SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Häufig gestellte Fragen zum Datenschutz in Vereinen

Seit dem 25. Mai 2018 gilt die Europäische Datenschutz-Grundverordnung (DS-GVO) und das neue Bundesdatenschutzgesetz (BDSG 2018). Beide Vorschriften sind wie einige Spezialgesetze bei der Verarbeitung personenbezogener Daten durch Vereine unmittelbar anzuwenden. Gefordert sind hier Vorstände, ehren- und hauptamtliche Mitarbeiter, die personenbezogene Daten verarbeiten, sowie Datenschutzbeauftragte, soweit sie zu benennen sind (siehe unten 7.). Der Landesbeauftragte für den Datenschutz bietet hier Beratungshilfe an. Die Folgen von datenschutzrechtlichen Verstößen können gravierend sein. Was ist zur Einhaltung des Datenschutzes bzw. zur Vermeidung verwaltungsrechtlicher Maßnahmen und Bußgelder zu tun? Folgende zehn Fragen sind besonders wichtig:

1. Welche Daten sind zu schützen?

Geschützt sind personenbezogene Daten. Dies sind alle Einzelangaben über persönliche und sachliche Verhältnisse einer natürlichen Person, Art. 4 Nr. 1 DS-GVO. Dazu gehören z. B. Name, Adresse, Geburtsdatum, Bankverbindung, Kontaktdaten, Bildnisse, Hobbys und Leistungsdaten, z. B. von Sportlern. Besonders schützenswert sind besondere Kategorien personenbezogener Daten. Dies sind Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung, Art. 9 Abs. 1 DS-GVO.

Geschützt sind diese Daten, wenn sie automatisiert oder in geordneten Akten verarbeitet werden. „Verarbeiten“ meint als Oberbegriff jeden Vorgang im Zusammenhang mit den personenbezogenen Daten wie das Erheben, Ordnen, Speichern, Verändern, Auslesen, Übermitteln, Verbreiten oder den Abgleich.

2. Wer trägt im Verein welche Verantwortung?

Datenschutz ist Chefsache. Die Organisation und Gesamtverantwortung für den Datenschutz liegt beim Vorstand. Ihm obliegt es, Zuständigkeiten und Verantwortlichkeiten bezüglich des Datenschutzes festzulegen. Gegebenenfalls ist der Fortbildungsbedarf für den Datenschutzbeauftragten oder die Mitarbeiter, die die Datenverarbeitung durchführen, zu ermitteln. Die Mitarbeiter des Vereins sind dafür verantwortlich, dass die konkrete Ihnen übertragene Verarbeitung personenbezogener Daten entsprechend der Rechtslage erfolgt. Dazu sollten sie auf die Einhaltung des Datenschutzes verpflichtet werden. Näheres dazu finden Sie im Kurzpapier Nr. 19 der Datenschutzkonferenz[1]. Der Datenschutzbeauftragte schließlich berät zu Fragen des Datenschutzes und überwacht die Einhaltung.

3. Wann ist die Verarbeitung personenbezogener Daten grundsätzlich zulässig?

Bevor personenbezogene Daten verarbeitet werden, sollte die Zulässigkeit der Verarbeitung geprüft werden. Dabei ist folgender Grundsatz zu beachten: Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn eine gesetzliche Erlaubnisregelung dies gestattet oder eine informierte und freiwillige Einwilligung der betroffenen Person vorliegt, Art. 6 Abs. 1 DS-GVO.

Gemäß Art. 6 Abs. 1 Satz 1 lit. b DS-GVO ist die Verarbeitung im Verein zulässig, soweit personenbezogene Daten für die Mitgliederverwaltung bzw. den sich aus der Satzung ergebenden Vereinszweck erforderlich sind. Hierunter fallen z. B. Daten für die Mitgliederlisten oder Spielerpässe (Name, Adresse, vereinsbezogene Interessen, Meldung zu (Sport-) Veranstaltungen, Übermittlungen an die Liga, Rechnungs- und Spendendaten; weitere Daten, wenn auch sie erforderlich sind).

