bitte bedenken Sie, dass gerade auch die vereinseigene Homepage ein erhebliches Gefährdungspotential für Schadensersatzansprüche oder sogar Geldbußen beinhaltet. Das Impressum mit Belehrung sollte geprüft werden, ebenso ist z. B. zu prüfen, ob Cookies o.ä. verwendet werden und hierüber zukünftig ordnungsgemäß informiert wird. Kann das Mitglied über die Homepage Kontakt aufnehmen, ist anzuraten, diesen Weg zu verschlüsseln.

- Die eigenen Bemühungen sollten möglichst sorgfältig dokumentiert werden, da Dokumentationspflichten in dem neuen Datenschutzrecht sehr groß geschrieben sind. Insgesamt sind die Informationspflichten nach dem neuen Datenschutzrecht wesentlich umfangreicher, ebenso die Nachweispflichten. So muss der Verantwortliche die Einhaltung aller Regelungen nachweisen können!

Zu betonen ist, dass die obigen Ausführungen zunächst lediglich als erster Überblick über die auf uns zukommende Situation dienen können. Das bisherige deutsche Datenschutzrecht wird nicht nur materiell geändert, sondern wird zusätzlich geprägt durch ein noch komplizierteres Regelungsgeflecht. Bis der Umfang der Neuerungen für alle Anwender rechtssicher bestimmt ist, werden wohl noch Jahre vergehen. Leider haben der Gesetzgeber und insbesondere auch das Bundesinnenministerium es bisher nicht geschafft, geeignete Handreichungen für die anstehenden Probleme zur Verfügung zu stellen.

Die obigen Darlegungen sind daher lediglich als vorläufige Einführung zum Stand Januar 2018 zu betrachten. Sie sind rechtlich unverbindlich und stellen keine Rechtsberatung im Einzelfall dar.

Rechtsanwältin Kiera, Justitiarin des Deutschen Angelfischerverbands
Stand 10.01.2018