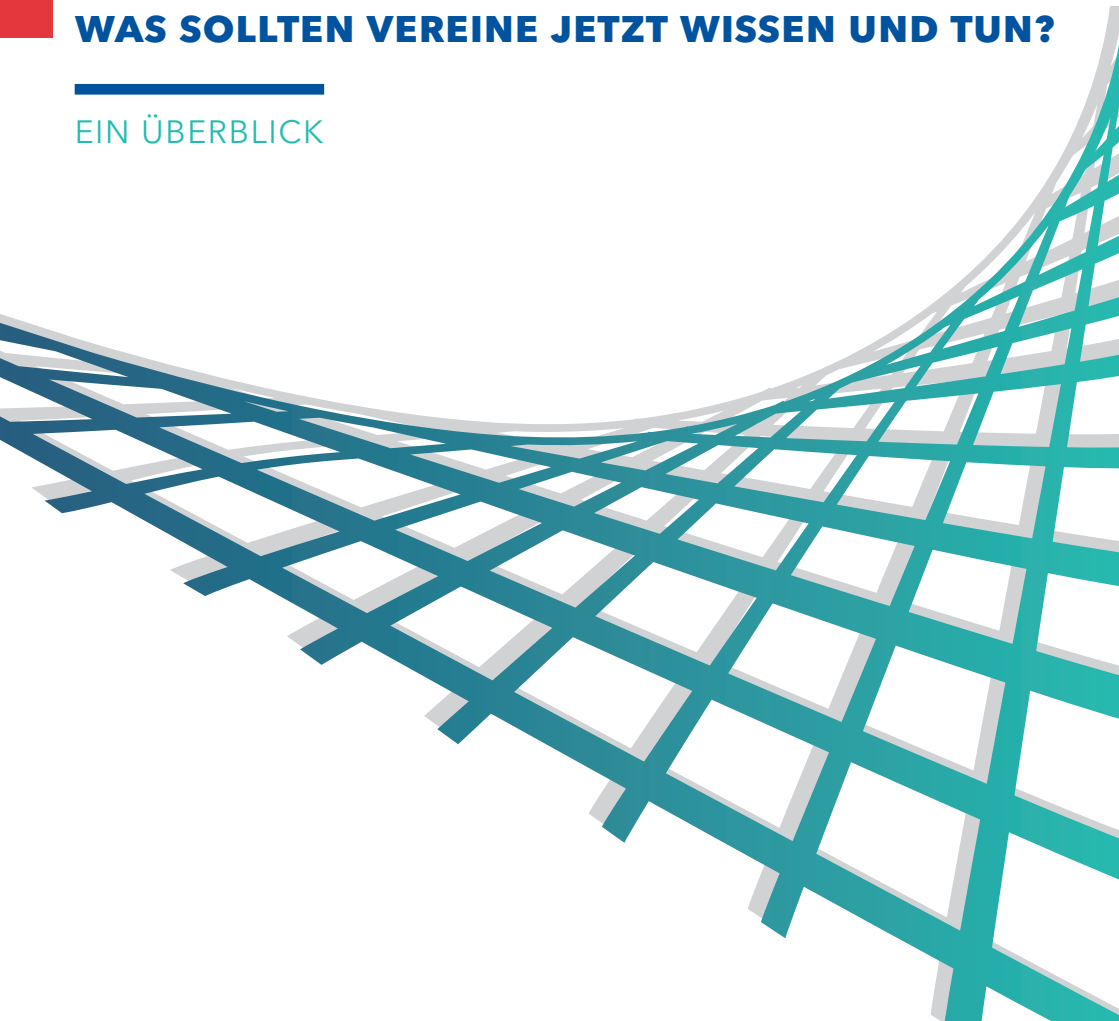
Hessische Landesregierung

HESSEN

DIE **NEUE**
EUROPÄISCHE DATENSCHUTZ-GRUNDVERORDNUNG

WAS SOLLTEN VEREINE JETZT WISSEN UND TUN?

EIN ÜBERBLICK



Seit dem 25.05.2018 gilt die Datenschutz-Grundverordnung (DS-GVO) in den Staaten der Europäischen Union. Das neu konzipierte Bundesdatenschutzgesetz ergänzt die unmittelbar geltende DS-GVO um die Bereiche, in denen die EU-Verordnung den Mitgliedstaaten Gestaltungsspielräume lässt.

Die DS-GVO lehnt sich in weiten Bereichen an das bisher geltende deutsche Datenschutzrecht an, so dass mit ihr eine vollständige Neuerung des Datenschutzrechts nicht verbunden ist. Schon in der Vergangenheit mussten eingetragene und nicht eingetragene Vereine den Datenschutz daher beachten. Unabhängig davon, ob die Vereinsverantwortlichen bislang den Schutz von Daten im Blick hatten oder nicht: Spätestens jetzt sollten sie sich mit dem Datenschutz im Verein und den Regelungen der DS-GVO auseinandersetzen.

Die DS-GVO hat sich zum Ziel gesetzt, die Grundrechte und Grundfreiheiten natürlicher Personen zu schützen, insbesondere deren Recht auf Schutz **personenbezogener** Daten. Auf der anderen Seite soll aber der freie Verkehr von Daten innerhalb der EU nicht eingeschränkt werden (Artikel 1 DS-GVO).

Wenn im Folgenden Artikel (Art.) ohne Gesetz genannt werden, sind Artikel der DS-GVO gemeint.

1

Was sind personenbezogene Daten?

Das sind alle Informationen, die sich auf einen identifizierten oder identifizierbaren Menschen (natürliche Person) beziehen (Art. 4 Nr. 1). Einige Beispiele: Name, Adresse, Familienstand, Geburtsdatum, Staatsangehörigkeit, Vertrags- und Besitzverhältnisse, Beruf, Partei- und Vereinsmitgliedschaften, Überzeugungen, Aussehen, Eigenschaften, Krankheiten. Man sieht also, dass sämtliche Informationen gemeint sind, die einen Menschen und seine Lebensumstände beschreiben. Es genügt, dass die Person identifizierbar ist. So beinhaltet etwa das Autokennzeichen die personenbezogene Information über den Halter des Fahrzeugs, mag dieser bekannt oder von Polizei oder Versicherung zu ermitteln sein.

