DSVGO - Anforderungen an Vereine und Verbände

Hinweise und Anforderungen

Im Dezember 2015 wurde nach langen Verhandlungen der europäischen Mitgliedsstaaten eine europaweite Verordnung für den Datenschutz verabschiedet. Diese Datenschutzgrundverordnung (DSGVO) ist verbindliches und einheitliches Recht für die gesamte EU. Lediglich für einige Teile wurden, um nationale gesetzliche Besonderheiten abzudecken, Öffnungsklauseln ermöglicht.

Für Deutschland gilt jetzt neben DSGVO das BDSG (neu) und für den Bereich Telemedien das Telemediengesetzt (TMG).

Die neuen Anforderungen haben auch auf Vereine und Verbände zum Teil gravierende Auswirkungen.

Nachfolgend sind kurz die wesentlichen Anforderungen aus der neuen DSGVO aufgeführt, die jeder Verein und Verband für sich intensiv auf Anpassungsmaßnahmen prüfen sollte. Bereits gem. Art. 5 der DSGVO hat der Verein und Verband einen Nachweis (Rechenschaftspflicht) über die Einhaltung der gesetzlichen Anforderungen zu erbringen.

Ziele und Grundsätze

Die primären Ziele der DSGVO sind der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DSGVO) und der freie Verkehr personenbezogener Daten (Art. 1 Abs. 3 DSGVO). Dies soll durch die in Art. 5 DSGVO festgelegten Grundsätze der Verarbeitung personenbezogener Daten erreicht werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

Zusätzlich sollte durch die DSGVO erreicht werden, dass in ganz Europa gleiches Datenschutzrecht gilt, was unter der Richtlinie EU95/46 nie der Fall war.

Bußgelder und Sanktionen

Bisher galt die weitläufige Meinung, dass eine Nichtumsetzung des Datenschutzes ein Kavaliersdelikt sei und, dass durch deutsche Aufsichtsbehörden schlimmstenfalls eine Verwarnung ausgesprochen würde.

Ein Ziel der EU-Kommission für den Datenschutz war, den Schutz personenbezogener Daten auf ein Rechtsniveau mit anderen EU-Verordnungen anzuheben, vergleichbar mit Wettbewerbsrecht oder Kartellrecht. Dies spiegelt sich in Bußgeld- und Sanktionsmöglichkeiten wieder, die auch für Vereinen und Verbänden zum Tragen kommen und zukünftig bis zu 20 Millionen Euro als Strafe bedeuten würden. Geldbußen sollen wirksam, verhältnismäßig und abschreckend sein (Art. 81 Abs. 1 DSGVO)

Verantwortlich für die Umsetzung und Einhaltung der DSGVO sind die gesetzlichen Vertreter der Vereine und Verbände. Eine Nichtbefolgung der Pflichten, die sich aus der DSGVO ergeben, könnte Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes angenommen werden, wofür Vorstände persönlich haften würden

Vereine sind deshalb gut beraten, dieses Thema ernst zu nehmen, zumal der Aufwand zur Umsetzung für einen Verein in der Regel einen Manntag nicht überschreiten dürfte.

Beschäftigtendatenschutz

Für Beschäftigte von Vereinen und Verbänden sind keine speziellen Regelungen in der DSGVO vorhanden, jedoch im BDSG (neu) wird dieser Bereich im § 26 detailliert behandelt.

Neues zur Videoüberwachung

Auch zur Videoüberwachung findet man in der DSGVO keine expliziten Informationen. Diese ist unter § 4 BDSG (neu) geregelt, jedoch findet man die gesetzlichen Grundlagen hierzu unter **Art. 6 DSGVO** (Rechtmäßigkeit der Verarbeitung), **Art. 13 DSGVO** (Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person) **Art. 14 DSGVO** (Informationspflicht), **Art. 17 DSGVO** (Recht auf Löschung).

Datenportabilität

Diese Vorgabe ist neu. Mitgliedern oder auch Beschäftigten muss auf Wunsch deren Daten elektronisch in einem einfachen maschinenlesbaren Format zur Verfügung gestellt werden. Damit soll der Wechsel eines Mitarbeiters oder Mitgliedes vereinfacht werden und er beim neuen Arbeitgeber oder Verein die Stammdaten elektronisch eingespielt werden können.

