Maßnahmenkatalog zur DSGVO

Die neuen Anforderungen aus der Datenschutz-Grundverordnung (DSGVO) haben auch für Vereine und Verbände zum Teil gravierende Auswirkungen. Jeder Verein und Verband sollte die hier aufgeführten Anforderungen intensiv prüfen und alle notwendigen Anpassungs-, Änderungs- und Ergänzungsmaßnahmen durchführen.

Ziele und Grundsätze

Neben der weitgehenden Vereinheitlichung des europäischen Datenschutzrechts verfolgt die DSGVO in erster Linie den Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und hier insbesondere deren Recht auf Schutz personenbezogener Daten.

Für die Realisierung der Ziele wurden in der DSGVO Grundsätze für die Verarbeitung von personenbezogenen Daten festgelegt: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit sowie Rechenschaftspflichten.

Anforderungen an Einwilligungserklärungen

Das betroffene Personen in Verarbeitung ihrer personenbezogenen Daten einwilligen müssen, ist auch schon im bisherigen Datenschutzgesetz verpflichtend. Grundlage hierfür ist das Grundrecht auf informationelle Selbstbestimmung, das jedem Bürger das Recht einräumt, für sich zu entscheiden, wer welche Informationen über ihn erhält.

An dieser Stelle sind Vereine und Verbände besonders gefordert, die Umsetzung und Anpassung an die DSGVO sicherzustellen. In der Vergangenheit waren es hauptsächlich die Einwilligungserklärungen sowie die Nutzung von Fotos in Vereinen, die immer wieder zu Beschwerden bei den Aufsichtsbehörden geführt haben.

Informationspflichten

Durch die DSGVO kommen auf Vereine, Verbände und deren Verantwortliche ein paar Neuerungen bei den Informationspflichten zu. Die neue Gesetzgebung verfolgt das Ziel einer fairen und transparenten Datenverarbeitung. Die betroffenen Personen - Vereinsmitglieder - sollen in die Lage versetzt werden, die Erhebung, Verarbeitung und Nutzung aufgrund der vom Verein zur Verfügung gestellten Informationen zu überprüfen.

Für die Vereine und Verbände bedeutet dies, dass sie für alle Mitglieder, Interessenten und sonstige Personen sicherstellen müssen, die Anforderungen an die Informationspflichten zu erfüllen.

Besondere Kategorien personenbezogener Daten

Schon in der bisherigen Fassung des BDSG ist der Umgang mit besonders sensiblen Daten geregelt. Darunter fallen u.a. Gesundheitsdaten, Daten zur ethnischen Herkunft oder zur Religionszugehörigkeit.

Neu kommen jetzt noch biometrische und genetische Daten hinzu. Für alle besonders sensiblen Daten benötigen Vereine und Verbände ausdrückliche Einwilligungserklärungen.

... 2

Bei der Verarbeitung ist auf jeden Fall eine Datenschutz-Folgenabschätzungen durchzuführen. Somit müssen auch Vereine und Verbände diese Vorgaben bei der Umsetzung berücksichtigen.

Verzeichnis von Verarbeitungstätigkeiten

In der DSGVO ist ebenfalls geregelt, dass Vereine und Verbände ein Verzeichnis aller Verarbeitungstätigkeiten führen müssen, mit den personenbezogenen Daten verarbeitet werden. Aufgrund dieser Aufstellung kommt dem Verzeichnis der Verarbeitungstätigkeiten eine ganz wichtige Bedeutung zu.

Auftragsverarbeitung

In Deutschland ist das Prinzip der Auftragsdatenverarbeitung (ein Auftragnehmer verarbeitet auf Weisung eines Auftraggebers personenbezogene Daten, wobei die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber liegt) schon lange im BDSG (alte Fassung) verankert.

