Datenschutz im Verein - hier ADAC Ortsclubs

(Stand 19.03.2018)

Vorbemerkung:
Dieses Dokument hat keinen Anspruch auf Vollständigkeit sondern listet ausschließlich die wesentlichen Punkte der EU-DSGVO auf, welche ein Verein zu berücksichtigen hat. Den Ortsclubs wird empfohlen, sich mit den neuen Regelungen vertraut zu machen und entsprechende Maßnahmen zu ergreifen.

Hinweise und Anforderungen
Nachfolgend sind kurz die wesentlichen Anforderungen aus der neuen EU-DSGVO aufgeführt, die alle nicht nur für „Unternehmen", sondern für alle natürlichen und juristischen Personen, also auch für jeden Verein und Verband gelten. Es wird empfohlen, dass jeder Ortsclub für sich intensiv entsprechende Anpassungsmaßnahmen prüft und – soweit erforderlich – ergreift. Bereits gem. Art. 5 der EU-DSGVO hat der Verein und Verband einen Nachweis (Rechenschaftspflicht) über die Einhaltung der gesetzlichen Anforderungen zu erbringen.

Einen ausführlichen Gesamtüberblick bietet die aktuelle Orientierungshilfe des Landesbeauftragten für den Datenschutz Baden-Württemberg „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)".

Inhalt

1. Wer ist im Ortsclub für den Datenschutz zuständig?

Die Hauptverantwortung für die Organisation und Durchführung entsprechender Datenschutzmaßnahmen liegt beim Vorstand.
Sind mehr als 10 Personen mit der automatisierten Verarbeitung von Daten, d. h. mit einer technisch unterstützten Verarbeitung mittels einer Datenspeicherungsanlage, beschäftigt, muss – wie bisher auch schon – ein Datenschutzbeauftragter bestellt werden (s. Ziffer 10.).

2. Welche Daten sind betroffen?

Geschützt sind personenbezogene Daten, also Einzelangaben, die eine Person betreffen oder auf sie bezogen werden können. Betroffene Personen sind im Verein insbesondere Mitglieder, Veranstaltungsteilnehmer, Sponsoren, Geschäftspartner, usw. Datenverarbeitungen erfolgen typischerweise bezüglich Name, Vorname, Anschrift, Telefonnummer, E-Mailadresse, Geburtsdatum, Eintrittsdatum, Bankverbindung, Platzierungen / sportliche Leistungen bei Wettbewerben, etc. Dabei spielt es keine Rolle, ob die Erfassung per Computer oder in Papierform erfolgt.

3. Welche Ziele und Grundsätze hat die EU-DSGVO?

Die Ziele der EU-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). Die vorangestellten Ziele sollen durch die in Art. 5 DSGVO festgelegten und zu beachtenden Grundsätze der Verarbeitung personenbezogener Daten erreicht werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

4. Auf welcher Grundlage dürfen Daten überhaupt verarbeitet werden?

Die Verarbeitung personenbezogener Daten darf nur erfolgen soweit eine Rechtsvorschrift dies erlaubt bzw. einen dazu verpflichtet oder der Betroffene eingewilligt hat. Erlaubt ist beispielsweise die Datenverarbeitung soweit dies im Rahmen eines Vertragsverhältnisses für dessen Durchführung notwendig ist. Bei Vereinen besteht eine vertragliche Beziehung mit den Mitgliedern, wodurch zur Mitgliederverwaltung die Verarbeitung von Name, Vorname, Geburtsdatum und Bankverbindung gerechtfertigt ist, allerdings nicht von weitergehenden Daten, wie Telefonnummer, Fotos, etc., die nur auf Basis einer freiwilligen Einwilligung gespeichert werden dürfen. Weiterführende Informationen zur Einwilligung finden Sie über das Kurzpapier des Bayerischen Landesamts für Datenschutzaufsicht.

Der Aufnahmeantrag muss sich auf die Erhebung der für die Mitgliederverwaltung erforderlichen Daten beschränken und entsprechende datenschutzrechtliche Hinweise sowie – soweit erforderlich – Einwilligungserklärungen enthalten. Stets sind technisch organisatorische Maßnahmen zum Schutz personenbezogener Daten zu ergreifen (s. dazu die Ausführungen zur Datensicherheit unter Ziffer 11.).

Personen, die mit der Datenverarbeitung betraut sind, sind auf das Datengeheimnis zu verpflichten. Dies sollte über ein entsprechendes Formular mit Merkblatt und Unterschrift geschehen und dokumentiert werden.

