1. Definition – Um was handelt es sich bei der Datenschutzgrundverordnung?

Die Datenschutzgrundverordnung (DSGVO) ist in der Zusammenfassung die Neuregelung der Datenschutzgesetze durch die EU. Sie trat am 24.05.2016 in Kraft und wird ab dem 25.5.2018 unmittelbar Anwendung finden. Bislang sind diese Gesetze EU-weit uneinheitlich gewesen, und die DSGVO wurde geschaffen, um sie zu vereinheitlichen und zu verbessern.

Viele Betreiber von Websites, sei es im Handel, im Service oder im **Verein**, blicken der verbindlichen EU-DSGVO mit Sorge entgegen, da sie viele schwer verständliche Neuregelungen befürchten. Dabei sind die neuen Regeln erstens nicht so zahlreich wie gedacht (viele von ihnen bestehen bereits im Bundesdatenschutzgesetz, dem BDSG) und zweitens gut verständlich formuliert. Die Herausforderung liegt in der praktischen und technischen Umsetzung der DSGVO 2018, die 99 Artikel umfasst.

1.1 EU Vorgaben für die DSGVO

Das Hauptanliegen der EU ist es, dem Verbraucher eine größere Kontrolle über die Verwendung seiner Daten einzuräumen. Zwar sind diverse Missstände im Laufe der Jahre sukzessive behoben worden, doch die neue Verordnung soll diesen Prozess umfassend auf ein höheres Niveau heben. Wer ab Mai 2018 persönliche Daten erheben, speichern und verwenden möchte, muss dafür eine ganze Reihe von Regeln befolgen. Die Zuwiderhandlung kann mit empfindlichen Bußgeldern geahndet werden.

1.2 Technische und organisatorische Maßnahmen

In jedem Umfeld, in dem persönliche Daten erhoben werden, müssen technische und organisatorische Maßnahmen die DSGVO möglich machen. Das bedeutet vor allem, dass die Personen, um deren Daten es geht,

- ihre Zustimmung geben müssen
- Widerspruch einlegen können
- Einsicht in die Daten verlangen können
- den Verwendungszeck erfragen können
- die Daten berichtigen oder unter Umständen sperren lassen können

Wer die Möglichkeiten dafür noch nicht auf seiner Website eingerichtet hat, muss dieses Versäumnis bis zum 25. Mai 2018 nachholen.

2. Die gesetzlichen Rahmenbedingungen der DSGVO

Wie der Name „Datenschutz*grundverordnung*“ bereits andeutet, handelt es sich bei der DSGVO nicht um das unverrückbare Ende der Datenschutzregeln. Zwar stehen die Regelungen, die die EU beschlossen hat, über der Gesetzgebung aller Mitgliedsstaaten und müssen daher beim Entwurf neuer Gesetze berücksichtigt werden. Allerdings ist die DSGVO kein Gesetz an sich.

2.1 Öffnungsklauseln

Durch die über 70 Öffnungsklauseln der DSGVO erlaubt die EU den einzelnen Mitgliedsstaaten, die Grundverordnung in ihren eigenen Gesetzen zu ergänzen und zu konkretisieren, aber auch zu modifizieren. Letzteres ist in solchen Fällen erlaubt, in denen laut staatlichem Gesetz die Verantwortlichen (Vereine, Unternehmen) anderslautende rechtliche Verpflichtungen haben. Das bedeutet für Deutschland, dass die Regelungen des Bundesdatenschutzgesetzes von der DSGVO nicht außer Kraft gesetzt werden. Gegenteilig wurden sie überarbeitet und ergänzen die DSGVO nun.

2.2 Art. 28 – Die Auftragsverarbeiter-Klausel

Vor allem größere Vereine setzen häufig externe Dienstleister ein, die beispielsweise den **Newsletter** versenden. Mit ihnen müssen Sie eine Vereinbarung über die Auftragsdatenverarbeitung abschließen. Diese bindet dem Dienstleister die Hände hinsichtlich der erhaltenen Daten – er verpflichtet sich, sie nicht anders als für den angegebenen Zweck zu verwenden. Darüber hinaus müssen die Mitglieder oder Interessenten darüber aufgeklärt werden, dass ihre Daten an den entsprechenden Dienstleister weitergeleitet werden. Auch die Benachrichtigung beim Wechsel des Auftragsverarbeiters ist in Art. 28 DSGVO geregelt. Die genaue Beschreibung der Verwendung ist ebenfalls verbindlich.

