Deutscher Dart-Verband e.V.

Generalsekretär Volker Bernardi
als Datenschutzbeauftragter
Otto-Fleck-Schneise 12
D – 60528 Frankfurt am Main
Fon +49 (0)176 64 19 77 02

volker.bernardi@ddv-online.com
www.ddv-online.com

Deutscher Dart-Verband e.V.

An die
Landesverbände im DDV zum Verbleib
und zur Weiterleitung an Mitgliedsvereine

Frankfurt am Main, 16. Mai 2018

Zur EU-DS-GVO (Datenschutz-Grundverordnung) mit Gültigkeit ab 25. Mai 2018
Verordnung (EU) 2016/679 (DS-GVO)

Sehr geehrte Damen und Herren,

die vorliegende Handreichung des DDV-Datenschutzbeauftragten dient für die Landesverbände und deren Mitgliedsvereine im Deutschen-Dart Verband e.V. als Erstinformation über die von der Europäischen Union beschlossene EU-Datenschutz-Grundverordnung (EU-DS-GVO). Die Verordnung tritt am 25. Mai 2018 in Kraft und wird mit weitreichenden Änderungen zu einer erheblichen Verschärfung datenschutzrechtlicher Regelungen führen.

Vorab schon zur Frage, ob die diverse spezifischen Regelungen der EU-DS-GVO überhaupt für die organisierte deutsche Dartlandschaft Gültigkeit haben, ob also bspw. die vielen Sportorganisationen jeweils Datenschutzbeauftragte benennen müssen: das ist alleine schon wegen der regelmäßigen Vielzahl der mit der Verarbeitung der Datensätze beschäftigten Personen in Sportverbänden und Vereinen der Fall. Näheres dazu unter dem Punkt „Datenschutzbeauftragter“.

Die neuen Regelungen sollen und werden zu einer weitgehenden Vereinheitlichung europäischen Datenschutzrechtes führen. Während bislang durch nationale Gesetzgebungen auf Grundlage der EU-Datenschutzrichtlinie doch erhebliche Unterschiede bestanden, wird die Datenschutz-Grundverordnung direkt geltendes Recht in allen Mitgliedsstaaten sein mit teilweise gravierenden Auswirkungen auch auf Vereine und Verbände.

In dieser Handreichung sind nur die wesentlichen Anforderungen aus der neuen EU-DS-GVO aufgeführt, die jeder Verein und Verband für sich intensiv auf Anpassungsmaßnahmen prüfen sollte.

Ziele und Grundsätze der EU-DS-GVO – mehr Schutz für personenbezogene Daten
Die DS-GVO regelt vor allem, wie persönliche Daten von Bürgern bei EU-internen Transaktionen gespeichert und geschützt werden müssen und den Export solcher Daten in Länder außerhalb der Europäischen Union. Rechtlich sind das der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten (Art. 1 Abs. 2 DS-GVO) und der freie Verkehr personenbezogener Daten (Art. 1 Abs. 3 DS-GVO). Die vorangestellten Ziele sollen durch die in Art. 5 DS-GVO festgelegten

Grundsätze der Verarbeitung personenbezogener Daten erreicht werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht.

Die wichtigsten Änderungen mit Auswirkung auf Verbände und Vereine auf einen Blick

1.) EU-weit gelten die gleichen Datenschutzregeln. Das bedeutet auch eine gestiegene Verantwortung und Haftung für alle, die persönliche Daten verarbeiten, einschließlich Verbände und Vereine.

2.) Recht auf Vergessen: Wollen Nutzer ihre Daten nicht weiterhin verarbeitet sehen, sind diese zu löschen - vorausgesetzt, es spricht aus juristischer Sicht nichts dagegen.

3.) "Opt-in" statt "Opt-out“: Sollen persönliche Daten verarbeitet werden, müssen Nutzer aktiv zustimmen (und nicht aktiv widersprechen wie bisher).

4.) Recht auf Transparenz: Nutzer haben ein Recht auf Transparenz - sie dürfen erfahren, welche Daten über sie gesammelt und wie diese verarbeitet werden.

5.) Zugang und Portabilität: Der Zugang zu den bei Dritten über einen selbst gespeicherten Daten soll einfacher möglich sein. Zudem ist die Datenportabilität zu gewährleisten - also sicherzustellen, dass persönliche Informationen leichter von einem Dienstanbieter zu einem anderen übertragen werden können.