5. Was gibt es Neues zur Videoüberwachung?

Für die Videoüberwachung auch bei Vereinen und Verbänden gab es schon bisher nach der deutschen Gesetzgebung hohe Anforderungen. Mit der EU-DSGVO werden die Risiken für eine nicht korrekt betriebenen Videoüberwachung größer. Daher ist dringend – falls im Einsatz oder geplant – eine Interessenabwägung vorzunehmen und die Erforderlichkeit sowie die datenschutzkonforme Anwendung von Videoüberwachungen zu prüfen und den neuen Anforderungen anzupassen. Dabei ist ein besonderes Augenmerk auf inhaltliche Voraussetzungen, Transparenzanforderungen und Hinweisbeschilderung, Speicherdauer /

Löschungsgebot, eine sichere und datenschutzfreundliche Gestaltung der Videoüberwachung sowie eine entsprechende Dokumentation im Verfahrensverzeichnis zu legen. Details können Sie dem Kurzpapier Nr. 15 der Datenschutzkonferenz entnehmen.

6. Muss ein Verzeichnis von Verarbeitungstätigkeiten angelegt werden?

Ja, mit der Datenschutz-Grundverordnung muss auch ein Verein oder Verband nach Art. 30 DSGVO ein Verzeichnis aller Verarbeitungstätigkeiten von personenbezogenen Daten führen. Dies ist nur eine von mehreren, neuen Vorgaben zur Dokumentationspflicht. Bei der Einhaltung aller gesetzlichen Vorgaben wird das Verzeichnis aber eine tragende Rolle spielen. Denn es enthält eine Dokumentation und Übersicht über alle eingesetzten Verfahren, bei denen personenbezogene Daten verarbeitet werden. Es muss insbesondere Angaben zum Verantwortlichen, zum Ansprechpartner, zum Zweck der Verarbeitung, eine Beschreibung der Kategorien der Daten, der Kategorien der betroffenen Personen, der Kategorien von Empfängern, die Daten erhalten, vorgesehene Löschfristen für die verschiedenen Datenkategorien enthalten. Ein für alle Vereine typisches relevantes Beispiel für ein Verfahren ist die Verarbeitungstätigkeit „Mitgliederverwaltung“. Weiterführende Informationen zu diesen Verzeichnissen finden Sie im Kurzpapier Nr. 1 der Datenschutzkonferenz.

7. Was muss bei Auftragsverarbeitungen beachtet werden?

In Deutschland definiert sich die Auftragsverarbeitung als Datenverarbeitung durch einen Auftragnehmer auf Weisung eines Auftraggebers, bei dem die Verantwortung für die ordnungsgemäße Datenverarbeitung verbleibt. In der Datenschutz-Grundverordnung werden diese nun erstmals europaweit einheitlich geregelt. Für Vereine und Verbände sind hier vor allem die Hoster der Internetauftritte und eigenen Apps zu berücksichtigen, Dienstleister für IT-Themen, Daten- und Aktenvernichter sowie z. B. Auslagerung von Diensten wie Sportveranstaltungen an Dienstleister. Hierzu ist eine Bestandsaufnahme zu machen und es sind mit allen bereits bestehenden und neuen Auftragsverarbeitern entsprechende Datenschutzvereinbarungen abzuschließen mit entsprechender Checkliste zu den TOM`s (technische und organisatorische Maßnahmen). Weiterführende Informationen finden Sie im Kurzpapier Nr. 13 der Datenschutzkonferenz. Eine Formulierungshilfe für einen Auftragsverarbeitungsvertrag hat der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg über diesen Link zur Verfügung gestellt.

8. Was gilt für Websitebetreiber?

Website Betreiber müssen eine Vielzahl an Vorschriften beachten. Sie sollten sehr sorgfältig überlegen, ob und welche personenbezogenen Daten im Internet veröffentlicht werden. Weiterhin sind entsprechende Informationspflichten gegenüber den betroffenen Personen zu beachten. Folgende Inhalte müssen auf der Website abrufbar sein: Impressum, Datenschutzerklärung und Haftungshinweise (Verwendung von Links, Plugins, Cookies, …). Regelungen zur Website-Compliance finden sich u.a. in den §§ 11 ff. Telemediengesetz (TMG), insbesondere in § 13 TMG, der die Pflichten des Diensteanbieters 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 EU-DSGVO abgestimmt werden. Zusätzlich wird hier für Vereine und Verbände die ggf. ebenfalls zum Mai 2018 in Kraft tretende ePrivacy-Verordnung der EU zu berücksichtigen sein, die Informationspflichten und Einwilligungen in die Nutzung von Cookies auf Webseiten fordert.