3. Die Rolle des Datenschutzbeauftragten

Wann genau ein Datenschutzbeauftragter bestellt werden muss, ist nach der entsprechenden Öffnungsklausel für Deutschland im neuen BDSG festgelegt worden: § 38 besagt, dass ein Datenschutzbeauftragter immer dann notwendig wird, wenn sich mehr als neun Personen im Verein immer mit der automatisierten Verarbeitung der personenbezogenen Daten der Mitglieder beschäftigen.

Ob es sich um einen internen oder einen externen **Datenschutzbeauftragten** handelt, bleibt dem jeweiligen **Verein** oder Unternehmen überlassen. Wichtig ist, dass er sich mit der Materie gut auskennt und selbstständig stets auf dem neuesten Stand bleibt, um jederzeit auf Änderungen und Weiterentwicklungen reagieren zu können. Er muss der zuständigen Aufsichtsbehörde gemeldet werden; das wird in Artikel 37 Absatz 8 der DSGVO festgelegt.

Im neu ausdefinierten **Datenschutz** besagt die Grundverordnung, dass der Datenschutzbeauftragte

- mit der Aufsichtsbehörde zusammenarbeitet
- die Verantwortlichen berät
- die Mitarbeiter, die Daten verarbeiten, schult und sensibilisiert
- dafür Sorge trägt, dass die DSGVO eingehalten wird
- für die Dokumentation der Maßnahmen rund um die Datenerhebung und -verarbeitung sorgt

Bereiten Sie Ihren Verein auf das neue Datenschutzrecht 2018 vor und vermeiden Sie teure Bußgelder!

3.1 Wie ist die Haftung nach der DSGVO geregelt?

Entsteht einer Person ein Schaden immaterieller oder materieller Natur durch den Verstoß eines Vereins oder Unternehmens gegen die Regeln der DSGVO, hat sie Anspruch auf Schadenersatz. Der Verantwortliche ist zunächst einmal der Verein/das Unternehmen selbst oder der engagierte Auftragsverarbeiter. Letzteres trifft aber nur zu, wenn der Dienstleister den rechtmäßigen Anweisungen des Auftraggebers nicht Folge geleistet oder im Rahmen seiner Arbeit die Pflichten aus der DSGVO nicht erfüllt hat.

Ist der Schaden, der zum Schadenersatz führt, auf eine mangelhafte Beratung zurückzuführen, geht die **Haftung** auf den Datenschutzbeauftragten laut DSGVO über: „Jeder an einer Verarbeitung beteiligte Verantwortliche haftet für den Schaden, der durch eine nicht dieser Verordnung entsprechende Verarbeitung verursacht wurde“, heißt es in Art. 2, Abs. 2. In kleineren Organisationen ohne Berater haftet also das Unternehmen oder der Verein. Wurde allerdings ein Datenschutzbeauftragter bestellt, der durch fehlende Akkuratesse in seinem Job den Schaden verursacht hat, ist er der Verantwortliche.

4. Welche Bedeutung und Implikationen hat der DSGVO für Vereine?

Vereine sollten vor dem 25. Mai 2018 alle Prozesse, die auf ihrer Website und in ihrer EDV-Abteilung mit den persönlichen Daten ihrer Mitglieder, Mitarbeiter oder Interessenten zu tun haben, genau überprüfen. Für die legale Erhebung und Verarbeitung der Daten ist es nötig, dass

- die betreffenden Personen aktiv ihre Einwilligung geben
- die Daten samt Verarbeitung notwendig sind zum Abschluss eines Vertrags
- die Daten samt Verarbeitung Voraussetzung sind, **damit der Verein eine rechtliche Pflicht erfüllen kann**

- die Daten samt Verarbeitung berechtigte Interessen des Vereins wahren, wenn nicht die Interessen der betroffenen Person überwiegen

Gerade letzterer Punkt erfordert Interpretation und Fingerspitzengefühl. Im Zweifelsfall ist es im Einklang mit der DSGVO für Vereine immer besser, weniger Daten preiszugeben als zu viele.

5. Diese Neuerungen treten 2018 in Kraft

Jedes Mitglied hat das **Recht, über die Sammlung und Verwendung der Daten** informiert zu werden. Ein aktives Einverständnis ist zwingend erforderlich.

Jedes Mitglied hat das **Recht auf das Vergessenwerden**. Das bedeutet, dass Sie nach Ende der Mitgliedschaft alle Daten löschen und einem eventuellen Auftragsverarbeiter sowie Ihrem Dachverband und allen weiteren Stellen Bescheid geben müssen, dass auch sie die Daten löschen.

Sie müssen allen Mitgliedern das **Recht auf den Zugriff auf die eigenen Daten** und deren Verwendungszweck gewähren. Das funktioniert online in passwortgeschützten Bereichen oder auf elektronischem Wege.