2

Die DS-GVO regelt die Verarbeitung personenbezogener Daten – auch durch Vereine, ob ins Vereinsregister eingetragen oder nicht. **Was ist unter Verarbeitung zu verstehen?**

Verarbeitung umfasst die gesamte Bandbreite dessen, was mit Daten gemacht werden kann: Erheben, Erfassen, Organisation, Ordnen, Speicherung, Anpassung oder Veränderung, Auslesen, Abfragen, Verwendung, Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, Abgleich oder Verknüpfung, Einschränkung, Löschen oder Vernichtung, also letztlich jede Form der Verwendung und Nutzung von personenbezogenen Daten (Art. 4 Nr. 2).

Dabei ist nicht allein der **automatisierte** (digitale) Umgang mit Daten gemeint. Vielmehr gilt die DS-GVO auch für die **nichtautomatisierte** Verarbeitung personenbezogener Daten, die in einem Dateisystem (Art. 4 Nr. 6) gespeichert sind oder gespeichert werden sollen (Art. 2 Abs. 1). Damit sind personenbezogene Daten gemeint, die in einer geordneten Sammlung aufbewahrt und nach bestimmten Kriterien zugänglich oder auffindbar sind.

Beispiel: Ein Verein nutzt für seine Mitgliederverwaltung keine EDV, sondern ein Karteikartensystem, in dem die Mitglieder alphabetisch oder nach Nummern

geordnet und zugänglich sind. Ein Verein würde nur dann der DS-GVO „entfliehen" können, wenn seine Mitgliederverwaltung gänzlich unstrukturiert und ungeordnet wäre. Dies kann man aber sicher in der Praxis ausschließen. Häufig nutzen Vereine sowohl die automatisierte wie die nichtautomatisierte Form der Datenverarbeitung, etwa wenn ein schriftlicher Aufnahmeantrag Verwendung findet, der nach Vereinseintritt in einem Ordner abgeheftet wird, während die abgefragten Daten in die elektronische Mitgliederdatenbank eingegeben werden.

Fazit: Die DS-GVO gilt für jede automatisierte sowie nichtautomatisierte Verwendung personenbezogener Daten. Die Person, deren Daten verarbeitet werden, heißt im Sprachgebrauch der DS-GVO „betroffene Person" (Art. 4 Nr. 1).

3

Wann ist die Verarbeitung personenbezogener Daten erlaubt?

Die Verarbeitung personenbezogener Daten ist beispielsweise rechtmäßig, wenn …

- … die Verarbeitung für die **Erfüllung eines Vertrags** mit der betroffenen Person oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen (Art. 6 Abs. 1 b) oder
- … die Verarbeitung ist zur Wahrung der **berechtigten Interessen** des Verantwortlichen (Verein) erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt (Art. 6 Abs. 1 f).
- … die betroffene Person ihre **Einwilligung** gegeben hat (Art. 6 Abs. 1 a)

Es gibt noch weitere Gründe, aber die hier Genannten dürften die für Vereine in der Praxis relevantesten sein. Hierauf wird im Folgenden näher eingegangen:

a.

Was hat die Erfüllung eines Vertrages mit Vereinen zu tun?

Zum einen können Vereine in die Erfüllung von Verträgen wie jede andere Person eingebunden sein, z.B. bei Kauf- oder Mietverträgen oder auch bei Dienstverträgen, wie dies z.B. gegenüber Übungsleitern oder Mini-Jobbern der Fall ist. Hier dürfen die Daten des/der Vertragspartner(s) verarbeitet werden, soweit dies für die Durchführung des jeweiligen Vertrages erforderlich ist.

Zum anderen ist auch die Mitgliedschaft in einem Verein als gegenseitiges Vertragsverhältnis anzusehen. Das Mitglied hat gegenüber dem Verein ebenso Rechte und Pflichten wie der Verein gegenüber dem Mitglied. Zu nennen sind etwa die Pflicht zur Beitragszahlung einerseits sowie das Recht zur Nutzung der Vereinseinrichtungen andererseits. Auch ist der Verein verpflichtet, im Interesse seiner Mitglieder die satzungsgemäßen Vereinszwecke und -ziele zu verfolgen, denn aus diesem Grund sind die Mitglieder in den Verein eingetreten. Daraus ist zu folgern, dass der Verein die personenbezogenen Daten seiner Mitglieder verarbeiten darf, soweit dies für die Erfüllung des Mitgliedschaftsvertrages sowie der Satzungszwecke erforderlich ist.

Ähnlich verhält es sich mit den vorvertraglichen Maßnahmen, die auf Anfrage der betroffenen Person erfolgen. Diese Maßnahmen gehen dem Mitgliedschaftsverhältnis voraus, was etwa der Fall ist, wenn eine Person sich an den Verein wendet, weil sie Interesse an einer Mitgliedschaft hat. Soweit die Verarbeitung personenbezogener Daten in diesem Zusammenhang erforderlich ist, darf sie vorgenommen werden.

Zusammenfassend kann man sagen:

Die Datenverarbeitung im Verein ist rechtmäßig, wenn und soweit dies für die Begründung der Mitgliedschaft oder die Mitgliederverwaltung und zur Erfüllung der Vereinszwecke unbedingt erforderlich ist, so dass ohne diese Verarbeitung ein geregeltes Funktionieren des Vereins nicht möglich wäre.

Für welche Daten gilt das?

Ein Verein kann üblicherweise auf folgende Daten nicht verzichten:

- Name und Anschrift des Mitglieds;
- Eintrittsdatum;
- Funktionen im Verein, aktive oder passive Mitgliedschaft, Abteilungszugehörigkeit;
- Telefonnummern und E-Mail-Adressen von Vorstandsmitgliedern und Funktionsträgern.