9. Welche Anforderungen gelten für Einwilligungen?

Die Einwilligung in die Verarbeitung seiner personenbezogenen Daten durch den Betroffenen ist seit jeher zentraler Bestandteil des Datenschutzrechts. Aufgrund des Grundrechts der informationellen Selbstbestimmung kann jeder Bürger für sich entscheiden, wer welche Informationen über ihn erhält. Hier müssen Vereine und Verbände eine saubere Umsetzung und Anpassungen sicherstellen, da vor allem die

Einwilligung in Nutzung von Fotos in Vereinen immer wieder zu Verstößen und Beschwerden bei den Aufsichtsbehörden führt. Schriftliche Einwilligungen, die vor Geltung der EU-DSGVO rechtswirksam eingeholt wurden und den Vorgaben der EU-DSGVO entsprechen, gelten grundsätzlich weiter fort und müssen nicht neu eingeholt werden. Weiterführende Informationen zur Einwilligung finden Sie über das Kurzpapier des Bayerischen Landesamts für Datenschutzaufsicht. Details zur Einwilligung eines Kindes finden Sie ebenfalls in einem entsprechenden Kurzpapier des Bayerischen LfD.

10. Ist ein betrieblicher Datenschutzbeauftragter zu bestellen?

Das Modell Datenschutzbeauftragter ist in Deutschland seit langem bekannt und viele Unternehmen müssen bereits jetzt einen Datenschutzbeauftragten bestellen. Für Deutschland gilt weiterhin, auch für Vereine und Verbände, dass ein Datenschutzbeauftragter zu benennen ist, wenn mehr als 10 Personen mit der Verarbeitung (Erheben, Speichern, Nutzen, ...) personenbezogener Daten betraut sind. Weitergehende Informationen finden Sie auch im Kurzpapier Nr. 12 der Datenschutzkonferenz.

11. Was gilt für die Datensicherheit?

Mit der DSGVO ändern sich die Vorgaben zur Datensicherheit und somit auch die der technischen und organisatorischen Maßnahmen. Manche Begriffe werden durch die Verordnung noch abstrakter, als sie es bisher gewesen sind, einige Vorgehensweise ähneln der jetzigen Handhabung und wiederum andere Anforderungen, wie der Stand der Technik, Belastbarkeit oder data protection by default, sind neu. Auf Vereine und Verbände kommt daher eine Menge Arbeit zu, die technischen und organisatorischen Maßnahmen, wie beispielsweise Zutrittskontrolle, Zugriffskontrolle, Weitergabekontrolle, etc. durch abschließbare Räumlichkeiten, Passwortschutz, Einsatz von Verschlüsselungen, usw. zum Schutze der Daten zu erfüllen.

12. Was gibt es für Informationspflichten?

Die Datenschutz-Grundverordnung führt für Vereine, Verbände und Verantwortlichen eine Reihe von neuen Informationspflichten ein. Dabei ändert sich im Vergleich zu den bisherigen Vorschriften des Telemedien- und Bundesdatenschutzgesetz einiges an den Anforderungen. Denn der europäische Gesetzgeber verfolgt das Ziel, dem Grundsatz der fairen und transparenten Datenverarbeitung gerecht zu werden. Die Betroffenen Nutzer sollen zukünftig besser in der Lage sein, eine Datenerhebung, - verarbeitung oder -nutzung, anhand den zur Verfügung gestellten Informationen, zu überprüfen. Daher müssen die Vereine und Verbände bis zum Mai 2018 sicherstellen, dass alle neuen Informationspflichten erfüllt werden. Beitrittsformulare, Einwilligungserklärungen, etc. sind an die aktuellen Anforderungen anzupassen.

13. Muss eine Datenschutz-Folgenabschätzung durchgeführt werden?

Die Datenschutzfolgenabschätzung ist neu. Hier muss der Verein und Verband belegen, dass bei bestimmten Verarbeitungen, die Risiken und Bedrohungen für die Betroffenen mit entsprechenden Maßnahmen gemindert werden. Diese Prüfung ist regelmäßig zu wiederholen und zu dokumentieren und auf Anforderung der Datenschutzaufsichtsbehörde zur Verfügung zu stellen.