Darüber hinaus kann eine Verarbeitung gemäß Art. 6 Abs. 1 Satz 1 lit. f DS-GVO zulässig sein, wenn die berechtigten Interessen des Vereins die Interessen der betroffenen Personen überwiegen. Für die Verarbeitung personenbezogener Daten hauptamtlich Beschäftigter ist insbesondere § 26 BDSG 2018 zu berücksichtigen. Daten von Besuchern, Gästen, Kursteilnehmern etc. dürfen verarbeitet werden, soweit dies für den jeweiligen („vertragsähnlichen“)

[1] Soweit auf Kurzpapiere der Datenschutzkonferenz hingewiesen wird, finden Sie diese auf der Homepage des Landesbeauftragten unter http://lsaurl.de/Kurzpapiere

Zweck erforderlich ist (z. B. für Teilnehmer- oder Besucherlisten, sofern diese z. B. aufgrund des Verwendungsnachweises für Zuschüsse erforderlich sind). Sofern für die Erfüllung des Vereinszwecks erforderlich, können auch Newsletter an die Mitglieder versendet werden. Geschieht dies per E-Mail, sollte dies allerdings so erfolgen, dass kein Empfänger Kenntnis über die E-Mail-Adressen der anderen Empfänger erlangt (Versand als „Blindkopie“).

Für Verarbeitungen, die über die genannten Vorschriften hinausgehen (und nur dafür!), ist eine Einwilligung erforderlich. Einwilligungen sind nur wirksam, wenn sie freiwillig erfolgen, d. h. betroffene Personen sie verweigern können, ohne Nachteile zu erleiden. Zudem muss die betroffene Person auf die Widerrufsmöglichkeit hingewiesen werden. Einwilligungen von Kindern sind nur wirksam, wenn sie in der Lage sind, die Folgen der Verwendung ihrer Daten einzuschätzen und sich deshalb verbindlich dazu äußern können (Einwilligungsfähigkeit). Bei Kindern unter 14 Jahren ist dies regelmäßig zu verneinen. Im Online-Bereich können Kinder erst ab dem Alter von 16 Jahren wirksam einwilligen, Art. 8 DS-GVO. Sind Kinder nicht einwilligungsfähig, ist die Einwilligung der Sorgeberechtigten einzuholen.

Die Einwilligung muss nachgewiesen werden. Sie ist regelmäßig erforderlich für die Weitergabe von Mitgliederdaten bei Drittzwecken, z. B. zu Werbezwecken und an die allgemeine Gruppenversicherung, zur persönlichen Gratulation zu Geburtstagen, Hochzeitstagen und ähnlichen Anlässen.

Besondere Kategorien personenbezogener Daten dürfen nur unter den in Art. 9 Abs. 2 DS-GVO genannten Voraussetzungen (z. B. einer „ausdrücklichen“ Einwilligung) verarbeitet werden.

4. Was ist bei der Vereinshomepage zu beachten?

Die Vereinshomepage bedarf zunächst eines Impressums. Darüber hinaus ist aufgrund der Informationspflichten (siehe unten 6.) eine Datenschutzerklärung erforderlich, wenn mithilfe der Homepage personenbezogene Daten verarbeitet werden. Dies gilt z. B. bei der Verwendung von Webtracking-Tools wie Google Analytics oder Kontaktformularen. Im Internet werden hier einige Datenschutzhinweis-Generatoren angeboten, deren Verwendung für den Verein hilfreich sein kann. Werden durch Online-Formulare (Aufnahmeanträge, Anmeldungen zu Veranstaltungen) personenbezogene Daten erhoben, müssen die Informationspflichten direkt bei der Erhebung erfüllt werden, z. B. durch einen Link auf die Datenschutzerklärung. Zudem muss die Übertragung personenbezogener Daten, die in Online-Formulare eingetragen werden, verschlüsselt erfolgen. Derzeit entspricht die Verschlüsselung mithilfe des Protokolls TLS in Version 1.2 dem Stand der Technik.