Die Notwendigkeit der Verarbeitung folgender Daten hängt vom Satzungszweck bzw. der Satzungsgestaltung ab:

- Bankverbindung bei ausschließlichem Bankeinzug des Beitrags gemäß Satzung;
- E-Mail-Adressen von Mitgliedern ohne Funktion, wenn die Satzung Kommunikation per E-Mail vorsieht;
- Geburtsdatum, wenn dies für die Erfüllung des Satzungszwecks (z.B. Altersklassen im Sport) oder der satzungsgemäßen Mitgliederrechte (z.B. Stimmrecht erst ab Volljährigkeit oder einem anderen bestimmten Alter, unterschiedliche Beitragsstufen nach Alter) erforderlich ist.

Warum besteht hier eine Abhängigkeit von der Satzung bzw. vom Satzungszweck?

Nehmen wir an, laut Satzung kann der Beitrag nach Wahl des Mitglieds auch per Überweisung oder bar gezahlt werden: Dann besteht keine unbedingte Notwendigkeit, die Bankverbindung preiszugeben.

Aber wenn jemand z. B. im Aufnahmeantrag die Bankverbindung mitteilt, dann geschieht dies doch immer freiwillig, also mit Einwilligung?

Nein, das ist nicht richtig. Von Freiwilligkeit kann keine Rede sein, wenn die betroffene Person eine Angabe in der falschen Annahme macht, die betreffende Information sei für die Erfüllung des Mitgliedschaftsvertrages gemäß der Satzung erforderlich (Art. 7 Abs. 4).

Das Problem lässt sich dadurch lösen, dass das Mitglied etwa wie folgt informiert wird:

Muster: *Die Angabe der Bankverbindung ist freiwillig und nicht erforderlich für den Eintritt in den Verein. Für den Verein würde es die Beitragsverwaltung erheblich vereinfachen und wäre daher wünschenswert, wenn Sie Ihre Bankverbindung angeben und sich mit dem Bankeinzug des Beitrags einverstanden erklären würden. Aber dies ist keine Voraussetzung für die Aufnahme in den Verein.*

Entsprechend ist zu verfahren, wenn die Satzung keine Kommunikation per E-Mail kennt oder sich kein satzungsgemäßer Grund für die Angabe des Geburtsdatums findet. Der verständliche Wunsch, einem Mitglied zum Geburtstag gratulieren zu wollen, findet dann keinen Rückhalt in der Satzung.

Allerdings erfassen Vereine nicht nur Daten ihrer Mitglieder, sondern auch von Nichtmitgliedern (z.B. Eltern von Minderjährigen, Übungsleitern, Minijobbern, Teilnehmer an Veranstaltungen). Auch dies muss einer Prüfung unter Berücksichtigung des Vereinszwecks oder des jeweiligen Vertragsverhältnisses (z.B. Vertrag mit Übungsleiter oder Minijobber, s.o.) standhalten.

b.

Was bedeutet die in (Art. 6 Abs. 1 f) vorgesehene Abwägung von Interessen?

Der Verein darf Daten verarbeiten, wenn seine berechtigten Interessen mindestens genauso wichtig sind wie die Interessen und Rechte der betroffenen Person. Überwiegt jedoch die Schutzbedürftigkeit der betroffenen Person, besonders deren Rechte auf Schutz ihrer Privatsphäre, darf der Verein seine Datenverarbeitung nicht auf diese Klausel stützen.

Diese nicht immer leichte Abwägung hat vor allem Bedeutung, wenn ein Verein Daten von Nichtmitgliedern verwendet, mit denen kein Vertrag besteht.

c.

Wozu dürfen die erhobenen Daten verwendet werden?

Zum einen vereinsintern im Rahmen der Mitglieder- oder Vereinsverwaltung, also zum Zwecke des Funktionierens des Vereins nach innen. Hierbei entstehen üblicherweise keine Probleme.

Dürfen die Daten denn aber auch an andere weitergegeben werden, also etwa in der Vereinszeitung oder im Internet veröffentlicht werden?

Dies betrifft die Übermittlung von Daten an „Dritte" (Art. 4 Nr. 10). Darunter versteht man

- jede natürliche oder juristische Person außerhalb des Vereins (z. B. einen übergeordneten Dachverband), auch die Öffentlichkeit oder eine unbegrenzte Anzahl von Personen (z.B. bei Veröffentlichung auf der Homepage oder in der Vereinszeitung);
- jede Person im Verein, die für die jeweilige Verarbeitung nicht befugt, also für die Einsicht in die Daten oder deren Weitergabe nicht zuständig ist (z.B. solche Vereinsmitglieder, die keine Funktion im Verein haben oder die nach ihrer Funktion mit den Daten oder einem Teil der Daten nicht arbeiten müssen).

Die Übermittlung von Daten an Unbefugte im Verein ist unzulässig, es sei denn die eigentlich unbefugten Personen können im konkreten Fall ein Recht geltend machen. Macht ein Mitglied glaubhaft, dass es die Mitgliederliste zur Wahrnehmung seiner satzungsgemäßen Rechte (z.B. Minderheitenrechte, Teilnahmerechte) benötigt, wird ihm eine Datei der notwendigen Daten gegen die schriftliche Versicherung ausgehändigt, dass Namen, Adressen und sonstige Daten nicht zu anderen Zwecken Verwendung finden und die erhaltenen Daten, sobald deren Zweck erfüllt ist, zurückgegeben, vernichtet oder gelöscht werden. Dies gilt auch beim sog. Sekretariatsmodell.

Daten dürfen an andere juristische oder natürliche Personen sowie an die Öffentlichkeit weitergegeben werden, wenn dies durch den Vereinszweck gedeckt ist.

- Dies betrifft etwa Meldungen von Sportvereinen an einen **Dachverband**, sofern dies für die Durchführung und Organisation des Sportbetriebs oder für die Erlangung von Lizenzen und Spielerpässen notwendig ist.
- Daneben dürfen Daten im Zusammenhang mit öffentlichen Vereinsveranstaltungen (Ankündigungen, Berichte, Ergebnislisten, Fotos) auf der Homepage oder in sozialen Medien veröffentlicht werden. Hier spielt einerseits das Recht des Vereins auf Öffentlichkeitsarbeit eine Rolle und andererseits, dass die betroffenen Personen (Zuschauer, Mitwirkende oder Sorgeberechtigte von Minderjährigen) mit der Veröffentlichung von Berichten und Fotos rechnen müssen. Trotz dieser Erwartungshaltung sollte aber vor allem auf die beabsichtigte Erstellung von Fotos und den damit verbundenen Zweck (z.B. Veröffentlichung von Fotos auf der Homepage oder in sozialen Medien) deutlich hingewiesen werden, etwa vor dem Ticketkauf, im Rahmen der der Anmeldung oder durch Aushang.