Dies wird vermutlich daran scheitern, dass z.B. bei einem Vereinswechsel sich auch die Daten ändern werden.

Auftragsdatenverarbeitung

Alle Tätigkeit, die einen internen Prozess nach außen zu einem Dienstleister verlagern, sind in der DSGVO unter Art. 28 als Auftragsdatenverarbeitung definiert. Für Vereine könnte das sein:

- Gestalten der Webseite durch einen Dienstleister (z.B. Zugriff auf Kontaktdaten)
- Lohn- und Gehaltsabrechnung durch eine Steuerkanzlei
- Speicherung von Vereinsdaten in einer Cloud-Umgebung
- Durchführung von Newsletter durch einen Dienstleister
- Verteilung der Vereinszeitung durch einen Lettershop
- Etc.

In allen diesen oder ähnlichen Fällen muss der Verein seinen Dienstleister sorgfältig aussuchen, muss sich vergewissern, dass dieser den Datenschutz und technische und organisatorische Maßnahmen ordnungsgemäß umsetzt und ihn durch einen Vertrag zur Einhaltung des Datenschutzes verpflichten.

Die Überprüfung des Dienstleisters kann durch Besuch vor Ort, durch Befragung (z.B. durch einen Fragebogen) erfolgen oder der Dienstleister kann dies durch eine Zertifizierung bestätigen (z.B. ISO 27001).

Gemeinsam für die Verarbeitung Verantwortliche

Die Mitgliederverwaltung durch den VDST stellt keine Auftragsdatenverarbeitung dar, da Mitglieder des Vereins über diesen auch Mitglied im VDST und im jeweiligen Landesverband sind. Da sowohl der Verein, als auch Landesverbände und der VDST gleichermaßen für die Mitgliederdaten verantwortlich sind, gilt hier Art. 26 DSGV (**Gemeinsam für die Verarbeitung Verantwortliche**). Hierfür sind zwischen VDST, Landesverbänden und Vereinen Vereinbarungen zu treffen, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt, insbesondere was die Wahrnehmung der Rechte der betroffenen Person angeht, und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 nachkommt.

Vorsicht Vereins-Website

Website Betreiber müssen eine Vielzahl an Vorschriften beachten. Regelungen zur Website-Compliance finden sich u.a. in den §§ 11 ff. Telemediengesetz (TMG), insbesondere in § 13 TMG, der die Pflichten des Dienstanbieters vorgibt. Die Datenschutz- Grundverordnung wird zwangsläufig Auswirkungen auf die aktuellen Anforderungen an Website-Compliance haben. Zwar bleiben viele gesetzliche Pflichten erstmal bestehen, andererseits sollte aber die Datenschutzerklärung mit den Vorgaben der DSGVO abgestimmt werden. Zusätzlich wird hier für Vereine und

Verbände die vermutlich 2019 in Kraft tretende ePrivacy-Verordnung der EU zu berücksichtigen sein, die Informationspflichten und Einwilligungen in die Nutzung von Cookies auf Webseiten fordert.

Anforderungen an eine Einwilligung

Eine der Grundsätze für eine datenschutzkonforme Verarbeitung von personenbezogenen Daten stellt die Einwilligung gem. Art. 7 der DSGVO dar. Diese muss entweder schriftlich oder elektronisch durch Double-Opt-In erfolgen (z.B. Abonnement von Newsletter).

Die Einwilligung kann aber auch durch konkludentes Verhalten erteilt werden (z.B. Bestellung von Waren oder auch Antrag auf Mitgliedschaft in einem VDST-Verein). In diesen Fällen ist keine zusätzliche Einwilligung notwendig.

