Wegweiser zur Umsetzung der EU-Datenschutzgrundverordnung im Verein

Am 25.5.2018 tritt die neue EU-Datenschutzgrundverordnung in Kraft und bringt auch für Vereine eine Vielzahl an neuen und teilweise verschärften Regularien zum Schutz personenbezogener Daten. Einhergehend mit den verschärften Regelungen zum Datenschutz wird sich auch der mögliche Bußgeldrahmen deutlich erhöhen. Für die Vereinsvertreter ist die Umsetzung der Datenschutz-Maßnahmen im Verein bis zum 25.5.2018 ein großer Berg an Aufgaben. Aufgrund dessen bieten wir Vereinen im Folgenden einen möglichen Weg zur ersten Umsetzung als Hilfestellung:

	Umsetzungsschritt	*Erläuterung und Arbeitsmaterialien*
1	**Klärung der Zuständigkeiten und Informationsbeschaffung**	• Machen Sie die neue DSGVO und deren Umsetzung in Ihrem Verein zu einem wichtigen Vorstandsthema. • Benennen Sie einen oder mehrere Vorstandsmitglieder die sich mit dem Thema Datenschutz bzw. der Umsetzung der DSGVO beschäftigen. Grundsätzlich ist der gesamte nach § 26 BGB vertretungsberechtigte Vorstand verantwortlich bzw. zuständig. • Berufen Sie eine Arbeitsgruppe aus den Verantwortlichen im Vorstand sowie weiteren Vereinsmitgliedern die mit der Erhebung und Verarbeitung von Daten in Ihrem Verein in Berührung kommen ein. Die Arbeitsgruppe sollte sich der Umsetzung und der Einrichtung der Kontrolle der späteren Einhaltung der DSGVO im Verein annehmen *(Tipp: Lassen Sie die Verantwortung und die Umsetzungsarbeit nicht auf einer einzigen Person liegen!)* • Informieren Sie und die Arbeitsgruppe sich über die neuen Anforderungen der DSGVO und des neuen (ebenfalls ab dem 25.05.2018 geltenden) Bundesdatenschutzgesetzes. Informationen finden Sie hier: - https://www.lsvs.de/index.php?id=2072 - https://www.dsgvo-gesetz.de/ • [illegible] diesem Thema • Haben Sie bereits einen Datenschutzbeauftragten? → Beziehen Sie diesen in die Arbeitsgruppe mit ein! • *Tipp: Legen Sie sich gleich einen Ordner zum Thema Datenschutz an.*

2	**Bestandsaufnahme und Kategorisierung**	• Erfassen Sie kritisch alle Stellen im Verein, an denen personenbezogene Daten[1] erhoben[2] werden sowie welche Daten das sind und zu welchem Zweck diese erhoben werden. Danach erfassen Sie genauso kritisch alle Abläufe in Ihrem Verein, bei denen die personenbezogene Daten verarbeitet werden, insbesondere wo diese gespeichert sind und wie die personenbezogenen Daten wozu verwendet werden. *Tipp: Diese Auflistung dient als Grundlage für alle weiteren Schritte. Halten Sie sich möglichst konkret und lassen Sie nichts aus, dann ist die halbe Arbeit für später schon erledigt.* • Stellen Sie sich dabei auch folgende Fragen: - Werden Daten an Dritte übergeben oder von Dritten verarbeitet (z.B. Mitgliederverwaltung in der Cloud; Kontaktformular auf der Webseite, etc.) - Wozu werden die personenbezogenen Daten weitergegeben? • Lassen Sie dabei möglichst keinen Gedanken aus: Zum Beispiel gehören auch WhatsApp Gruppen, offene E-Mailverteiler, o.Ä. dazu! • Halten Sie diese Auflistung nach deren Erstellung stets aktuell und prüfen Sie die Aktualität regelmäßig. • Arbeitsmaterial: Nutzen Sie hierzu unsere Vorlage, um Ihre Auflistung in Tabellenform zu erfassen.
3	**Datenorganisation**	• Hinterfragen Sie kritisch - im Hinblick auf den Grundsatz der Datenminimierung (Art. 5 Abs. 1c DSGVO) - welche Daten, die Sie bisher erheben oder planen zu erheben, wirklich benötigen. • Löschen Sie nicht mehr benötigte Daten, somit müssen Sie diese zukünftig nicht mehr in Ihren Betrachtungen (z.B. bzgl. der Informationspflichten, etc.) mit einbeziehen • Zentralisieren Sie möglichst alle personenbezogenen Daten auf wenige Personen und (Aufbewahrungs-)orte.
4	**Einordnung der Rechtsgrundlage**	• Personenbezogene Daten dürfen nur verarbeitet werden, wenn eine Rechtsgrundlage dafür gegeben ist. Lesen Sie sich deshalb in die Rechtsgrundlagen zur Verarbeitung personenbezogener Daten (insb. Art. 6 Abs.1 DSGVO) sowie die formalen Anforderungen an eine Einwilligungserklärung (Art. 4 Nr. 11, 7 Abs. 2 DSGVO) ein. • Ordnen Sie daraufhin allen in Punkt 2 erfassten Abläufen und Datenverarbeitungen/-erhebungen die entsprechende Rechtsgrundlage zu. Fehlt es bei einer der Datenerhebungen oder –Verarbeitung an einer dies erlaubenden Rechtsgrundlage, muss die entsprechende Verarbeitung unterbleiben oder aber eine Einwilligung der betroffenen Personen eingeholt werden.
5	**Satzung und Datenschutzordnung**	• In der Satzung und einer diese aufgrund einer entsprechenden Satzungsregelung ergänzenden Datenschutzordnung können die grundlegenden Regeln für die Datenverarbeitung im Verein festgelegt werden (z.B. wer im Verein gegebenenfalls als einziger welche Daten für was wie verarbeiten darf). • Keinesfalls können aber eine Regelung in der Satzung oder der Datenschutzordnung eine erforderliche Einwilligung der betroffenen Person ersetzen oder für sich alleine die sonstigen Anforderungen der DSGVO erfüllen.
6	**Prüfung der eigenen technischen Maßnahmen der Datensicherheit**	• Dokumentieren Sie, wer mit welchen technischen Mitteln und Möglichkeiten und welchen Berechtigungen, personenbezogene Daten verarbeitet (auf PC-Systeme des Vereins, im Programm der Mitgliederverwaltung, auf E-Mailadressen, Internetseite des Vereins etc.) • Prüfen Sie, ob bei den zuvor dokumentierten automatisierten