Was gilt bei Fotos?

Für Fotos besteht allerdings seit vielen Jahren eine besondere Rechtsgrundlage in den §§ 22, 23 Kunsturhebergesetz (KUG). Dieses Gesetz und die dazu ergangene Rechtsprechung haben im Ergebnis die Verbreitung von Fotos von Teilnehmern und Zuschauern an öffentlichen Veranstaltungen meist erlaubt. Ob die §§ 22, 23 KUG neben der DS-GVO fortbestehen oder künftig allein die DS-GVO anwendbar sein wird, ist aber rechtlich umstritten. Nach Meinung z. B. der Bundesbeauftragten für den Datenschutz, des Hessischen Datenschutzbeauftragten und des Bundesinnenministeriums gelten die §§ 22, 23 KUG auch weiterhin. Das bedeutet: Für die Veröffentlichung eines Fotos, auf dem Personen erkennbar sind, benötigt man grundsätzlich die Einwilligung der erkennbaren Personen (Recht am eigenen Bild). Ausnahmen u.a.: Die Fotos zeigen ein zeitgeschichtliches Ereignis oder eine Versammlung. Diese Ausnahmen können meist auf öffentliche Vereinsveranstaltungen angewendet werden (z.B. Sportwettkampf, Vereinsfest). Auch sollte bedacht werden, die Veröffentlichung zeitlich zu begrenzen. Besteht nämlich kein Informationsinteresse mehr, sind die Informationen zu löschen.

Ergänzung

Selbst wenn man die Ansicht verträte, dass das KUG von der DS-GVO abgelöst worden sein sollte, würde das aber keineswegs heißen, dass Fotos nur noch mit Einwilligung aller betroffenen Personen zulässig wären. Denn hier würde die oben dargestellte Abwägung (Art. 6 Abs. 1 f) eingreifen. Die Interessen des Vereins liegen auf der Hand: Die Öffentlichkeitsarbeit des Vereins ist ein wichtiger Bestandteil des jeweiligen Vereinszwecks zur Außendarstellung und Gewinnung neuer Mitglieder. Auch muss zugunsten der Vereine berücksichtigt werden, dass im Rahmen einer öffentlichen Veranstaltung meist bestimmte Daten (z. B. Namen der Mitwirkenden) ohnehin unweigerlich öffentlich werden, so dass auch deshalb der weiteren Verbreitung keine rechtlichen Hindernisse mehr im Wege stehen. Würde man Fotos von Vereinsveranstaltungen von einer Einwilligung der Mitwirkenden und Zuschauer abhängig machen, wäre die Berichterstattung und damit die Öffentlichkeitsarbeit der Vereine nahezu unmöglich. Demgegenüber haben Teilnehmer und Zuschauer bei öffentlichen Veranstaltungen keine überwiegenden Interessen, die ein Verbot von Fotos rechtfertigen können, zumal sie beim Besuch von solchen Veranstaltungen mit der Berichterstattung in Wort und Bild rechnen müssen. Sollte dies im Einzelfall anders sein, darf erwartet werden, dass sie der Veranstaltung fernbleiben oder dem Verein ihre Interessen im Einzelnen schildern, damit der Verein eine konkrete Interessenabwägung treffen kann.

Diese Abwägung gilt auch für die sonstige Berichterstattung ohne Fotos sowie im Sportbereich etwa für die Veröffentlichung von Ergebnislisten.

- Bei **internen Vereinsveranstaltungen** ist die Situation anders. Hier bedarf es einer Einwilligung der betroffenen Personen, wenn der Verein Fotos im Internet veröffentlichen will. Die Frage nach einer Einwilligung bzw. deren Erlangung dürfte hier auch kein unlösbares Problem sein.
- Soweit sich aus dem Satzungszweck keine Notwendigkeit der Weitergabe oder Veröffentlichung ableiten lässt (z.B. bei Ehrungen und Gratulationen, Weitergabe aus wirtschaftlichen Gründen, wie etwa beim Sponsoring) bedarf es einer **Einwilligung** der betroffenen Person.

d.

Welche Voraussetzungen müssen bei einer Einwilligung (Art. 4 Nr. 11, Art. 7) erfüllt sein, damit diese rechtswirksam ist?

- Eine Einwilligung ist eine freiwillige Entscheidung.
- Es bedarf der vorherigen Aufklärung über den Zweck der Datenverarbeitung
- Es muss auf die Widerrufsmöglichkeit sowie die Folgen einer Verweigerung der Einwilligung hingewiesen werden. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
- Der Verein ist beweispflichtig für die Einwilligung.
- Die Einwilligung kann schriftlich oder elektronisch (z. B. per E-Mail) erteilt werden.
- Das Ersuchen um Einwilligung muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von anderen Sachverhalten in dem gleichen Text klar zu unterscheiden ist (z. B. durch besondere Hervorhebung im Text).

4

Gelten die oben genannten Grundsätze für alle Daten?

Nein, besonders sensible Daten werden besonders geschützt (Art. 9):

Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

Ausnahmsweise erlaubt ist die Datenverarbeitung u.a., wenn

- eine Einwilligung der betroffenen Person vorliegt;
- die Datenverarbeitung sich nur auf Mitglieder oder ehemalige Mitglieder eines gemeinnützigen Vereins bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden
- die Verarbeitung sich auf personenbezogene Daten bezieht, die die betroffene Person offensichtlich öffentlich gemacht hat.
- wenn die Datenverarbeitung zur Geltendmachung und Ausübung von Rechtsansprüchen erforderlich ist.

5

Wie muss ein Verein die Datensicherheit in technischer und organisatorischer Hinsicht gewährleisten?