6.) Schnellere Meldung: Tritt ein Datenverlust auf, müssen Organisationen im Regelfall binnen 24 Stunden, höchstens 72 Stunden, mindestens aber so schnell wie möglich, ihrer behördlichen Meldepflicht nachkommen.

7.) Weniger Behördenchaos: Organisationen müssen sich nur noch mit einer einzigen Aufsichtsbehörde auseinandersetzen - und zwar dort, wo sie ihren Hauptsitz haben

8.) Grenzübergreifend: Privatanwender dürfen jeden Fall von Datenmissbrauch an ihre nationale Aufsichtsbehörde melden - selbst dann, wenn die betroffenen Daten im Ausland verarbeitet wurden.

9.) Erweiterter Geltungsbereich: Die EU-Richtlinie gilt auch für Organisationen, die keinen Sitz in der EU haben, sobald sie Waren oder Dienstleistungen in der EU anbieten oder auch nur Online-Marktforschung unter EU-Bürgern betreiben.

10.) Höhere Bußgelder: Verstößt eine Organisation gegen die Datenschutzbestimmungen, droht ein Bußgeld in Höhe von bis zu vier Prozent des Jahresumsatzes.

11.) Bürokratieabbau: Administrative Umstände wie Meldepflichten für Organisationen, die persönliche Daten verarbeiten, entfallen.

12.) Altersgrenze: Die rechtswirksame Anmeldung bei Internetservices wie Social Media soll Jugendlichen im Regelfall erst ab 16 Jahren möglich sein. Nationale Gesetze sollen laut Datenschutzverordnung hier aber Ausnahmen möglich machen

Bußgelder und Sanktionen
Die EU-Datenschutz-Grundverordnung enthält eigene Vorschriften zu Möglichkeiten für Bußgelder und Sanktionen. Diese würden auch bei Vereinen und Verbänden Anwendung finden mit empfindlichen Strafhöhen. Nationale Datenschutzbehörden werden dabei in ihren Kompetenzen gestärkt, so dass sie die neuen EU-Regeln besser umsetzen können. Unter anderem dürfen sie einzelnen Unternehmen verbieten, Daten zu verarbeiten und können bestimmte Datenflüsse sofort stoppen sowie Bußgelder gegen Organisationen verhängen, die bis zu vier Prozent der jeweiligen weltweiten Jahreseinkünfte oder 20.000.000,- € betragen. Darüber hinaus dürfen sie Gerichtsverfahren in Datenschutzfragen anstrengen

Datenportabilität
Diese Vorgabe ist neu. Mitgliedern oder Nutzern muss auf Wunsch deren Daten elektronisch in einem einfachen maschinenlesbaren Format zur Verfügung gestellt werden. Damit soll der Wechsel zu anderen Anbietern vereinfacht werden und beim neuen Verband oder Verein können die Stammdaten elektronisch eingespielt werden.

Auftragsdatenverarbeitung
In Deutschland definiert sich die Auftragsdatenverarbeitung als 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 zu berücksichtigen, Dienstleister für IT-Themen, Daten- und Aktenvernichter und z.B. Auslagerung von Diensten wie Seminaranmeldungen.

Betreiber von Webseiten
Betreiber von Webseiten 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 Diensteanbieters vorgibt.

Die Datenschutz-Grundverordnung wird zwangsläufig Auswirkungen auf die aktuellen Anforderungen an die sog. „Website-Compliance“ haben. Zwar bleiben viele gesetzliche Pflichten erstmal bestehen, andererseits sollten aber die jeweiligen Datenschutzerklärungen mit den Vorgaben der EU-DS-GVO abgestimmt werden.

Zusätzlich wird hier für Vereine und Verbände die 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.

Inhalte zur Website-Compliance – Datenschutzerklärung

- Facebook „Like“-Buttons oder ähnlicher Social-Plugins anderer Anbieter (Twitter, LinkedIn etc.),
- Webformulare (Kontaktformulare, Newsletter etc.),
- Cookies (Informationen zu Zweck, Empfänger der Daten etc.)
- Analyse-Tools (wie Piwik oder etracker) und

- Tageting- bzw. Audience Optimisation Tools (z. B. AddThis)

Anforderungen an eine Einwilligung
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.

