



SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Häufig gestellte Fragen zum Datenschutz in Vereinen

Seit dem 25. Mai 2018 sind die Europäische Datenschutz-Grundverordnung (DS-GVO) und das neue Bundesdatenschutzgesetz (BDSG) anzuwenden, welches zuletzt im November 2019 geändert wurde. Die Vorschriften sind wie einige Spezialgesetze bei der Verarbeitung personenbezogener Daten durch Vereine unmittelbar anzuwenden. Gefordert sind hier Vorstände, ehren- und hauptamtliche Mitarbeiter¹, die personenbezogene Daten verarbeiten, sowie Datenschutzbeauftragte, soweit sie benannt wurden (siehe unten 8.). Der Landesbeauftragte für den Datenschutz hilft hier beratend.

Folgen von datenschutzrechtlichen Verstößen können gravierend sein. Was ist zur Einhaltung des Datenschutzes bzw. zur Vermeidung verwaltungsrechtlicher Maßnahmen und Bußgelder zu tun? Elf Fragen sind besonders wichtig:

¹ Genderhinweis: Aus Gründen der besseren Lesbarkeit wird in der Folge auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Inhalt

1. Welche Daten sind zu schützen?.....	3
2. Wer trägt im Verein welche Verantwortung?.....	3
3. Wann ist die Verarbeitung personenbezogener Daten grundsätzlich zulässig?.....	4
4. Herausgabe von Mitgliederlisten	6
5. Was ist bei der Vereinshomepage zu beachten?	6
6. Wann ist die Veröffentlichung von Fotos mit erkennbaren Personen zulässig?.....	8
7. Welche Betroffenenrechte müssen gewahrt werden?.....	10
8. Wann müssen Vereine einen Datenschutzbeauftragten benennen?.	12
9. Was muss hinsichtlich der Datensicherheit beachtet werden?.....	13
10. Welche Dokumentations-, Nachweis- und Meldepflichten sind zu beachten?.....	14
11. Was ist zu tun, wenn der Verein Daten durch Dienstleister verarbeiten lässt?.....	15
Impressum	16

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 Interessen, die Vereinsmitgliedschaft als solche 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 innerhalb des Vereins beim **Vorstand (§ 26 BGB)**. 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 Datenschutzkonferenz². Der Datenschutzbeauftragte schließlich berät zu Fragen des Datenschutzes und überwacht die Einhaltung. Die datenschutzrechtliche Verantwortlichkeit nach außen liegt beim **Verein als Organisation**. Bei Verstößen gegen datenschutzrechtliche Bestimmungen wird grundsätzlich der Verein (aufsichtsbehördlich) in die Verantwortung genommen.

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). Bei Dachverbänden ist darauf zu achten, ob auch die Mitglieder der Vereine selbst Mitglied im Dachverband sind.

Darüber hinaus kann eine Verarbeitung gemäß **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** zu

² Soweit auf Kurzpapiere der Datenschutzkonferenz hingewiesen wird, finden Sie diese auf der Homepage des Landesbeauftragten unter <http://Isaurl.de/Kurzpapiere>

berücksichtigen. Daten von Besuchern, Gästen, Kursteilnehmern etc. dürfen verarbeitet werden, soweit dies für den jeweiligen („vertragsähnlichen“) 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“).

Nach dem Grundsatz der **Datenminimierung (Art. 5 Abs. 1 lit. c DS-GVO)** dürfen immer nur „so wenig wie möglich“ personenbezogene Daten verarbeitet werden. Vorstände, Funktionsträger, Mitarbeiter, Vereinsmitglieder etc. dürfen deshalb im Verein immer nur **Zugriffsrechte** für diejenigen personenbezogenen Daten haben, die sie zur Aufgabenerfüllung bzw. zur Ausübung ihrer Rechte **unbedingt kennen** müssen.

Nicht erforderlich und deshalb **unzulässig** sind **öffentliche Aushänge über Streitigkeiten** mit (ehemaligen) Vereinsmitgliedern, wenn nachvollziehbar ist (z. B. durch Namensnennung), um welche konkreten Personen es sich handelt. Auch bei **Hausverboten** genügt generell die postalische Bekanntgabe gegenüber den Betroffenen und die vereinsinterne Mitgliederinformation.