Auch die Weitergabe der Daten an Dritte (z.B. Weitergabe der Daten für die Verbandszeitschrift, die VDST-Versicherung oder die Hotline) bedarf keiner Einwilligung, da dies grundlegende Leistungen des VDST für seine Mitglieder darstellt und diese Leistungen nicht ausgeschlossen werden können. Die Einwilligung wird durch das Aufnahmeformular zur Mitgliedschaft erteilt. Hier gilt nur eine Informationspflicht.

Aber Vorsicht, die Pflicht zur Einwilligung trifft zu, wo man es häufig nicht vermutet. Fotos oder Geburtstagslisten (z.B. von Jubilaren) auf Vereinswebseiten, in der Vereinszeitung oder in Sozialen Netzen (Vereins-Newsgroup), führen immer wieder zu Verstößen und Beschwerden bei den Aufsichtsbehörden. Vor einer Veröffentlichung muss immer eine Einwilligung der Betroffenen eingeholt werden. Dies gilt auch für Fotos von Veranstaltungen.

Informationspflichten

Die DSGVO sieht im Art. 13 umfangreiche Informationspflichten vor. Dabei sollen Betroffene (Mitglieder) schon vorab über die Erhebung, Speicherung und Verarbeitung ihrer Daten informiert werden. Solche Informationen können bereits auf der Webseite aufgeführt werden, sollten aber zumindest auf dem Aufnahmeformular vorhanden sein.

Auch bei vielen anderen Leistungen muss der Betroffene erkennen können, wo seine Daten gespeichert werden bzw. über welche Dienstleister sie verarbeitet werden.

Betrieblicher Datenschutzbeauftragter

Für die meisten Vereine dürfte eine Bestellung eines Datenschutzbeauftragten (DSB) nicht in Frage kommen, wenn sie nicht mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Aber Vorsicht, Vereine und Verbände, die in Sachabteilungen Funktionäre haben, die z.B. Teilnehmerlisten, Wettkamplisten oder ähnliches führen, müssen, wenn hier mehr als 9 tätig sind, einen Datenschutzbeauftragten bestellen.

Eine Befreiung von der Bestellung eines DSB ist allerdings keine Entbindung von den Pflichten, die durch die DSGVO festgelegt sind. Dies bedeutet, dass der Verein anderweitig die Umsetzung erfüllen muss. Hat der Verein in den eigenen Reihen niemanden, der sich mit diesem Thema auskennt, kann ein externer Berater zurate gezogen werden.

Datensicherheit

Mit der DSGVO ändern sich die Vorgaben zur Datensicherheit und somit auch die der technischen und organisatorischen Maßnahmen. Die in Art. 32 DSGVO geforderte Sicherheit der Verarbeitung von personenbezogenen Daten fordert Maßnahmen, die deren Vertraulichkeit, Integrität und Verfügbarkeit gewährleistet. Zusätzlich sollen diese Maßnahmen belastbar sein und dem Stand der Technik entsprechen.

Gerade in Vereinen ist dies nur schwer zu kontrollieren, da die personenbezogenen Daten meist dezentral auf die Rechner der Funktionäre verteilt sind. Um der DSGVO gerecht zu werden, sollte überlegt werden, ob die Vereinsdaten nicht zentralisiert und damit besser vor Angriffen und Verlusten geschützt werden können.

Begriffe wie „data protection by default/by design“ weisen darauf hin, dass dabei die Systeme des Vereins so eingestellt werden sollten, dass Fehler durch Benutzer weitgehend ausgeschlossen werden können.

Datenschutz-Folgenabschätzung

Neu hinzugekommen ist die Datenschutz Folgeabschätzung. Sensible Daten sollen hier besonders geschützt werden. Daher muss anhand von Bedrohungs- und Risikoanalysen festgestellt werden, ob und welche Gefahren die personenbezogenen Daten bedrohen und mit welchen Maßnahmen diese Bedrohungen verhindert bzw. zumindest gemildert werden können.

Der Verein muss dies für seine Verfahren belegen. Die Datenschutz Folgeabschätzung muss in regelmäßigen Abständen widerholt werden.

