Hinweis: *Das vorliegende Skript stellt im Wesentlichen eine Zusammenfassung der wichtigsten Punkte des Vortrages „Grundzüge der DS-GVO“ dar. Das Skript erhebt dabei keinen Anspruch auf Vollständigkeit und kann eine Rechtsberatung nicht ersetzen!*

Literaturempfehlungen:

- Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine, Herausgeber: Bayerisches Landesamt für Datenschutzaufsicht, Verlag C.H. Beck 2017, ISBN 978 3 406 71662 1
- Datenschutz im Verein nach der DS-GVO, Herausgeber: Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, abrufbar unter: https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/03/OH-Datenschutz-im-Verein-nach-der-DSGVO.pdf
- Formulierungshilfe für ein Verarbeitungsverzeichnis, abrufbar unter: https://www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- Formulierungshilfe für einen Auftragsverarbeitungsvertrag, abrufbar unter: https://www.lda.bayern.de/media/muster_adv.pdf

I. Ziele der DS-GVO:

Die Datenschutz-Grundverordnung (DS-GVO) ist seit dem 25.05.2018 wirksam. Als Verordnung ist sie in all ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat der Europäischen Union.

Sie schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten, Art. 1 Abs. 2 DS-GVO.

II. Sachlicher Anwendungsbereich der DS-GVO

Die DS-GVO gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen, vgl. Art. 2 Abs. 1 DS-GVO.

1. Begriffserklärungen:

a. Personenbezogene Daten

Personenbezogene Daten sind dabei alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person *beziehen*, vgl. Art. 4 Nr. 1 DS-GVO.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Beispiele für personenbezogene Daten sind insbesondere:

Name, Adresse, Steuernummer, Lichtbilder, Videoaufnahmen, etc.

b. Verarbeiten

Der Begriff des Verarbeitens von Daten ist weit zu verstehen, vgl. Art. 4 Nr. 2 DS-GVO.

Unter einem **Verarbeiten** versteht man daher insbesondere das Erheben, Erfassen, Ordnen, Speichern, Verändern, Abfragen, Verwenden, Übermitteln und Löschen von Daten.

Dabei ist nicht entscheidend, ob es sich bei dem Verarbeiter der personenbezogenen Daten um eine natürliche oder juristische Person handelt. Ferner ist nicht entscheidend, ob sich die Verarbeitung im öffentlichen oder nicht-öffentlichen Bereich abspielt.

(1) Automatisierte Verarbeitung

Die DS-GVO gilt bei einer **ganz oder teilweise automatisierten** Verarbeitung personenbezogener Daten. Das ist der Fall, wenn sog. Datenverarbeitungsanlagen zum Einsatz kommen.

Als Beispiele für automatisierte Verarbeitungen können daher die Videoüberwachung, die Aufzeichnung durch Dashcams, Smart-Phones, Drohnen oder Tonbandgeräte genannt werden.

(2) Nichtautomatisierte Verarbeitung

Ferner findet die DS-GVO auch Anwendung bei der **nichtautomatisierten Verarbeitung** personenbezogener Daten bei Speicherung in ein Dateisystem. Hierunter ist die *rein manuelle Verarbeitung* zu verstehen. Hauptanwendungsfall dürfte demnach das Festhalten von Informationen durch einen Menschen mit Hilfe eines Stifts auf einem Blatt Papier sein.

Fallbeispiel: Austausch und Ablage einer Visitenkarte

2. Ausnahmen vom Anwendungsbereich der DS-GVO, vgl. Art 2. Abs. 2 lit. c

Ausgenommen vom Anwendungsbereich der DS-GVO sind insbesondere *rein persönliche oder familiäre* Tätigkeiten. Hierunter sind alle Tätigkeiten zu verstehen, denen jeglicher Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit fehlen, vgl. EG 18 DS-GVO.

Exemplarisch hierfür lassen sich etwa das Sammeln von Adress- bzw. Geburtsdaten privater Kontakte anführen.

Bei der Nutzung von „Sozialen Netzwerken“ (Facebook, etc.) ist allerdings Vorsicht geboten. Richtet sich die Veröffentlichung von Informationen nämlich an einen *unbestimmten Personenkreis*, kann nach Auffassung der Rechtsprechung nicht mehr von einer rein persönlichen oder familiären Tätigkeit ausgegangen werden.

Auch beim Einsatz von Überwachungskameras ist Vorsicht geboten. Grundsätzlich ist die Videoüberwachung von Privateigentum als privater Zweck zwar anerkannt -mit der Folge-, dass die DS-GVO keine Anwendung findet. Dies gilt allerdings dann nicht, wenn gleichsam *öffentlicher Raum* aufgezeichnet wird.