[1] Nach Art. 4 Abs. 1 DSGVO bezeichnet „personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; 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;“ → **Dies bedeutet, dass die DSGVO immer dann zur Anwendung kommt, wenn es sich um Daten handelt die eine lebende, natürliche Person - sprich einen Mensch - in irgendeiner Art und Weise identifizierbar machen.**

[2] Nach Art. 4. Abs. 2 DSGVO bezeichnet „jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im 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; → **Dies bedeutet, dass unter den Begriff „Verarbeitung“ jeglicher Umgang mit den Daten fällt.**

		Verarbeitungen unter Berücksichtigung des Stands der Technik, der Kosten der Einführung und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen ein angemessenes Schutzniveau gegeben ist. Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch - unbeabsichtigte oder unrechtmäßige Vernichtung, Verlust, Veränderung personenbezogener Daten - unbefugte Offenlegung von personenbezogenen Daten - unbefugten Zugang zu personenbezogenen Daten die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden. • Prüfen Sie, wenn möglich, bei Anschaffung neuer Software- oder Hardwaresysteme, dass der Anbieter die Anforderungen der DSGVO in seinem Produkt umgesetzt hat. Lassen Sie sich dies ggf. schriftlich bestätigen.
7	**Prüfen und Abschließen von Verträgen mit Auftragsverarbeitern**	• Prüfen Sie, ob und in welchen Fällen Sie personenbezogene Daten von Personen oder Unternehmen außerhalb Ihres Vereins in Ihrem Auftrag verarbeiten (z.B. Hosting der Vereinshomepage auf der Mitgliederdaten veröffentlicht werden oder Mitgliederverwaltung in der Cloud, etc.) und fassen Sie sich die Ergebnisse ebenfalls in einer einfachen Auflistung zusammen. • Arbeitsmaterial: Vorlage „Übersicht Auftragsdatenverarbeitungs-Verträge“: • Arbeitsmaterial: „Mustervertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO“ • Prüfen Sie zudem, ob Sie mit Unternehmen in einem Drittland – d.h. außerhalb der EU - entsprechende Vertragsbeziehungen haben (z.B. mit dropbox inc. mit Sitz in San Francisco, USA). Hier sind weitere strenge rechtliche Regelungen zu beachten. • Schließen Sie mit jedem dieser Unternehmen einen entsprechenden Vertrag zur Auftragsdatenverarbeitung ab, oder aktualisieren Sie bestehende Verträge. Die Anforderungen an die Inhalte solcher Verträge finden Sie in Art. 28 Abs. 3 DSGVO. *Tipp: In der Regel haben diese Unternehmen bereits Vorlagen für entsprechende Verträge, die sie Ihnen auf Anfrage zukommen lassen.* • Dokumentieren Sie Ihre Abstimmungen und Absprachen mit den Unternehmen stets schriftlich und sortieren Sie diese ebenfalls in Ihren Ordner Datenschutz ein.
8	**Information bei der Erhebung personenbezogener Daten**	• Eine wesentliche Neuerung im Datenschutz, die mit der DSGVO umgesetzt wird, sind die umfassenderen Informationspflichten. Sie als Verein müssen den Personen, deren personenbezogene Daten Sie erheben, bereits „zum Zeitpunkt der Erhebung dieser Daten“ eine Reihe an Informationen übermitteln. Diese mitzuteilenden Informationen finden Sie detailliert aufgeführt in Art. 13 DSGVO. • Überprüfen Sie, ob Sie bei jeder Datenerhebung (z.B. auf dem Aufnahmeantrag, bei Online-Formularen auf Ihrer Vereins-Webseite, etc.) die betreffende Person, deren Daten Sie erheben, zum Zeitpunkt der Erhebung entsprechend informieren. • Diese Informationspflicht gilt gegenüber allen Personen, deren personenbezogenen Daten Sie ab dem 25.05.2018 erheben. • Die textliche Gestaltung der zu übermittelnden Informationen können Sie dem folgenden Arbeitsmaterial entnehmen. • Arbeitsmaterial: Mustertexte für z.B. ein Aufnahmeformular: „Datenschutzrechtliche Informationen zur Verwendung der von Ihnen angegebenen Daten“.
9	**Überprüfung Aufnahmeantrag mit Einwilligungserklärung sowie ggf. nachträgliche Einholung fehlender**	• Prüfen Sie, anhand der unter Punkt 4 erstellen Auflistung und Einordnung der Rechtsgrundlage, für welche Verarbeitung personenbezogener Daten Sie keine andere Rechtsgrundlage für die