Die DS-GVO legt nicht im Einzelnen fest, welche konkreten Maßnahmen ein Verein treffen muss, um die in seiner Obhut befindlichen Daten vor Eingriffen Unbefugter und Verlust zu schützen (Art. 32). Vielmehr beschränkt sich die Regelung auf Zielsetzungen und Rahmenbedingungen. Sie verlangt u.a. ein dem Risiko angemessenes Schutzniveau unter Berücksichtigung des Stands der Technik und der Kosten sowie der Verarbeitungszwecke und der Eintrittswahrscheinlichkeit und Schwere des Risikos. Als Beispiele werden genannt:

- Verschlüsselung von Daten;
- Sicherung der Vertraulichkeit und Belastbarkeit der Systeme;
- Fähigkeit zur raschen Wiederherstellung der Daten nach einem physischen oder technischen Zwischenfall;
- Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen.

Vor diesem Hintergrund muss jeder Verein selbst entscheiden, welche Maßnahmen für ihn in Betracht kommen. Das Neueste und Teuerste muss es nicht sein, wohl aber müssen die Daten so gut geschützt werden, dass Verstöße gegen die DS-GVO

(vor allem Eingriffe durch unbefugte Personen oder Datenverluste) aller Wahrscheinlichkeit nach ausgeschlossen sind, wobei besonders sensible Daten (z. B. Gesundheitsdaten) den besten Schutz verdienen. Im Folgenden einige Beispiele:

a. Der Verein muss den Zugang zum PC sichern. Das bedeutet: Verhinderung des körperlichen Zugangs durch Sichern und Abschließen des jeweiligen Raums, in dem sich die DV-Anlagen befinden, und Verhinderung des technischen Zugangs durch passwortgeschützte Bereiche. Der Verein muss somit festlegen, welche Personen Zugang zum PC und zu allen Daten haben dürfen. Das sollten möglichst wenige Personen sein. Ausschließlich diese Personen sollten mit einem Schlüssel in zweifacher Bedeutung ausgestattet sein: Einem Schlüssel zu dem Raum, in dem sich der PC befindet, sowie einem Passwort für die Nutzung der Daten. Andere Personen dürfen nur von Fall zu Fall und im Zusammenhang mit ihrer jeweiligen Aufgabe Zugang zum PC und den jeweils benötigten Daten haben, z.B. mit gesondertem Passwort zu einem Teil der Daten.

b. Möglichst sichere Kommunikation wenigstens innerhalb des Vorstands nutzen (E-Mails nur über Vereins-Account, End-zu-End-Verschlüsselung).

c. Bei Webseiten mit Kommunikation mit dem Nutzer (Kontaktformular, Newsletterbestellung, Kommentarfunktion etc.) ist ab 25.05.2018 folgendes verpflichtend: Verwendung eines Hypertext Transfer Protocol Secure (*Transportverschlüsselung*; Kommunikationsprotokoll im World Wide Web, um Daten abhörsicher zu übertragen) für die Webseite. Eine solche verschlüsselte Verbindung erkennt man daran, dass die Adresszeile des Browsers von "http://" auf "https://" wechselt. Vereine sollten hierzu ihren Provider ansprechen.

d. Regelmäßiges Aufspielen von Software- und Sicherheitsupdates,

e. zeitnahe Datensicherung.

f. Datenverschlüsselung auf mobilen Endgeräten,

g. Geheimhaltung von Zugangsdaten zum mobilen Zugriff.

h. besondere Sicherheitsvorkehrungen bei paralleler Nutzung zu privaten Zwecken oder paralleler Nutzung durch andere Personen (Familien-PC).

Was ist das „Verzeichnis der Verarbeitungstätigkeiten"?

Schriftlich oder in einem elektronischen Format muss ein Verein ein internes Verzeichnis führen, in dem er den „Status Quo" seines Umgangs mit personenbezogenen Daten darlegt (Art. 30). Das Verzeichnis ist der Aufsichtsbehörde (Hessen: Hessischer Datenschutzbeauftragter, https://datenschutz.hessen.de/datenschutz/vereine) auf Anfrage zur Verfügung zu stellen.

Welche Angaben gehören in dieses Verzeichnis?

- Name und Kontaktdaten des Vereins, des Vertreters des Vereins (Vertretungsvorstand, § 26 BGB) sowie eines etwaigen Datenschutzbeauftragten;
- Zwecke der Verarbeitung (z.B. Erfüllung der Satzungszwecke, Mitgliederverwaltung, Beitragseinzug, Sportbetrieb, Förderung von Kunst und Kultur, Öffentlichkeitsarbeit, Erfüllung von Dienst- , Arbeits- und sonstigen Verträgen);
- Beschreibung der Gruppen betroffener Personen und der Gruppen personenbezogener Daten (z.B. Vereinsmitglieder: Name, Anschrift, Geburtsdatum, E-Mail-Adresse etc.; Übungsleiter, Betreuer, Ausbilder: Dienstvertrag, Name, Anschrift, Geburtsdatum, E-Mail-Adresse, Lizenz, frühere Dienstverhältnisse etc.; Arbeitnehmer: Name, Anschrift, Geburtsdatum etc.);
- Gruppen von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden (An wen werden Daten weitergegeben? Interne Zugriffsberechtigte: Geschäftsführender Vorstand, Geschäftsführer, Abteilungsleiter, Übungsleiter etc., extern: Dach- und Fachverbände, Öffentlichkeit über Homepage, Steuerberater etc.);
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datengruppen (z.B. Mitgliederdaten: 1 Jahr nach Beendigung der Mitgliedschaft; Übungsleiterdaten: 6 Monate nach Beendigung des Vertrages etc.);
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zum Schutz der Daten (z. B. Datenschutzklausel

in Satzung/Datenschutzordnung; Typ der Software; regelmäßiges Aufspielen von Software- und Sicherheitsupdates; Regelung des körperlichen und technischen Zugangs; nur 3 Personen haben Zutrittsberechtigung zum PC; Geschäftsstelle wird abgeschlossen, wenn kein Mitarbeiter dort ist; Vorsitzender schließt zu Hause Zimmer mit PC ab; technischer Zugriffsschutz durch Passwörter; Erfassung, Verarbeitung, Weiterleitung von Daten über gesicherte Verbindungen; Verfügbarkeit nach technischem Zwischenfall durch Backup-System etc.)