Bei der Veröffentlichung von Fotos dürfte der persönliche und familiäre Bereich dann überschritten sein, wenn das Recht am eigenen Bild des Betroffenen verletzt wird.

Fallbeispiele: Findet die DS-GVO Anwendung?

1. Vereinsmitglied A notiert sich die Daten der Heizungs- und Sanitär-GmbH, die bauliche Maßnahmen im Vereinsheim durchführen soll.

   Da in dem vorliegenden Beispielfall keine *personen*bezogenen Daten erhoben werden, findet die DS-GVO keine Anwendung.

2. Vereinsmitglied B erhält die Visitenkarte eines potentiellen Mitglieds und legt diese sodann im Vereinsbüro ab.

   Da personenbezogene Daten in einem Ordnungssystem abgelegt werden, findet die DS-GVO Anwendung.

3. Vereinsmitglied C feiert seinen Geburtstag im Vereinsheim und fotografiert dabei seine Gäste. Sodann stellt er die Bilder bei Facebook ein.

   Hier ist zu differenzieren:

   Beim Fotografieren der Gäste durch ein Vereinsmitglied als Privatperson (!) handelt es sich grundsätzlich um eine rein persönliche Tätigkeit ohne wirtschaftlichen Bezug, so dass die DS-GVO keine Anwendung findet.

Das Einstellen der Fotos auf Facebook hingegen richtet sich an einen unbestimmten Personenkreis, so dass nicht mehr von einer rein privaten Tätigkeit ausgegangen werden kann. Folglich würde die DS-GVO Anwendung finden.

4. Der Kunstverein fotografiert Vereinsmitglieder im Rahmen einer Veranstaltung und stellt die Bilder auf seine Vereinshomepage.

   Die DS-GVO findet Anwendung.

5. Der Verein „Kleingarten e.V." unterhält eine Internetseite mit einem Kontaktformular.

   Die DS-GVO findet Anwendung.

Frage: Welche Daten werden eigentlich auf einer Internetseite gesammelt?

→ IP-Adresse, etc.

III. Wann darf ich personenbezogene Daten erheben?

In der DS-GVO gilt ein sogenanntes **Verbot mit Erlaubnisvorbehalt.**

Dies bedeutet, dass personenbezogene Daten nur dann verarbeitet werden dürfen, wenn hinsichtlich der jeweiligen Verarbeitung entweder eine ausdrückliche Einwilligung des Betroffenen vorliegt oder eine entsprechende Rechtsgrundlage besteht.

Mit anderen Worten: Fehlt es an einer Einwilligung oder Erlaubnisnorm ist die Verarbeitung personenbezogener Daten rechtswidrig.

> **Merke:** Vor jeder Verarbeitung personenbezogener Daten ist daher zu prüfen, ob hinsichtlich des *konkreten* Zwecks der Datenverarbeitung entweder eine Einwilligung des Betroffenen vorliegt oder eine Rechtsgrundlage besteht.

1. Erlaubnisnormen, Art. 6 DS-GVO

Die im Rahmen der Vereinsarbeit wichtigsten Erlaubnisnormen (vgl. Art. 6 DS-GVO) werden nachfolgend dargestellt. Demnach ist die Verarbeitung personenbezogener Daten auch ohne das Vorliegen einer entsprechenden Einwilligung zulässig, wenn die Verarbeitung insbesondere

- zur Erfüllung eines Vertrages oder zur Durchführung vorvertraglicher Maßnahmen (Art. 6 Abs. 1 lit. b DS-GVO),
- zur Erfüllung einer rechtlichen Verpflichtung (Art. 6 Abs. 1 lit. c DS-GVO) oder
- zur Wahrung der berechtigten Interessen, (Art. 6 Abs. 1 lit. f DS-GVO)

erforderlich ist.

a. Als Rechtsgrundlage kommt in erster Linie Art. 6 Abs. 1 lit. b DS-GVO in Betracht, da es sich bei der Vereinsmitgliedschaft um ein Vertragsverhältnis zwischen den Mitgliedern und dem Verein handelt. Den wesentlichen Inhalt dieses Vertragsverhältnisses regeln dabei die Vereinssatzung und die darin enthaltenen Vereinsziele.

Gemäß Art. 6 lit. b DS-GVO dürfen grundsätzlich nur solche Daten erhoben werden, die entweder zur Verfolgung der konkreten Vereinsziele oder für die Betreuung und Verwaltung der Mitglieder zwingend erforderlich sind.

b. Es ist auch denkbar, dass sich die Verarbeitung personenbezogener Daten von Vereinsmitgliedern auf das *besondere Interesse* des Vereins stützen lässt, vgl. Art. 6 lit. f DS-GVO. Dies setzt indes voraus, dass ein berechtigtes Interesse des Vereins besteht, ohne dass dabei schutzwürdige Interessen des Betroffenen entgegenstehen.