	Einwilligungen	Verarbeitung haben und deshalb die Einwilligung der entsprechenden Mitglieder bzw. Personen benötigen. • Erstellen Sie darauf aufbauend entsprechende Einwilligungserklärungen (zum Beispiel auf dem Aufnahmeantrag). Die Anforderungen, wie eine Einwilligungserklärung formuliert sein muss und welche Inhalte diese umfassen muss, ist in Art. 4 Nr. 11, 7 Abs. 2 DSGVO detailliert aufgeführt. • Prüfen Sie zudem, ob die von Ihnen gegebenenfalls bereits vor dem 25.05.2018 eingeholten Einwilligungen zur Datenverarbeitung in Form und Inhalt bereits den verschärften Informationspflichten der DSGVO genügen. Ist dies nicht der Fall, müssen Sie sich eine neue Einwilligung anhand der neuen Vorlage einholen. • Beachten Sie bei der Verarbeitung personenbezogener Daten von Kindern die besonderen Anforderungen, insbesondere nach Art. 8 DSGVO. Wird das Kind volljährig, muss dies erneut selbst eine Einwilligung erteilen. • Stellen Sie sicher, dass ein Widerruf der Einwilligung genau so einfach zu erklären ist, wie die Einwilligung selbst (z.B. via Formular oder Bekanntmachung an wen ein Widerruf zu richten ist) • Ordnen Sie die entsprechenden Einwilligungserklärungen zur Nachweispflicht und zum schnellen Auffinden ein, z.B. in Ihren Ordner Datenschutz oder zu den entsprechenden Mitgliedsanträgen. • Arbeitsmaterial: Mustertexte für z.B. ein Aufnahmeformular: „Datenschutzrechtliche Informationen zur Verwendung der von Ihnen angegebenen Daten“.
10	**Erstellung des Verfahrensverzeichnisses**	• Nach Art. 30 DSGVO sind Sie dazu verpflichtet ein Verzeichnis aller Verarbeitungstätigkeiten zu führen. Art. 30 Abs. 5 DSGVO enthält zwar die Ausnahme, dass dies nur auf Unternehmen mit mehr als 250 beschäftigten Mitarbeiter zutrifft, jedoch nur bei gelegentlicher Verarbeitung. Ob das bei Ihnen gegeben ist, müssen Sie prüfen. In vielen Vereinen dürfte eine regelmäßige und nicht nur gelegentliche Datenverarbeitung stattfindet. • Art. 30 gibt vor, welche Angaben in den Verfahrensverzeichnissen enthalten sein müssen. • Als Basis zur Erstellung dieses Verzeichnisses dient hierbei wiederum Ihre gute Vorarbeit im Rahmen der Bestandsaufnahme. Ziehen Sie die von Ihnen gesammelten Datennutzungen heran und führen Sie diese in das Verzeichnis von Verarbeitungstätigkeiten über. Ggf. müssen Sie hier einige wenige Punkte noch ergänzen. • Arbeitsmaterial: Muster „Verzeichnis von Verarbeitungstätigkeiten“.
11	**Datenschutz-Folgeabschätzung**	• Prüfen Sie, ob eine in Ihrem Verein eingesetzte Form der Datenverarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für personenbezogene Daten zur Folge hat. Dokumentieren Sie das Ergebnis und die Gründe dafür. • Bezüglich der Formen der Datenverarbeitung, bei denen Sie ein hohes Risiko feststellen, müssen Sie vor der ersten Verarbeitung in dieser Form eine Abschätzung der möglichen Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durchführen. Sofern Ihr Verein einen Datenschutzbeauftragten hat, haben Sie bei der Durchführung einer Datenschutz-Folgenabschätzung dessen Rat einzuholen. • Die von Ihnen zu dokumentierende Folgenabschätzung enthält zumindest Folgendes: a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen; b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck; c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