Zur Veröffentlichung personenbezogener Daten auf der Homepage sollte Folgendes beachtet werden: Eine Veröffentlichung im Internet ist eine weltweite Bereitstellung dieser Daten. Die Daten können durch Jedermann ggf. auch für unlautere Zwecke recherchiert, genutzt und verändert werden. Daher ist die Veröffentlichung personenbezogener Daten im Internet grundsätzlich unzulässig, wenn die betroffene Person nicht ihre freiwillige und informierte Einwilligung erklärt hat. Ausnahmen bestehen für „dienstliche“ Kontaktdaten der Funktionsträger (Vorstand, Trainer) und für Daten von Vereinsmitgliedern im Zusammenhang mit Veranstaltungen (z. B. Spielergebnisse, Mannschaftsaufstellungen, Torschützen, persönliche Leistungen), soweit die Mitglieder informiert sind, die Veröffentlichung auf das erforderliche Maß befristet ist und keine entgegenstehenden Interessen der betroffenen Personen überwiegen. Letzteres kann der Fall sein, wenn belastende Umstände (Schlechtleistungen) hervorgehoben oder persönliche Gründe benannt werden.

5. Wann ist die Veröffentlichung von Fotos mit erkennbaren Personen zulässig?

Die Veröffentlichung von Fotos von Veranstaltungen, auf denen natürliche Personen erkennbar sind, ist zulässig, wenn sie zur Wahrung berechtigter Interessen erforderlich ist und keine Interessen der Abgelichteten überwiegen, Art. 6 Abs. 1 Satz 1 lit. f DS-GVO. Dies wird häufig der Fall sein bei der Veröffentlichung von Fotos von Veranstaltungen oder auch bei Mannschaftsfotos, sofern die Abgelichteten darüber informiert wurden. Generell sollte darauf geachtet werden, dass die Abgelichteten nicht unvorteilhaft dargestellt werden. Bei Veranstaltungen ist es ratsam, über die Veröffentlichung von Fotos zu informieren, z. B. schon im Eingangsbereich durch eine Informationstafel.

Liegen die Voraussetzungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO nicht vor, was insbesondere bei Portraitfotos der Fall sein kann, ist eine Einwilligung erforderlich (siehe Textvorschlag).

Bei der Veröffentlichung zu journalistischen Zwecken ist § 23 des Kunsturhebergesetzes zu berücksichtigen. Danach können z. B. Fotos veröffentlicht werden, auf denen Personen nur als Beiwerk erscheinen.

Textvorschlag für eine Einwilligungserklärung zur Veröffentlichung von Fotos im Internet

1) *„... Der Verein ... beabsichtigt, zur Vorstellung seiner Arbeitsgruppen in der Öffentlichkeit Fotografien anzufertigen, auf denen die Mitglieder erkennbar sein sollen und diese im Internet auf seiner Homepage für die Dauer eines Jahres zu veröffentlichen.*

2) *Wir weisen darauf hin, dass die Fotos mit der Veröffentlichung im Internet weltweit abrufbar sind. Eine Weiterverwendung oder Veränderung dieser Fotos durch Dritte kann daher nicht generell ausgeschlossen werden.*

3) *Zur Veröffentlichung im Internet wird die Einwilligung der abgelichteten Mitglieder benötigt. Die Einwilligung ist jederzeit widerrufbar. Durch den Widerruf wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt...*

4) *Ich habe den obigen Text zur Kenntnis genommen und willige freiwillig in die Veröffentlichung eines Fotos von mir für ein Jahr auf der Homepage des Vereins ein.*

... Name, Datum, Ort und Unterschrift des Mitglieds“

6. Welche Betroffenenrechte müssen gewahrt werden?

Die DS-GVO enthält in den Artikeln 12 bis 22 eine Fülle von Betroffenenrechten. Hier kurze Erläuterungen zu den Wichtigsten:

Wesentlich erweitert wurden die Informationspflichten, Art. 12 bis 14 DS-GVO, die ab der Erhebung personenbezogener Daten zu erfüllen sind. Näheres enthält das Kurzpapier Nr. 10 der Datenschutzkonferenz. Es ist empfehlenswert, die entsprechenden Informationen schon im Aufnahmebogen für die Vereinsmitgliedschaft zu berücksichtigen.