In diesem Zusammenhang sind insbesondere die *vernünftigen Erwartungen* der betroffenen Person zu berücksichtigen. Dabei ist auch zu prüfen, ob die betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten absehen kann, dass eine Verarbeitung für diesen Zweck erfolgen kann, vgl. EG 47 der DS-GVO.

> → Vereine sollten die betroffene Person zum Zeitpunkt der Erhebung ihrer personenbezogenen Daten so *transparent* und *umfassend* wie möglich in Bezug auf die konkrete Verarbeitung ihrer personenbezogenen Daten informieren.
>
> **Merke:** Da den Verein die rechtliche Verpflichtung trifft, die Grundzüge der Datenverarbeitung schriftlich zu regeln, empfehlen die Datenschutzbehörden dies in die Vereinssatzung aufzunehmen oder eine *Datenschutzordnung* bzw. Datenschutzrichtline festzulegen (vgl. etwa Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg, „Datenschutz im Verein nach der DS-GVO, S. 8 ff.).

Diverse Fallbeispiele im Vortrag: Handeln die Vereine rechtmäßig?

1. Ein neues Mitglied füllt den Antragsbogen zur Vereinsmitgliedschaft aus und gibt darin seinen Namen, seine Anschrift und sein Geburtsdatum an.

In der Regel dürften die vorgenannten Daten zur Verwaltung der Mitgliedschaft erforderlich sein, so dass eine Einwilligung nicht benötigt wird, vgl. Art 6 lit. b DS-GVO.

Wie wäre es, wenn der Verein noch die Religionszugehörigkeit oder die Parteimitgliedschaft des Mitglieds abfragt?

Eine Abfrage dieser Daten im Rahmen des Antrags auf Mitgliedschaft wäre nicht rechtmäßig, da dies weder für die Mitgliederverwaltung noch für die Erfüllung des Vereinszwecks hier erforderlich ist.

2. Die Freiwillige Feuerwehr nutzt auf ihrer Internetseite die Tracking-Software -Google Analytics-.

Wird Google Analytics dergestalt verwendet, dass die IP-Adresse des Seitenbesuchers (personenbezogenes Datum) in nicht-anonymisierter Form an Google (Dritter) übermittelt wird, wäre die Nutzung von Google Analytics rechtswidrig.

3. Im Vortrag genannte Beispiele der Übermittlung personenbezogener Daten an Dritte, welche eine Verarbeitung personenbezogener Daten darstellen:

- Datenübermittlung an Vereinsmitglieder (z.B. Weitergabe von Mitgliederlisten)
- Veröffentlichungen im Internet (z.B. auf der Vereinshomepage oder am Schwarzen Brett, etc.)
- Datenübermittlung an Dachverbände
- Datenübermittlung an sonstige Dritte (Behörden, Sponsoren, Versicherungen, etc.)

2. Die Einwilligungserklärung

Des Weiteren ist die Verarbeitung personenbezogener Daten dann rechtmäßig, wenn die betroffene Person ihre Einwilligung zu der Verarbeitung erteilt hat.

Hinsichtlich der Einwilligungserklärung ist allerdings zu beachten, dass sie strengen Anforderungen unterliegt:

- die Einwilligung muss ausdrücklich für einen *bestimmten* Zweck erteilt werden,
- die Einwilligung muss *transparent* gestaltet sein, sodass der konkrete Zweck der Verarbeitung klar und deutlich erkennbar ist,
- der Betroffene muss hinsichtlich der Reichweite der Verarbeitung seiner personenbezogenen Daten informiert sein,
- der Betroffene muss die Einwilligung *freiwillig* (d. h. frei von Zwang) erteilen,
- der Betroffene ist darauf hinzuweisen, dass er seine Einwilligung jederzeit für die Zukunft widerrufen kann,
- der Verantwortliche muss die Einwilligung *nachweisen* können.

→ Nähere Erläuterung anhand einer konkreten Einwilligungserklärung

> **Merke:** Im Falle einer erteilten Einwilligung ist insbesondere zu beachten, dass der Betroffene diese jederzeit mit Wirkung für die Zukunft widerrufen kann. Insofern sind im Vorfeld entsprechende Maßnahmen zu ergreifen, um sicherzustellen, dass ein möglicher Widerruf unverzüglich umgesetzt werden kann.

Fallbeispiel:

Der Künstlerverein nimmt in seinen Mitgliedsantrag eine Klausel auf, wonach sich Mitglieder damit einverstanden erklären, dass sie bei Kunstausstellungen fotografiert und die Fotos, auf denen sie abgebildet sind, veröffentlicht werden dürfen. Ist die Einwilligung rechtmäßig?