Handhabung von Datenpannen

Werden personenbezogenen Daten entwendet bzw. gelangen an unbefugte Dritte, muss sofort reagiert werden. Sind durch die Datenpanne negative Folgen für den Betroffenen zu erwarten, muss spätestens 72 Stunden nach Entdeckung sowohl die Aufsichtsbehörde als auch die Betroffenen von dem Vorfall informiert werden. Den Betroffenen müssen Empfehlungen gegeben werden, wie Folgeschäden vermieden werden können.

Hierzu sind feste Standard-Prozesse zu definieren. Unterbleiben die Informationen, sieht die DSGVO erhebliche Sanktionen vor.

Verzeichnis von Verarbeitungstätigkeiten

Mit der Datenschutz-Grundverordnung muss auch ein Verein oder Verband nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten von personenbezogenen Daten führen. Dies sind in der Regel:

- Mitgliederverwaltung
- Kassenführung
- Versand der Vereinszeitschrift
- Newsletter
- Webseitenverwaltung
- Durchführen von Kursen und Veranstaltungen mit Teilnehmerlisten
- Wenn der Verein oder Verband Mitarbeiter hat, alle Verfahren des Personalwesens

Werden sensible Daten in den Verfahren verarbeitet (z.B. Mitgliederverwaltung mit Bankverbindungen, Nachweis der Tauchsportuntersuchung etc.), muss geprüft werden, ob es Bedrohungen für das Verfahren gibt und ob ausreichende Gegenmaßnahmen getroffen wurden. Diese Datenschutz Folgeabschätzung ist ebenfalls zu dokumentieren.

Das Recht auf Vergessenwerden

Die DSGVO schreibt vor, dass jeder Nutzer verlangen kann, dass seine Daten gelöscht werden. Dies ist natürlich nur dann möglich, wenn das Vorhandensein von Daten nicht zwingend notwendig ist. So können Mitgliederdaten nicht einfach auf Verlangen gelöscht werden, da diese zur Abwicklung der „Geschäftszwecke“, also den Leistungen von Verein und Verband, zwingend notwendig sind. Allerding könnte ein Mitglied verlangen, dass seine Daten nach dem Ausscheiden gelöscht werden. Dies wäre dann auch möglich, wenn keine gesetzlichen Aufbewahrungsfristen betroffen sind. Meist reicht aber auch schon eine Teillöschung, z.B. aus der Newsletter-Datenbank, wenn ein Widerspruch vorliegt.

Aufbau eines Datenschutz-Managementsystems

Die für die DSGVO notwendigen Maßnahmen sind umfangreich und über die Vielzahl der Dokumentationen verliert man schnell den Überblick. Vor allem wiederkehrende Maßnahmen sind nur schwer nachvollziehbar. Deshalb sollte man sich ein sinnvolles Datenschutz-Managementsystem aufbauen. Hilfreich können hier Softwareprodukte sein, die bereits von der Struktur als Managementsystem fungieren.

Besondere Kategorien personenbezogener Daten

Besondere Anforderungen und Sicherheitsmaßnahmen sind zu treffen und zu belegen, wenn besondere Kategorien personenbezogener Daten verarbeitet werden, was oft in Vereinen und Verbänden vorkommt. Darunter fallen Daten der Gesundheit, zur ethnischen Herkunft, zur Religion u. a. Bei dieser Verarbeitung ist auf jeden Fall eine Datenschutzfolgenabschätzung durchzuführen. Solche Daten werden auch in Vereinen und Verbänden an vielen Stellen verarbeitet.

Datenverarbeitung von Kindern und Jugendlichen

Der Kinder- und Jugendschutz nimmt in der EU-Datenschutz-Grundverordnung (DSGVO) eine wichtige Rolle ein. So findet sich in der Verordnung z.B. erstmals eine ausdrückliche gesetzliche Regelung zu Anforderungen an die Rechtmäßigkeit der Einwilligung von Kindern. Hier sind vor allem für Vereine die neuen Anforderungen zu prüfen und rechtzeitig umzusetzen.

Ansprech-Partner beim Verband Deutscher Sporttaucher e.V.

Lothar Becker

Thalacker 5a
83043 Bad Aibling
Tel.: +49 (0)8061 495743

datenschutz@vdst.de