Gibt es Ausnahmen von der Pflicht, ein solches Verzeichnis zu erstellen?

Ja, bestimmte Unternehmen oder Einrichtungen sind von dieser Pflicht befreit, und zwar solche, die weniger als 250 Mitarbeiter beschäftigen, es sei denn die Verarbeitung erfolgt nicht nur gelegentlich. Letzteres tun jedoch Vereine in aller Regel: Das heißt, sie verarbeiten regelmäßig (also nicht nur gelegentlich) Daten (z.B. im Rahmen der Mitgliederverwaltung), so dass sie auch dann das Verzeichnis der Verarbeitungstätigkeiten anlegen müssen, wenn sie weniger als 250 Mitarbeiter beschäftigen.

Jedenfalls sollten Vereine dieses Verzeichnis anlegen. Es nützt ihnen selbst am meisten, da sie auf diese Weise einen Überblick über die im Rahmen der Vereinstätigkeit vorgenommene Datenverarbeitung gewinnen.

Muster für ein solches Verzeichnis finden sich auf den Webseiten des Hessischen Datenschutzbeauftragten und des Bayerischen Landesamtes für die Datenschutzaufsicht unter

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Hinweise%20zum%20Verzeichnis%20von%20Verarbeitungst%C3%A4tigkeiten_1.pdf

https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf sowie

https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf

7

Welche Rechte haben die betroffenen Personen?

Die Personen, deren Daten vom Verein verarbeitet werden, haben verschiedene Rechte gegen den Verein, insbesondere das Recht auf …

- Auskunft über die verarbeiteten Daten (Art. 15): Auskunft z. B. darüber, welche Daten zu welchen Zwecken verarbeitet und ggf. wohin weitergegeben werden;
- Berichtigung unrichtiger Daten (Art. 16);
- Löschung von Daten („Recht auf Vergessenwerden", Art. 17), die z. B. unrechtmäßig verarbeitet werden, die für die Zwecke, für die sie verarbeitet wurden, nicht mehr notwendig sind oder falls die notwendige Einwilligung widerrufen wurde.)
- Einschränkung der Verarbeitung (Art. 18; siehe auch § 35 BDSG), wenn z. B. gesetzliche, vertragliche oder satzungsgemäße Fristen der Löschung entgegenstehen.

8

Über was muss der Verein die betroffenen Personen (z. B. seine Mitglieder) informieren?

Der Verein muss den betroffenen Personen alle Informationen, die sich auf die Verarbeitung personenbezogener Daten beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln (Art. 12).

- Werden personenbezogene Daten bei der betroffenen Person (z. B. dem Mitglied) erhoben, so hat der Verein der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mitzuteilen (Art. 13): Vereinsname und Kontaktdaten des Verantwortlichen im Verein und seines Stellvertreters. Hier sind – neben dem Vereinsnamen – eine für den Datenschutz im Verein verantwortliche Person sowie deren Stellvertreter zu nennen.

- Kontaktdaten des Datenschutzbeauftragten, wenn vorhanden;

  Tipp: Der Übersichtlichkeit halber sollten Vereine ein eigenes Info-Blatt für jede Gruppe betroffener Personen anlegen (z. B. für Mitglieder, Betreuer, Arbeitnehmer);

- Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen (z. B. Erfüllung der Satzungszwecke, Mitgliederverwaltung, Sportbetrieb, Förderung von Kunst und Kultur, Öffentlichkeitsarbeit, Erfüllung von Dienst- und Arbeits- und sonstigen Verträgen);

- Rechtsgrundlage für die Verarbeitung (z.B. Art. 6 Abs. 1 b)

- Empfänger oder mögliche Empfänger, an welche die Daten (möglicherweise) weitergegeben werden (Interne Zugriffsberechtigte: Geschäftsführender Vorstand, Geschäftsführer, Abteilungsleiter, Übungsleiter etc., extern: Dach- und Fachverbände, Öffentlichkeit über Homepage, Steuerberater etc.);

- Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung der Speicherdauer (z. B. Löschung Mitgliederdaten: 1 Jahr nach Beendigung der Mitgliedschaft; Übungsleiterdaten: 6 Monate nach Beendigung des Vertrages etc.);

- Information über Pflichtdaten: z. B.: Welche Daten muss ich bereitstellen, um Vereinsmitglied zu werden (Pflichtangaben?) Welche Angaben sind freiwillig?

- ggf. Information über die Absicht, personenbezogene Daten an ein Drittland (Land außerhalb der EU) zu übermitteln, siehe Art. 45 ff.: Übermittlung nur zulässig in ein Land der EU oder ein Land mit angemessenem Schutzniveau gemäß Beschluss der Kommission (Eine jeweilige aktuelle Übersicht findet sich auf den Webseiten der EU-Kommission) oder aufgrund Einwilligung unter Hinweis auf Risiken. Dieser Fall kann eintreten, wenn etwa Mitgliederdaten in einer Cloud gespeichert werden, deren Server in den USA stehen.

Nähere Informationen hierzu finden Sie auf der Website des Hessischen Datenschutzbeauftragten unter:

- **https://datenschutz.hessen.de/datenschutz/internationales/angemessenheitsbeschl%C3%BCsse und**
- **https://datenschutz.hessen.de/datenschutz/internationales/privacy-shield**

Hier wird auch erläutert, unter welchen Bedingungen Datenübermittlungen an bestimmte Unternehmen in den USA zulässig sein können.

- Belehrung über Rechte, z. B.:

  Sie haben im Rahmen der geltenden gesetzlichen Bestimmungen das Recht auf Auskunft über Ihre gespeicherten personenbezogenen Daten (Art. 15 DS-GVO) sowie auf Berichtigung (Art. 16 DS-GVO), Löschung (Art. 17 GS-DVO), Einschränkung der Verarbeitung (Art. 18 GS-DVO), Widerspruch gegen die Verarbeitung (Art. 21 DS-GVO) und Datenübertragbarkeit (Art. 20 DS-GVO). Diese Rechte können Sie schriftlich oder per E-Mail bei dem oben genannten Verantwortlichen geltend machen.