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. Herausgabe von Mitgliederlisten

In bestimmten Fällen können Vereinsmitglieder das Recht haben, Namen und Anschriften anderer Mitglieder des Vereins zu erfahren. Beispielsweise könnte die Kenntnis dieser Daten zur Rechtsausübung nach § 37 BGB erforderlich sein. Verlangt ein Vereinsmitglied eine „**Mitgliederliste**“ ist genau zu **prüfen**, welche **Daten** das Mitglied nach den Umständen des konkreten Falles ausnahmsweise **unbedingt benötigt**, um das sich aus seiner Mitgliedschaft ergebende Recht auf Mitwirkung an der Willensbildung im Verein wirkungsvoll ausüben zu können.

5. Was ist bei der Vereinshomepage zu beachten?

Die Vereinshomepage bedarf zunächst eines **Impressums**. Darüber hinaus ist aufgrund der Informationspflichten (siehe unten 7.) 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. Helfen zur Erstellung einer **Datenschutzerklärung** auf der Homepage kann ein **Tool** des Landesbeauftragten für den Datenschutz Baden-Württemberg, welches er unter

<https://www.baden-wuerttemberg.datenschutz.de/ds-gvo.clever/#vereine> zur Verfügung stellt. Werden durch Online-Formulare (Aufnahmeanträge, Anmeldungen zu Veranstaltungen oder auch durch Webtracking-Tools) 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.

Die Einbindung von **Trackingtools** zur Analyse des Nutzerverhaltens, insbesondere, wenn dies webseitenübergreifend erfolgt und die Daten an Dritte zu deren eigenen Zwecken weitergegeben werden, ist nur mit vorheriger **Einwilligung** der Nutzer zulässig. Das gilt sowohl für Trackingtools, die Cookies setzen als auch für das sogenannte Device Fingerprinting. Dabei werden Informationen über das vom Nutzer verwendete Gerät gesammelt (z. B. Marke, Modell, Betriebssystem, Browser, verwendete Software), um so einen eindeutigen digitalen Fingerabdruck zu speichern und wiedererkennen zu können. Die Einwilligung wird in der Regel nach **§ 25 Abs. 1 Satz 1 TTDSG** erforderlich sein. Ihr Inhalt muss die Anforderungen von **Art. 7 DS-GVO** erfüllen. Soweit Trackingtools verwendet werden, die personenbezogene Daten der Nutzer in Länder außerhalb Europas übermitteln, kann dies datenschutzrechtlich problematisch oder sogar unzulässig sein.

Weitere Informationen zu diesem Thema finden Sie in der **Orientierungshilfe** der Aufsichtsbehörden für Anbieter von **Telemedien** ab dem 1. Dezember 2021 unter <https://lsaur.de/OHTelemedien>.

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.

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

Die Veröffentlichung von Fotos, auf denen natürliche Personen erkennbar sind, ist zulässig, wenn sie zur Wahrung **berechtigter Interessen erforderlich** ist und **keine überwiegenden** Interessen der Abgelichteten der Veröffentlichung **entgegenstehen**, **Art. 6 Abs. 1 Satz 1 lit. f DS-GVO**. Dies wird häufig der Fall sein, wenn die einzelne abgelichtete Person nur als **Beiwerk** erscheint, insbesondere im Rahmen der Darstellung von öffentlichen **Veranstaltungen** oder auch bei **Mannschaftsfotos**. Generell sollte darauf geachtet werden, dass die Abgelichteten **nicht unvorteilhaft** dargestellt werden. Dies gilt insbesondere bei der Darstellung von Kindern. Zum Widerspruch gegen die Veröffentlichung von Fotos gemäß **Art. 21 DS-GVO** siehe Nr. 7.

Liegen die Voraussetzungen des Art. 6 Abs. 1 Satz 1 lit. f DS-GVO nicht vor, ist eine **Einwilligung** erforderlich (siehe Textvorschlag). Dies ist z. B. bei **Portraitfotos** der Fall und regelmäßig, wenn Fotos von **vereinsinternen Veranstaltungen**, z. B. Mitgliederversammlungen veröffentlicht werden sollen.

Widerruft die abgelichtete Person die Einwilligung, muss die Veröffentlichung für die Zukunft unterbleiben.

Zudem muss der Verein seine **Informationspflichten** erfüllen (s. u. Nr. 7), bei Veranstaltungen z. B. durch Aufstellen einer Info-Tafel im Eingangsbereich.