Nach dem Recht auf Datenübertragbarkeit müssen Daten auf Antrag der betroffenen Person ihr oder einem anderen in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden, wenn Verarbeitung automatisiert erfolgt und auf Einwilligung oder Vertrag (auch: Mitgliedschaft) nach Art. 6 Abs. 1 Satz 1 lit. b DS-GVO beruht.

Zudem hat die betroffene Person das Recht, in besonderen Situationen der Verarbeitung zu widersprechen, die u. a. auf einer Interessenabwägung nach Art. 6 Abs. 1 Satz 1 lit. f DS-GVO beruht. Folge des Widerspruchs ist, dass keine Weiterverarbeitung zulässig ist, es sei denn, das Überwiegen zwingender schutzwürdiger Gründe ist nachzuweisen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Personenbezogene Daten sind z. B. zu löschen, wenn sie für den Zweck, zu dem sie erhoben wurden, nicht mehr notwendig sind oder eine Einwilligung widerrufen wurde.

Beim Ausscheiden eines Vereinsmitglieds sollten seine Daten ordnungsgemäß gelöscht werden. Bei Wechsel der Funktionsträger ist eine Aktualisierung sicherzustellen. Hat der Verein zu löschende Daten zuvor öffentlich bekannt gemacht (z. B im Internet), muss er angemessene Maßnahmen treffen, um die Verantwortlichen, die diese Daten verarbeiten (Dachverbände?), zu informieren, dass die betroffene Person Löschung verlangt hat, Art. 17 DS-GVO.

Ergänzende Hinweise zu diesen und weiteren Betroffenenrechten finden Sie in den Kurzpapieren der Datenschutzkonferenz (siehe Fußnote S. 1).

7. Wann müssen Vereine einen Datenschutzbeauftragten benennen?

Vereine müssen einen Datenschutzbeauftragten benennen, wenn in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, § 38 Abs. 1 BDSG 2018. Zu diesen Personen zählen alle Personen, auch Ehrenamtliche, Vorstandsmitglieder, Praktikanten, Trainer etc. jeweils als „vollwertige“ Person. „Ständig“ heißt hier, dass die Person dauerhaft mit der Tätigkeit betraut ist, gleichwohl ihr nicht in engen Zeitabständen konkret nachgehen muss. Wer z. B. als Kassenwart monatlich die Zahlung der Mitgliedsbeiträge kontrolliert, ist ständig mit der Verarbeitung beschäftigt. Wer diese Tätigkeit nur vorübergehend als Vertreter ausführt, ist nicht „in der Regel“ damit betraut.

Weitere, selten auf Vereine zutreffende Voraussetzungen, bei deren Vorliegen ein Datenschutzbeauftragter zu benennen ist, enthalten Art. 37 Abs. 1 DS-GVO und § 38 Abs. 1 BDSG 2018.

8. Was muss hinsichtlich der Datensicherheit beachtet werden?

Es müssen technische und organisatorische Maßnahmen getroffen werden, die gemäß Art. 32 DS-GVO je nach Verarbeitung und Risiko einen angemessenen Schutz der Daten gewährleisten können. Dabei muss vor allem die Vertraulichkeit, Integrität und Verfügbarkeit der Daten sichergestellt werden.

Dies kann insbesondere durch den Einsatz von Sicherheitssoftware wie Firewalls und Antivirensystemen, das regelmäßige Einbringen von System- und Software-Updates, das Erstellen von Sicherungen (Backups), den Einsatz von Verschlüsselungslösungen und das Verwenden sicherer Passwörter geschehen. Außerdem sollten Speichermedien und Datenverarbeitungsgeräte für Dritte unzugänglich aufbewahrt werden.