- Belehrung betr. Einwilligung, etwa:

  Sie können eine bereits erteilte Einwilligung jederzeit widerrufen. Der Widerruf kann schriftlich oder per E-Mail an den oben genannten Verantwortlichen gesandt werden. Die Rechtmäßigkeit der bis zum Widerruf erfolgten Datenverarbeitung bleibt vom Widerruf unberührt.

- Belehrung über Beschwerderecht:

  Ihnen steht ein Recht zur Beschwerde bei der zuständigen Aufsichtsbehörde zu. Zuständige Aufsichtsbehörde in datenschutzrechtlichen Fragen ist in Hessen der Hessische Datenschutzbeauftragte https://datenschutz.hessen.de (https://datenschutz.hessen.de/service/beschwerde).

Gibt es Ausnahmen von dieser Informationspflicht?

Die Informationspflichten bestehen nicht, wenn und soweit die betroffene Person bereits über die Informationen verfügt, also konkret Bescheid weiß.

Auf welche Weise teilt der Verein die Informationen mit?

Der Verein muss den betroffenen Personen alle Informationen, die sich auf die Verarbeitung personenbezogener Daten beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache übermitteln (Art. 12). Die Übermittlung der Informationen erfolgt schriftlich oder in anderer Form, gegebenenfalls auch elektronisch, z. B. per E-Mail und/oder auf der Homepage, soweit damit alle Anforderungen erfüllt sind. Insbesondere auf die leichte Zugänglichkeit muss bei elektronischer Darstellung geachtet werden.

Im Hinblick auf die Mitglieder kann der Verein die Informationen auch in der Satzung oder einer Datenschutzordnung bekannt geben.

Hinweis:

Die nach Art. 13 mitzuteilenden Informationen sollten auch in die besondere Datenschutzerklärung für die Webseite aufgenommen werden – neben den Informationen, die speziell das Telemediengesetz verlangt.

Für die Erstellung einer Datenschutzerklärung bietet auch das Internet geeignete Tools sog. Datenschutzerklärungs-Generatoren. Muster für eine Satzungsklausel sowie ein Informationsblatt für Mitglieder findet man auf der Website des Landessportbundes Hessen:

http://www.lsbh-vereinsberater.de/datenschutz/neues-datenschutzrecht/

9

Welcher Verein muss einen Datenschutzbeauftragten (DSB) bestellen?

Dies ist - wie bisher - der Fall, soweit Vereine in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. (Artikel 37, § 38 BDSG).

Die „Beschäftigung mit der Verarbeitung" ist weit auszulegen. Jede Nutzung von Daten aus der EDV ist damit gemeint. Auch Personen, die lediglich Informationen aus der Mitgliederdatei erhalten und selbst überhaupt nicht am PC tätig sind, können damit gemeint sein (z.B. Übungsleiter).

Kurz gefasst meint „beschäftigt mit der Datenverarbeitung" in diesem Sinne:

> **Jede(n), der (die) im Auftrag des Vereins regelmäßig mit Hilfe der EDV-Mitgliederverwaltung personenbezogene Daten verarbeitet (z. B. auch lediglich nutzt), unerheblich ob ehrenamtlich oder im Rahmen eines Dienstverhältnisses.**

An die „Regelmäßigkeit" sind keine hohen Anforderungen zu stellen. **Beispiel:** Auch der Kursleiter, der sich 2x im Jahr eine Liste seiner Teilnehmer ausdrucken lässt, handelt regelmäßig im Rahmen seiner Aufgabe.

Somit zählen zu den „Beschäftigten" etwa Vorstandsmitglieder, Abteilungsleiter, Webmaster, Übungsleiter, Betreuer, Geschäftsstellenmitarbeiter.

Wer darf DSB werden?

Zunächst: Wer darf es nicht werden? Vorstandsmitglieder und Personen, die (mit)verantwortlich für die Datenverarbeitung im Verein sind, dürfen nicht zugleich DSB sein. Anderenfalls stünde der DSB in einem Interessenkonflikt: Denn er berät den Vorstand und kann daher nicht zugleich im Vorstand für die Umsetzung seiner Empfehlungen Verantwortung tragen. Auch darf er sich nicht selbst überwachen.

Der Datenschutzbeauftragte wird auf der Grundlage insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt (Art 37, 39). Dies ist abhängig von Art und Umfang der Daten-

verarbeitung: Welche und wie viele Daten werden verarbeitet? Sind darunter besonders sensible Daten? Welche Risiken bestehen?

Selbstverständlich benötigt der DSB im Verein nicht das Fachwissen eines DSB in einem Krankenhaus oder einer Bank. Welches Fachwissen gemeint ist bzw. ob das eigene Fachwissen ausreicht, muss jeder anhand der jeweiligen Situation und Organisation selbst prüfen. Fachwissen kann jemand aufgrund beruflicher Erfahrungen bereits haben oder durch Schulungen oder im Selbststudium erwerben. Der DSB ist zu einer bestimmten Ausbildung nicht verpflichtet.

Als DSB kann ein Vereinsmitglied oder eine externe Person benannt werden.

Welche Stellung hat ein DSB?

Dies lässt sich im Wesentlichen so charakterisieren (Art. 37, 38):

- Der Vorstand benennt den DSB. Die Benennung ist dem Hessischen Datenschutzbeauftragten zu melden. Hierfür steht auf der Webseite des Hessischen Datenschutzbeauftragten ein Formular bereit:

  https://datenschutz.hessen.de/service/benennung-eines-datenschutzbeauftragten

- Der Vereinsvorstand unterstützt den DSB (Ressourcen werden gestellt, Zugang zu allen Datenverarbeitungsvorgängen etc.).
- Der DSB erhält im Zusammenhang mit seinen Aufgaben keine Weisungen.
- Der DSB berät den Vorstand und berichtet diesem.
- Der DSB hat keine Entscheidungsbefugnisse bei Ausübung seiner Aufgaben.
- Betroffene können den DSB zu Rate ziehen; der DSB ist zur Vertraulichkeit verpflichtet.
- Er haftet unter den Voraussetzungen des § 31 b Bürgerliches Gesetzbuch (BGB) nur für Vorsatz und grobe Fahrlässigkeit, sofern der DSB als Vereinsmitglied unentgeltlich im Auftrag des Vereins tätig ist. Ansonsten kann eine entsprechende Einschränkung der Haftung vertraglich vereinbart werden.