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“

7. 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:

Wichtig ist zunächst die Erfüllung der **Informationspflichten, Art. 12 bis 14 DS-GVO**, die ab der Erhebung personenbezogener Daten gelten. Näheres enthält das Kurzpapier Nr. 10 der Datenschutzkonferenz. Es ist empfehlenswert, die entsprechenden Informationen schon im **Aufnahmebogen** für die **Vereinsmitgliedschaft** zu berücksichtigen. Ein Muster für die Erfüllung der Informationspflichten anlässlich der Erhebung bei der betroffenen Person (insbesondere zur Nutzung auf Veranstaltungen) finden Sie unter:

<http://Isaurl.de/InfopflichtFoto>.

Nach **Art. 15 Abs. 1 DS-GVO** hat eine betroffene Person das **Recht auf Auskunft**, ob und inwieweit ihre Daten verarbeitet werden, damit sie anschließend die Rechtmäßigkeit der Datenverarbeitung überprüfen und/oder weitere Betroffenenrechte ausüben kann. Auf Verlangen ist der betroffenen Person auch eine **Kopie** ihrer Daten zur Verfügung zu stellen (**Art. 15 Abs. 3 DS-GVO**).

In der Auskunft ist genau anzugeben, welche Einzeldaten verarbeitet werden, z. B. die konkrete Schreibweise des verarbeiteten Namens (Maier, Meier oder Meyer), der E-Mail-Adresse, der Telefonnummer, der postalischen Anschrift etc.

Weitere Informationen sind dem Kurzpapier Nr. 6 der Datenschutzkonferenz, abrufbar unter <https://Isaurl.de/Kurzpapiere>, und den Leitlinien des Europäischen Datenschutzausschusses, abrufbar unter <https://Isaurl.de/EDSA012022>, zu entnehmen. Ein Muster für eine Auskunftserteilung befindet sich unter:

<https://Isaurl.de/MusterAuskunft>.

Nach dem Recht auf **Datenübertragbarkeit** müssen Daten auf Antrag der betroffenen Person ihr oder einem anderen in einem strukturierten, gängi-

gen 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 gemäß **Art. 21 Abs. 1 DS-GVO** das **Recht**, in besonderen Situationen (z. B. einer besonderen Gefahrenlage) 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. Bezüglich des **Zwecks** muss der Verein festlegen, welche Arten von Daten bis zu welchem **Ereignis** (z.B. Austritt aus dem Verein) oder für welche **Dauer** verarbeitet werden. Dies kann entweder in der **Vereinsatzung**, in einer **Datenschutzordnung** oder in einem **Datenlöschkonzept** erfolgen.

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).

8. Wann müssen Vereine einen Datenschutzbeauftragten benennen?

Vereine müssen einen Datenschutzbeauftragten benennen, wenn in der Regel **mindestens 20 Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, **§ 38 Abs. 1 BDSG**. 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. Wer als Übungsleiter keine personenbezogenen Aufzeichnungen tätigt, wird bei den 20 Personen nicht mitgezählt. Die Übungsleiter, die regelmäßig z. B. Leistungsdaten oder andere personenbezogene Daten Ihrer Übungsgruppe elektronisch speichern, sind allerdings mitzuzählen.

Weitere, auf Vereine **eher selten** zutreffende Voraussetzungen, bei deren Vorliegen ein Datenschutzbeauftragter zu benennen ist, enthalten **Art. 37 Abs. 1 DS-GVO** und **§ 38 Abs. 1 Satz 2 BDSG**.

Mehrere Vereine können denselben Datenschutzbeauftragten benennen, soweit kein Interessenskonflikt besteht. Dieser wäre z. B. anzunehmen, wenn ein Dachverband im Rahmen einer Auftragsverarbeitung die Mitgliederverwaltung für einen angeschlossenen Verein vornimmt. Hier sollten Dachverband und der dem Dachverband angeschlossene Verein unterschiedliche Datenschutzbeauftragte benennen.

9. 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.

10. 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://lsaur.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://lsaur.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 von Mitgliedern Zugang hatten.

11. 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://lsaur.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 des Landes Sachsen-Anhalt
Otto-von-Guericke-Str. 34a, 39104 Magdeburg

Tel.: (0391) 81803-0

poststelle@lfd.sachsen-anhalt.de

www.datenschutz.sachsen-anhalt.de



Stand: April 2023