14. Was ist bei einer Datenpanne zu tun?

Schon heute müssen Verantwortliche, unter bestimmten Voraussetzungen, Aufsichtsbehörde und Betroffenen eine Meldung bezüglich einer Datenpanne zukommen lassen. Nämlich dann, wenn Unberechtigte vermutlich oder erwiesenermaßen Zugang zu Daten hatten. Die Datenschutz-Grundverordnung wird diese Anforderungen und etwaige Sanktionen noch deutlich verschärfen.
Eine Datenschutzverletzung ist innerhalb von 72 Stunden der Aufsichtsbehörde zu melden. Die EU-DSGVO macht dazu klare Vorgaben. Daher sollte ein Standard- Prozess etabliert werden.

15. Ist der Aufbau eines Datenschutzmanagementsystems sinnvoll?

Neben dem angesprochenen Verzeichnis von Verarbeitungstätigkeiten findet sich in der Datenschutz-Grundverordnung eine Vielzahl von Normen, die eine Dokumentierung der getroffenen Datenschutzmaßnahmen fordern. Bei dieser Vielzahl von Anforderungen kann man schnell mal den Überblick verlieren. Daher bietet sich ein Datenschutzmanagement an, um die Einhaltung aller Vorgaben systematisch zu planen, umzusetzen und laufend zu kontrollieren.

16. Was bedeutet das Auskunftsrecht des Betroffenen?

Betroffene Personen haben ein Recht, Auskunft darüber zu verlangen, ob und – falls ja – welche Daten verarbeitet werden. Sind die Daten nicht korrekt, kann der Betroffene Berichtigung der Daten verlangen. Hier ist Vorsorge zu treffen, dass die Ansprüche auch zeitnah erfüllt werden können. Details zum Auskunftsrecht entnehmen Sie bitte dem Kurzpapier Nr. 6 der Datenschutzkonferenz.

17. Was ist das Recht auf Vergessenwerden?

Das Bundesdatenschutzgesetz enthält ein Recht auf Berichtung, Sperrung und Löschung. Dieses Recht auf Löschung wird in der Datenschutz-Grundverordnung um das Recht auf Vergessenwerden erweitert. Daten, deren Zweck erfüllt ist und keine gesetzliche Aufbewahrungspflicht besteht, sind zu Löschen. Die Nicht-Einhaltung dieser Vorgabe kann mit den höchsten Strafgeldern belegt werden. Weiterführende Informationen zum Recht auf Löschung und Vergessenwerden finden sich im Kurzpapier Nr. 11 der Datenschutzkonferenz.

18. Was gilt für besondere Kategorien personenbezogener Daten?

Besondere Anforderungen und Sicherheitsmaßnahmen sind zu treffen und zu belegen, wenn besondere Kategorien personenbezogener Daten verarbeitet werden. Darunter fallen Daten der Gesundheit, zur ethnischen Herkunft, zur Religion u. a. Bei dieser Verarbeitung ist auf jeden Fall eine Datenschutzfolgenabschätzung durchzuführen. Informationen dazu finden Sie im entsprechenden Kurzpapier des Bayerischen LfD.

19. Was gilt für die 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. Details zur Einwilligung eines Kindes finden Sie in einem entsprechenden Kurzpapier des Bayerischen LfD.

20. Welche Bußgelder und Sanktionen drohen?

Die EU-Datenschutz- Grundverordnung enthält eigene Vorschriften zu Bußgeld- und Sanktionsmöglichkeiten. Dieses würde auch bei Vereinen und Verbänden zum Tragen kommen und kann zukünftig im Extremfall bis zu 20 Millionen Euro als Strafe bedeuten. Sicherlich wird der Extremfall die Ausnahme darstellen, jedoch sind vier- bis fünfstellige Bußgelder auch im Verein durchaus denkbar.

21. Externe Links zu weiterführenden Informationen zur EU-DSGVO

- Informationen und Formulierunghilfen des Landesbeauftragten für Datenschutz und Informationssicherheit Baden-Württemberg
- Orientierungshilfe des Landesbeauftragten für den Datenschutz Baden-Württemberg „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)“
- Informationen und Formulierungshilfen des Bayerischen Landesamts für Datenschutzaufsicht
- Information der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit
- Gesellschaft für Datenschutz und Datensicherheit e.V.