Jedes Mitglied hat das **Recht, die Daten übertragen zu bekommen**. Integrieren Sie einen Weg, wie Sie angeforderte Daten sicher und maschinenlesbar übertragen können.

Jedes Mitglied hat das **Recht auf eine Berichtigung inkorrekter Daten**. Sind Daten fehlerhaft oder veraltet oder hat das Mitglied einen Einspruch eingelegt, müssen Sie unverzüglich die nötige Anpassung vornehmen.

Jedes Mitglied kann die **Einschränkung der Nutzung seiner Daten** fordern. Das bedeutet, dass Sie sie zwar abspeichern, aber nicht verwenden dürfen.

Jedes Mitglied kann von seinem **Einspruchsrecht gegen die Verwendung seiner Daten für das Direktmarketing** Gebrauch machen. Lehnt ein Mitglied das direkte Marketing ab, dürfen Sie die Daten dafür nicht mehr verwenden.

Bei einer Gefährdung der Datensicherheit haben die Mitglieder das **Recht, innerhalb von 72 Stunden benachrichtigt zu werden**. Dafür müssen Sie Prozesse einrichten, um Probleme in der Datensicherheit sofort zu erkennen und die Betroffenen innerhalb der Frist zu benachrichtigen.

6. DSGVO Checkliste

- Richten Sie ein Opt-in-Verfahren oder ein Double-Opt-in-Verfahren ein, mit dem die Mitglieder der Datennutzung aktiv zustimmen können. Das Opt-out-Verfahren, bei dem die Mitglieder das Häkchen bei der Zustimmung entfernen müssen, ist nicht mehr zulässig.

- Informieren Sie Ihre **Mitglieder** und Interessenten darüber, welche Daten Sie zu welchem Zweck erheben, wie Sie sie nutzen werden und wer sie verarbeitet (der Verein selbst oder ein Dienstleister).

- Dokumentieren und speichern Sie sorgfältig die Informations- und Zustimmungsverfahren.

- Sorgen Sie dafür, dass Daten gegebenenfalls sowohl in Ihrem EDV-System als auch in denen von Dienstleistern oder Dachverbänden zeitnah gelöscht werden können.

- Sie stellen Ihren Mitgliedern die eigenen Daten samt Verwendungszweck elektronisch zur Verfügung oder richten online einen Bereich ein, in dem sie ihre Daten einsehen können. Für Letzteres müssen die Bereiche passwortgeschützt sein, damit jeder nur seine eigenen Daten zu sehen bekommt.

- Auf Wunsch senden Sie die Daten auf elektronischem Wege, wofür Sie sicherstellen müssen, dass tatsächlich nur die Person die Daten erhält, die darauf ein Anrecht hat.

- Sie stellen eine sofortige Berichtigung fehlerhafter Daten in Ihrem EDV-System und an allen anderen Speicherstellen sicher.

- Sie sorgen dafür, dass ohne Zeitverzögerung die Datennutzungseinschränkungen und die Einwände gegen die Nutzung gegen das Direktmarketing umgesetzt werden.

- Verstärken Sie die Sicherheitsvorkehrungen für die persönlichen Daten Ihrer Mitglieder, Mitarbeiter und Interessenten, wenn sie nicht auf dem neuesten Stand sind.

- Kommt es trotzdem zu einer Offenlegung, einer versehentlichen Löschung oder einer Veränderung der Daten oder hatte jemand Unbefugtes Zugang dazu, müssen Sie die Risiken für die betroffenen Personen abschätzen: Wie groß ist die Wahrscheinlichkeit, dass sie finanziellen Schaden erleiden oder diskriminiert werden? Wie wahrscheinlich ist ein Identitätsdiebstahl? Bei einem hohen Risiko informieren Sie die betroffenen Personen innerhalb von 72 Stunden und dokumentieren Sie alle Schritte, die Sie zur Schadensbegrenzung und zur Risikobewertung vorgenommen haben.

7. Die DSGVO auf den Punkt gebracht

Tatsächlich bringt die DSGVO Neuerungen mit sich, die bei vielen Vereinen die Überarbeitung der Website nötig machen. Allerdings ist auch den Vereinen damit geholfen: Bessere Sicherheitssysteme gegen Datendiebstahl sorgen dafür, dass es gar nicht erst zu Problemen kommt.

Auch bringen die vereinheitlichten Regelungen nicht nur Komplikationen für Vereine und Unternehmen mit sich, sondern auch Vereinfachungen, etwa im Hinblick auf die vereinfachte Einwilligung, die nicht mehr nur schriftlich erfolgen darf. Die Datenschutzgrundverordnung ist aber vor allem dazu gedacht, auf einem globalen Markt die Interessen von Einzelpersonen bestmöglich zu schützen und international anzugleichen.