Personenbezogene Daten sollten nicht leichtfertig und unnötig kopiert, bei außereuropäischen Cloud-Diensten gespeichert oder im Internet oder sozialen Netzwerken veröffentlicht werden, da die Gewähr für die korrekte Verarbeitung der Daten hierdurch eingeschränkt wird. Auch sollte darauf geachtet werden, sensible und umfangreiche Datenbestände nicht unverschlüsselt zu versenden oder zu transportieren.

Bei der Entsorgung von Speichermedien und Datenverarbeitungsgeräten ist darauf zu achten, diese mit entsprechenden Programmen vorher zu bereinigen. Beim sicheren Löschen werden Speichermedien komplett mit Zufallswerten überschrieben, was ein Wiederherstellen zuvor gespeicherter Daten unmöglich macht.

9. Welche Dokumentations-, Nachweis- und Meldepflichten sind zu beachten?

Werden personenbezogene Daten regelmäßig verarbeitet (was in wohl jedem Verein zutreffen dürfte), ist ein Verzeichnis von Verarbeitungstätigkeiten zu führen, welches der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen ist, Art. 30 DS-GVO. Hinweise zu diesem Verzeichnis und ein Vordruck als Word-Dokument sind auf der Homepage des Landesbeauftragten veröffentlicht:

http://lsaurl.de/VerzVerarb

Darüber hinaus ist der Verein für die Einhaltung der Grundsätze der Datenverarbeitung (Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit) im Rahmen der Rechenschaftspflicht nachweispflichtig, Art. 5 Abs. 2 DS-GVO.

Verletzungen des Schutzes personenbezogener Daten sind möglichst binnen 72 Stunden der Aufsichtsbehörde zu melden, Art. 33 DS-GVO. Eine Verletzung des Datenschutzes kann insbesondere vorliegen, wenn Unberechtigte Zugang zu personenbezogenen Daten erlangen (z. B. Diebstahl eines nicht verschlüsselten Laptops, auf dem sich die Mitglieder-Datenbank befindet). Ein Meldeformular ist abrufbar unter:

http://lsaurl.de/DSVerletzung

Besteht voraussichtlich ein hohes Risiko für die betroffene Person, ist sie unverzüglich zu benachrichtigen, Art. 34 DS-GVO. Dies liegt nahe, wenn Dritte z. B. zu Kontodaten Zugang hatten.

10. Was ist zu tun, wenn der Verein Daten durch Dienstleister verarbeiten lässt?

Einige Vereine nutzen für die elektronische Verwaltung der Vereinsdaten Dienstleister. Sofern diese auf Weisung des Vereins tätig werden, ist ein Vertrag über eine Auftragsverarbeitung nach Art. 28 DS-GVO erforderlich. Näheres erläutert das Kurzpapier Nr. 13 der Datenschutzkonferenz. Eine Formulierungshilfe für einen solchen Vertrag ist aufrufbar unter:

http://lsaurl.de/MusterAV

Ein besonderer Fall der Auftragsverarbeitung ist z. B. die Speicherung von personenbezogenen Daten in einer Cloud. Befindet sich der Speicher außerhalb der Europäischen Union bzw. des Europäischen Wirtschaftsraumes, ist eine Speicherung hier nur zulässig, wenn die Voraussetzungen der Art. 44 ff. DS-GVO vorliegen, z. B. für den Staat, in dem gespeichert werden soll, ein sog. Angemessenheitsbeschluss der Europäischen Kommission vorliegt.

Impressum

Herausgeber:
Der Landesbeauftragte für den Datenschutz Sachsen-Anhalt
Leiterstr. 9, 39104 Magdeburg
Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt .de

www.datenschutz.sachsen-anhalt.de

Stand: August 2018