Welche Aufgaben hat ein DSB?

Das lässt sich so zusammenfassen:

- Unterrichtung und Beratung des Vorstands und der mit der Datenverarbeitung Beschäftigten;
- Überwachung der Einhaltung der DS-GVO sowie
- Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter;
- Infos zur Schulung und Muster unter:
  https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Der%20beh%C3%B6rdliche%20und%20betriebliche%20Datenschutzbeauftragte.pdf und
  https://www.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf

Wie ist die Situation, wenn kein DSB bestellt ist?

Dann reduzieren sich die gesetzlichen Pflichten keineswegs, sondern der Vereinsvorstand hat die Aufgaben des Datenschutzbeauftragten auf andere Weise sicherzustellen, z. B. Beaufsichtigung und Schulung der Vereinsmitarbeiter.

10

**Was versteht man unter „Auftragsdatenverarbeitung"?
Ist das auch für Vereine relevant?**

Unter Auftragsdatenverarbeitung versteht man die Verarbeitung von personenbezogenen Daten durch einen Auftragnehmer (Auftragsverarbeiter) gemäß den Weisungen des Auftraggebers (hier: der Verein) auf der Grundlage eines schriftlichen oder elektronischen Vertrags (Art. 28 f. DS-GVO). Der Verein gibt seine Verantwortung nicht ab, sondern behält ein umfassendes Weisungs- und Kontrollrecht.

Diese Situation können wir vorfinden, wenn Vereine Dienstleister in die Datenverarbeitung einschalten, z. B. zur Wartung der EDV und der Homepage, bei der Buchhaltung und der Gehaltsabrechnung. In diesen Fällen übermittelt der Verein anderen Personen oder Unternehmen die von ihm erhobenen und gespeicherten personenbezogenen Daten seiner Mitglieder, Spender, Arbeitnehmer etc., erlaubt das Abfragen der Daten durch Dritte und/oder gibt die Daten zwecks weiterer Verwendung an andere ab. Hierbei wird es sich meist um Auftragsdatenverarbeitung handeln.

Der Verein muss den Auftragsverarbeiter sorgfältig auswählen, denn auch der Verein haftet für dessen Fehlverhalten. Also muss der Verein genau prüfen, ob und wie der Auftragsverarbeiter die Gewähr dafür bietet, die datenschutzrechtlichen Vorgaben einzuhalten.

Was muss der Vertrag im Wesentlichen beinhalten? Zunächst die konkrete Festlegung von Art und Umfang des Auftrags, insbesondere die Beschreibung, welche Daten von welchen Personen Gegenstand der Auftragsdatenverarbeitung sein sollen. Weiter die Darlegung der Weisungsbefugnisse des Vereins und der Verpflichtung des Auftragsverarbeiters zur Vertraulichkeit sowie der Gewährleistung der technischen und organisatorischen Sicherheit der Datenverarbeitung. Auch weitgehende Kontrollrechte des Vereins müssen geregelt werden, etwa das Recht zur Durchführung unangemeldeter Kontrollen vor Ort. Außerdem muss der Vertrag Regelungen für den Fall seiner Beendigung einschließlich der Rückgabe oder Löschung von Daten enthalten.

Sowohl der Verein wie der Auftragsverarbeiter haften gegenüber den Inhabern der Daten, wenn sie gegen ihre jeweiligen Pflichten verstoßen. Daneben haftet der Verein für Fehlverhalten des Auftragsverarbeiters. Ein guter Auftragsdatenverarbeiter sollte selbst die Einhaltung der DS-GVO durch den Vertrag zusichern können.

11

Was passiert, wenn der Verein seinen Pflichten nach der DS-GVO nicht nachkommt?

Dann können u.a. Bußgelder (§ 43 BDSG) drohen. Allerdings ist davon auszugehen, dass etwaige Bußgelder für Vereine maßvoll und verhältnismäßig ausfallen werden, vor allem bei einem ersten Verstoß. Richtig ist, dass die Aufsichtsbehörden nunmehr relativ hohe Bußgelder verhängen dürfen. „Zielgruppe" hierfür sind jedoch in erster Linie große Unternehmen.

Grundsätzlich hat der Vereinsvorstand gegenüber dem Verein die Pflicht, die Datenschutzvorschriften umzusetzen. Verstößt der Vorstand gegen diese Pflicht und entsteht daraus ein Schaden, kann der Verein unter Umständen Schadensersatz gegen den Vorstand geltend machen, wobei der ehrenamtlich tätige Vorstand nur für Vorsatz und grobe Fahrlässigkeit haftet (§ 31 a BGB).

12

Weitere Links

- **https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf (Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg)**
- **https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Datenschutz_im_Verein__DS-GVO__-_Kompakt.pdf (Der Landesbeauftragte für den Datenschutz Rheinland-Pfalz)**
- **https://www.lda.bayern.de/media/muster_1_verein.pdf**

IMPRESSUM

HESSEN

Herausgeber

Hessische Staatskanzlei

Georg-August-Zinn-Str. 1

65183 Wiesbaden

www.hessen.de

www.gemeinsam-aktiv.de

Verantwortlich

Michael Bußer, Staatssekretär
Sprecher der Landesregierung

Redaktion

Hessische Staatskanzlei, Claudia Carnemolla

unterstützt von Herrn Rechtsanwalt Dr. Frank Weller (juristische Leitung)

Gestaltungskonzept & Artwork

Nina Faber de.sign, Wiesbaden

HESSEN

Hessische Landesregierung

Georg-August-Zinn-Straße 1
65183 Wiesbaden

www.hessen.de