Die Anforderungen an eine Einwilligung (informierte Einwilligung - DS-GVO Art. 4 Nr. 11) beinhalten:

- freie Entscheidung des Betroffenen
- ausführliche, erkennbare und bestimmte Information des Betroffenen
- Schriftform der Einwilligungserklärung
- Widerruflichkeit der Einwilligungserklärung
- Besondere Regeln für Minderjährige unter 16 Jahren

Datenschutzbeauftragter
Das Modell Datenschutzbeauftragter ist in Deutschland seit langem bekannt und viele Organisationen 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 (DS-GVO Art. 4 Nr. 2: Erheben, Speichern, Nutzen, Erfassen, Organisation, Ordnen, Anpassung, Veränderung, Auslesen, Abfragen, Verwendung, Weitergabe durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich, Verknüpfung, Einschränkung, Löschen, Vernichtung) personenbezogener Daten betraut sind.

Das trifft für die meisten Vereine zu, da nahezu jeder Abteilungsleiter Daten der Mitglieder verarbeitet wie oben dargestellt und ggf. sogar mit eigenen zusätzlichen Daten anreichert.

Aufgaben des Datenschutzbeauftragten

- Unterrichtung / Beratung der Verantwortlichen, der Auftragsverarbeiter und der Beschäftigten
- Überwachung der Einhaltung der DS-GVO und nationalen Sonderregelungen
- Sensibilisierung und Schulung
- Beratung und Überwachung im Zusammenhang mit der Datenschutz-Folgenabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde

Datensicherheit
Mit der DS-GVO 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 zum Schutze der Daten zu erfüllen.

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 Bundesdatenschutzgesetzes 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 Beschäftigten, Mitglieder, usw. mit den neuen Informationspflichten versorgt werden:

- Dauer der Speicherung
- Rechte der Betroffenen
- Widerrufbarkeit von Einwilligungen
- Beschwerderecht bei der Aufsichtsbehörde
- Verpflichtung zur Bereitstellung personenbezogener Daten
- Automatisierte Entscheidungsfindung und Profiling

Datenschutz-Folgenabschätzung
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.

Data Breach Notification – Benachrichtigung bei Verletzungen des Datenschutzes
Schon heute müssen Verantwortliche, unter bestimmten Voraussetzungen, Aufsichtsbehörde und Betroffenen eine Data Breach Notification 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.

Die Bedeutung der Data Breach Notification und deren Anzahl werden dadurch zwangsläufig steigen. Eine Datenschutzverletzung ist innerhalb von 72 Stunden der Aufsichtsbehörde zu melden. Die EU-DS-GVO macht dazu klare Vorgaben. Daher sollte ein Standard-Prozess in Vereinen und Verbänden dazu etabliert werden.

Data Breach Notification (Anzeigepflicht)

- Art. 33 DS-GVO - Meldungen an die Aufsichtsbehörde
- Art. 34 DS-GVO - Meldungen an die Betroffenen
- Risikoabwägung
- Ausnahmen ggf. bei Verschlüsselung
- Meldung innerhalb von 72 Stunden, sonst außerordentliche Begründung

Verzeichnis von Verarbeitungstätigkeiten
Mit der Datenschutz-Grundverordnung muss auch ein Verein oder Verband nach Art. 30 DS-GVO 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.

Aufbau eines Datenschutzmanagementsystems
Neben dem angesprochenen Verzeichnis von Verarbeitungstätigkeiten findet sich in der Datenschutz-Grundverordnung eine Vielzahl von Normen, die eine Dokumentierung der getroffenen Datenschutzmaßnahmen fordern. Daneben schafft die DS-GVO weitere Prozesse, die etabliert, und Aufgaben die wahrgenommen werden müssen. 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.

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.

Denn es gilt der Grundsatz „Speicherung höchsten so lange wie erforderlich“ (DS-GVO Art. 5 Abs. 1 lit. e):

- längere Speicherung nur wenn
- im öffentlichen Interesse liegende Archivzwecke
- wissenschaftliche Forschungszwecke
- historische Forschungszwecke
- für statistische Zwecke

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 bei Kindern und Jugendlichen
Der Kinder- und Jugendschutz nimmt in der EU-Datenschutz-Grundverordnung (DS-GVO) 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.