		d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen.
12	**Benennung eines Datenschutzbeauftragten**	• Der Verein muss einen Datenschutzbeauftragen benennen, sobald im Verein „in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt“ sind. (§ 38 Abs. 1 BDSG-neu) • Außerdem ist - unabhängig von der Zahl der mit der automatisierten Verarbeitung beschäftigten Personen - von Ihrem Verein ein Datenschutzbeauftragter zu bestellen, wenn Ihr Verein Verarbeitungen vornimmt, die einer (oben dargestellten) Datenschutz-Folgenabschätzung unterliegen. • Stellung und Aufgaben des Datenschutzbeauftragten ergeben sich aus Art. 38 und 39 DSGVO und wurden verschärft. • Melden Sie die Kontaktdaten des von Ihrem Verein benannten Datenschutzbeauftragten an die zuständige Aufsichtsbehörde (nach Art. 37 Abs. 8 DSGVO). [Das ist in S-H das unabhängige Landes-zentrum für Datenschutz in Schleswig-Holstein • Der Datenschutzbeauftragte darf nicht Mitglied des vertretungsberechtigten Vorstands sein.
13	**Bestimmung von Verantwortlichen und Erstellung von (Melde-) Abläufen**	• Beschreiben Sie Ihr mögliches Vorgehen zur Umsetzung bzw. Reaktion auf die Geltendmachung der Betroffenenrechte (nach Art. 15 bis 22 DSGVO) sowie die entsprechenden Verantwortlichkeiten bzw. handelnden Personen, sodass Sie ad hoc und schnell reagieren können (z.B. wer in sozialen Medien oder auf der Vereinshomepage schnell ein Foto oder Personendaten entfernen kann, etc.) • Beschreiben Sie zudem den Ablauf und die Verantwortlichkeiten, die ggf. auftretende Datenschutzverletzungen an die zuständige Aufsichtsbehörde (und die von der Verletzung betroffenen Personen meldet. *Hinweis: Beachten Sie, dass nach Art. 33 Abs. 1 DSGVO nun auch für Vereine die Pflicht besteht, eine „Verletzung des Schutzes personenbezogener Daten ... unverzüglich und möglichst binnen 72 Stunden, nachdem ... die Verletzung bekannt wurde, der ... zuständigen Aufsichtsbehörde“ zu melden. Nach Art. 34 DSGVO ist auch der Betroffene über die Datenschutzverletzung zu informieren. Diese Pflichten bestehen nur dann nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten des Betroffenen führt.*
14	**Dokumentation**	• Machen Sie sich bewusst, dass Sie über alle vorgenannten Anforderungen schriftlich Dokumente vorhalten sollten. Denn ab dem 25.05.2018 hat Ihr Verein im Streitfall nachzuweisen, dass er die datenschutzrechtlichen Anforderungen erfüllt hat. • Bewahren Sie deshalb alle Ihre zusammengestellten Dokumente, Auflistungen, Notizen und Dokumentationen möglichst zentral, schnell auffindbar an einem Ort und sicher auf.

Informationen, Links und weitere Materialien

- https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo
- https://datenschutz.saarland.de/ds-grundverordnung/einleitendes/
- https://datenschutz.saarland.de/themen/vereine/datenschutz-im-verein/

Für die im Vorherigen gemachten Ausführungen und Hinweise kann aufgrund der für jeden einzelnen Fall erforderlichen Prüfung und stetiger Änderungen bei der Rechtsprechung keine Haftung übernommen werden.

*Dieses Informationsblatt ist in Zusammenarbeit mit der **RKPN.de-Rechtsanwaltskanzlei Patrick R. Nessler**, Kastanienweg 15 in 66386 St. Ingbert entstanden. Wir bedanken uns für die Unterstützung und die Ausführungen. Sie finden die Kanzlei im Internet unter: www.rkpn.de*