Die DSGVO regelt diese Verarbeitung nun europaweit. Vereine und Verbände müssen sich in diesem Kontext nun intensiv mit ihren "ausgelagerten Verarbeitungen" auseinandersetzen (Hosting der Webseiten, Mitgliederverwaltung durch Geldinstitute, Auslagerung von Seminardurchführungen etc.).

Datenportabilität

Ein bislang unbekanntes Thema. Mitglieder und Beschäftigte erhalten das Recht, dass der Verein oder Verband die über die jeweilige Person gespeicherten Daten elektronisch in einem einfachen maschinenlesbaren Format zur Verfügung stellen muss. Durch diese Möglichkeit soll dem Mitglied bzw. dem Beschäftigten der Wechsel zu einem neuem Verein oder Arbeitgeber erleichtert werden.

Recht auf Vergessenwerden

Neben den bereits bekannten Regelungen zur Berichtigung, Sperrung und Löschung von Daten enthält die DSGVO ab Mai auch das Recht auf Vergessenwerden.

Dieses neue Recht ist eine Erweiterung des Rechts auf Löschung. Daten, für die keine Zweckbindung mehr besteht und keine Aufbewahrungspflichten mehr einzuhalten sind, müssen gelöscht werden. Wurden die Daten an andere Empfänger weitergegeben, sind diese über die Löschung zu informieren, damit auch dort die entsprechenden Daten gelöscht werden.

Eine Nichtbeachtung dieser Regelungen kann Bußgeldanordnung zur Folge haben.

Verarbeitung der Daten von Kindern und Jugendlichen

Die DSGVO legt besonderen Wert auf den Kinder- und Jugendschutz. Aus diesem Grund wurde erstmalig eine ausdrückliche gesetzliche Regelung an die Rechtmäßigkeit der Einwilligung von Kindern.

In diesem Zusammenhang müssen vor allem Vereine die neuen Anforderungen prüfen und rechtzeitig umsetzen.

… 3

Datenschutz-Folgenabschätzung

Vorabkontrolle war gestern, ab dem 25. Mai 2018 heißt das neue "Prüfinstrument" dann Datenschutz-Folgenabschätzung. Mit deren Anwendung müssen Vereine und Verbände nachweisen, dass bei bestimmten Verarbeitungen entsprechende Maßnahmen getroffen werden, um die Risiken und Bedrohungen für die Betroffenen zu reduzieren.

Die Datenschutz-Folgenabschätzungen sind regelmäßig zu wiederholen und zu dokumentieren. Auf Anforderung hin müssen die Ergebnisse der Aufsichtsbehörde zur Verfügung stellen.

Aufbau eines Datenschutz-Management-Systems

Eines der Hauptaugenmerke der DSGVO befasst sich mit der Dokumentation aller Datenschutzmaßnahmen. Die Verordnung fordert die Beschreibung aller Prozesse und Aufgaben, die wahrgenommen werden müssen.

Ähnlich einem Qualitätsmanagement-System sollen auch hier alle Vorgaben erfasst und beschrieben werden. Ein Datenschutz-Management-System unterstützt die regelmäßigen Arbeiten und deren Kontrolle.

Datensicherheit

Durch die neue Gesetzgebung der DSGVO treten maßgebliche Änderungen im Bereich der Datensicherheit sowie bei den technisch-organisatorischen Maßnahmen ein. Manche Begriffe werden nun noch abstrakter ausgelegt als bisher, einige Vorgehensweisen bleiben nahezu unverändert und es kommen auch neue Anforderungen hinzu.

Begriffe wie 'Stand der Technik', 'Belastbarkeit', 'Privacy by design' und 'Privacy by default' stellen Vereine und Verbände vor Herausforderungen, um die neuen technisch-organisatorischen Maßnahmen zum Schutz der Daten zu erfüllen

Benachrichtigungspflicht bei Datenschutzverletzungen

Zukünftig gibt es verschärfte Regeln, wenn sich vermutlich oder erwiesenermaßen eine "Datenpanne" ereignet hat. Eine Datenschutzverletzung muss innerhalb von 72 Stunden nach bekannt werden der Aufsichtbehörde gemeldet werden.