Rechte der Betroffenen
Die erweiterten Rechte der von Datenspeicherung betroffenen Personen beinhalten:

- Informationsrecht
- Auskunfts- und Widerspruchsrecht
- Recht auf Berichtigung, Löschung und Einschränkung
- Recht auf Datenübertragbarkeit

Handlungsempfehlungen
Aus den oben beschrieben Anforderungen ergeben sich für Verbände und Vereine die folgenden Übergruppen von Empfehlungen:

- Etablieren eines Managements für Datensicherheit oder Informationssicherheit
- Feststellen des Schutzbedarfes
- Bewertung von Risiken
- Treffen und Umsetzen der jeweiligen Maßnahmen
- Führen von Dokumentationen und Nachweisen

Liste der Hauptanforderungen an Verbände und Vereine
Zu den detaillierten Anforderungen an Verbände und Vereine gehören:

- Übersicht der Verarbeitungstätigkeit (Problem der Definition)
- Datenschutzfolgenabschätzung
- Überprüfung und Herbeiführung von Einwilligungen
- Transparenz- und Informationspflichten
- Speicherbegrenzung (Löschung)
- Datenportabilität
- Auskunftsersuchen
- Auftragsverarbeitung
- Widerspruch / Berichtigung / Einschränkung
- Technische und organisatorische Maßnahmen

Checkliste für Verbände und Vereine
Die folgende Checkliste beinhaltet wesentliche Schritte zur geforderten Datensicherheit.

I. Anforderungen an die Datenschutzorganisation im Verein:

1. Verankerung in der Satzung

- Allgemeine Regelungen zum Datenschutz im Verein
- Hinweis auf Datenschutzkonzept

2. Datenschutzkonzept

- Konkrete Maßnahmen zum Datenschutz
- Löschkonzept
- Technische und organisatorische Maßnahmen

Art. 5 Abs. 1 (f) DSGVO:
„Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (Integrität und Vertraulichkeit)".

3. IT Sicherheitskonzept

II. Die Schritte des Verbandes und Vereins auf dem Weg zur EU Datenschutz-Grundverordnung

- Sensibilisierung zum Thema Datensicherheit durchführen
- Bestandsaufnahme durchführen
- Verzeichnis der Verarbeitungstätigkeiten erstellen
- Rechtsgrundlagen prüfen (lassen) mit Rechtmäßigkeit der Datenerhebung und -verarbeitung
- Bereich personenbezogener Daten von Kindern besonders prüfen
- Betroffenenrechte und Informationspflichten umsetzen
- Datenschutzfolgeabschätzung implementieren
- Dokumentation organisieren – Datenschutzkonzept
- Verträge (Auftragsverarbeiter) überprüfen
- Melde– und Konsultationspflichten organisieren
- Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design" und „Privacy-by-Default") umsetzen

III. Die Rechte der von der Datenspeicherung Betroffenen sichern

- Recht auf Information über die Speicherung und transparente Kommunikation (Artt. 12/13 DS-GVO)
- Recht auf Löschung / Vergessen werden (Art. 17 DS-GVO)
- Recht auf Auskunft über gespeicherte Daten / Datenübertragbarkeit (Art. 20 DS-GVO)
- Recht auf Sperrung und Berichtigung / Einschränkung der Verarbeitung (Art. 18 DS-GVO)

IV. Die Informationspflichten von Verband und Verein

- Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person (Art. 13 DS-GVO)
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden (Art. 14 DS-GVO)
- Information über Bestellung eines Datenschutzbeauftragten (Art. 37 Abs. 7 DS-GVO)
- Information bei Datenpannen (Art. 33 DS-GVO)

Schlussbemerkung und Haftungsausschluss:
Es wird darauf hingewiesen, dass diese Zusammenstellung der wesentlichen Inhalte der DS-GVO im gegebenen Rahmen weder den Anspruch auf Vollständigkeit erheben noch die Hinzuziehung professioneller Unterstützung auf technischer und administrativer Ebene für Vereine und Verbände ersetzen kann.

Insofern ist eine Haftung des DDV für die in diesem Handout enthaltenen Informationen ausgeschlossen.

Auch wird darauf hingewiesen, dass gem. Art. 5 der EU-DS-GVO ein Verband oder Verein einen Nachweis im Rahmen seiner Rechenschaftspflicht über die Einhaltung der gesetzlichen Anforderungen zu erbringen hat.

Für Rückfragen steht der Datenschutzbeauftragte des DDV gerne zur Verfügung:

Telefon 0176/64197702
eMail: volker.bernardi@ddv-online.de

Mit freundlichen Grüßen

Volker Bernardi
DDV-Datenschutzbeauftragter