Je nach Schwere der Datenpanne besteht ebenfalls die Verpflichtung die betroffenen Personen zu informieren. Alle notwendigen Schritte sind ausführlich in der DSGVO beschrieben.

Für Vereine und Verbände hat dies zur Folge, dass sie einen Prozess entwickeln sollten, um im Fall einer Datenpanne angemessen reagieren zu können.

Datenschutzbeauftragter

Auch in diesem Punkt ist Deutschland bislang Vorreiter in Europa. Durch die DSGVO hat sich für Vereine und Verbände eigentlich nichts Grundlegendes geändert.

Es gilt weiterhin, dass wenn mehr als neun Personen mit der Verarbeitung (Erheben, Speichern, Nutzen etc.) personenbezogener Daten betraut sind, muss ein Datenschutzbeauftragter bestellt werden.

… 4

Diese Voraussetzung trifft auf fast jeden Verein zu, da jeder Abteilungsleiter, Trainer, Übungsleiter Daten der Mitglieder nutzt oder diese sogar noch um zusätzliche Daten ergänzt.

Videoüberwachung

In der Vergangenheit gab es bei der Videoüberwachung bereits hohe gesetzliche Hürden. Mit der DSGVO erweitert sich der Risikobereich, sollte eine Videoüberwachung nicht datenschutzkonform angewendet werden.

Beschäftigtendatenschutz

Sollten Sie in Ihrem Verein oder Verband Mitarbeiter*innen beschäftigen (Hauptamtliche, Trainer, Übungsleiter etc.) müssen Sie auch die jeweiligen Regelungen in der DSGVO beachten.

Des Weiteren bleibt es abzuwarten, welche Regelungen die Bundesregierung im Rahmen der Öffnungsklauseln im BDSG-neu oder eventuell doch in dem seit vielen Jahren angekündigten separaten Gesetz umsetzen wird.

Bußgelder und Sanktionen

Bislang wurden von den deutschen Aufsichtsbehörden eher geringfügige Bußgelder auferlegt. In diesem Punkt gibt es eine der markantesten Änderungen zum bisherigen Recht, da die DSGVO Vorschriften enthält, die zu deutlich spürbaren Bußgeld- und Sanktionsmöglichkeiten führen. Diese werden auch bei Vereinen und Verbänden zum Tragen kommen.

Schon um finanziellen Schaden von der Organisation oder einzelnen Personen fernzuhalten, ist es geboten, die vorstehenden Punkte ausführlich zu analysieren und der neuen Rechtsnorm anzupassen.

Betreiber von Webseiten

Insbesondere Webseiten der Vereine und Verbände stellen ein Risiko dar, wenn man diese nicht 'up-to-date' hält. Die DSGVO enthält bereits einige Anforderungen an die Website-Compliance und dann ist noch geklärt, ob auch die "ePrivacy-Verordnung" ebenfalls zum 25. Mai 2018 in Kraft treten wird. Dieses Gesetz löst dann das Telemediengesetz und das Telekommunikationsgesetz ab. Dementsprechend sind - sobald die "ePrivacy-Verordnung" in Kraft tritt auch die geänderten Informationspflichten und Einwilligungen in die Nutzung von Cookies auf den Webpräsenzen anzupassen.

Besonders zu beachten!

Ein wesentlicher Paradigmenwechsel durch die neue DSGVO ist die Beweislastumkehr! Vereine und Verbände müssen dann aktiv nachweisen können, dass ihre Datenverarbeitungen datenschutzkonform sind (Rechenschaftspflicht); Dokumentationspflichten sollen dies sicherstellen. Vereine und Verbände haben geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen und nachweisen zu können, dass bei der Datenverarbeitung die DSGVO eingehalten wird.