Nein, da die oben genannten Voraussetzungen für eine wirksame Einwilligung nicht erfüllt sind.

IV. Informationspflichten bei Erhebung personenbezogener Daten, Art. 13 DS-GVO

Wenn Sie personenbezogene Daten *bei dem Betroffenen* erheben, müssen Sie ihn vor dem Zeitpunkt der Erhebung dieser Daten auf bestimmte Mindestinformationen hinweisen:

Dies folgt aus dem Transparenzgebot. Zum einen soll der Betroffene hierdurch Kenntnis von den Verarbeitungsvorgängen erlangen. Zum anderen soll er Kenntnis von dem Verantwortlichen und seinen Rechten erhalten.

Hierbei ist zu beachten, dass die Informationen *proaktiv* -d.h. ohne besondere Aufforderung- zur Verfügung zu stellen sind.

Gemäß Art 13 DS-GVO sind insbesondere nachfolgende Informationen dem Betroffenen mitzuteilen:

- Kontaktdaten des Verantwortlichen
- Kategorien betroffener Person und Kategorien personenbezogener Daten
- Zweck und Rechtsgrundlage, für die die personenbezogenen Daten verarbeitet werden
- Dauer der Verarbeitung
- Rechte des Betroffenen

Eine Mitteilung ist dabei ausreichend, sodass es grundsätzlich keiner zwingenden Gegenzeichnung durch den Betroffenen bedarf.

> **Merke:** Eine Informationspflicht besteht auch dann, wenn Sie die bereits erhobenen Daten zu einem anderen als dem Erhebungszweck weiterverarbeiten wollen.

Beispiel 1: Der Kulturverein unterhält eine Vereinshomepage, auf der die relevanten Daten des Vereins angegeben sind. Ferner hält er ein Kontaktformular bereit.

Da der Verein personenbezogene Daten der Seitenbesucher verarbeitet (IP-Adressen sowie ggf. Anfragen über das Kontaktformular bzw. per E-Mail) muss eine Datenschutzerklärung auf der Internetseite bereitgehalten werden.

→ Erläuterung und Musterbeispiel: Datenschutzerklärung einer Internetseite

Beispiel 2: Ein potentielles Vereinsmitglied füllt in der Geschäftsstelle des Vereins ein schriftliches Antragsformular für eine Vereinsmitgliedschaft aus. Da der Verein auch hier personenbezogene Daten bei dem Betroffenen erhebt, müssen diesem die Pflichtinformationen aus Art. 13 DS-GVO mitgeteilt werden. Hier sollten die Datenschutzhinweise in *Papierform* bereitgestellt werden.

Hintergrund ist, dass die Bereitstellung der Information grundsätzlich *in demselben Medium* zu erfolgen hat wie die Datenerhebung:

Auf der Internetseite erfolgt die Datenerhebung *online*, so dass die Datenschutzerklärung gleichsam *online* zur Verfügung zu stellen ist. Beim Ausfüllen des Antragsformulars erfolgt die Datenerhebung *schriftlich*, so dass die Datenschutzhinweise gleichsam *schriftlich* bereitzustellen sind.

→ Erläuterung und Musterbeispiel: Datenschutzhinweise

V. Erläuterung der Betroffenenrechte

- Recht auf Auskunft gemäß Art. 15 DS-GVO
- Recht auf Berichtigung oder Löschung gemäß Art. 16, Art. 17 DS-GVO
- Recht auf Einschränkung der Verarbeitung gemäß Art. 18 DS-GVO
- Recht auf Datenübertragbarkeit gemäß Art. 20 DS-GVO
- Recht auf Widerspruch gegen die Verarbeitung gemäß Art. 21 DS-GVO
- Recht, sich bei einer Datenschutzaufsichtsbehörde über die Verarbeitung der Daten zu beschweren, Art. 77 DS-GVO
- Recht auf Widerruf einer erteilten Einwilligung

VI. Verarbeitungsverzeichnis, Art. 30 DS-GVO

Jeder Verantwortliche ist verpflichtet, ein Verzeichnis aller Verarbeitungstätigkeiten zu führen und dieses fortlaufend zu aktualisieren.

Der Verantwortliche soll damit überprüfen, ob alle Datenverarbeitungsvorgänge rechtskonform sind.

Das Verarbeitungsverzeichnis ist nur intern zu führen. Nur bei einer Aufforderung der zuständigen Datenschutzbehörde ist dieses Verzeichnis an die Behörde auszuhändigen.

In dem Verzeichnis sind u.a. nachfolgende Informationen aufzuführen:

- Kontaktdaten des Verantwortlichen
- Kategorien betroffener Person und Kategorien personenbezogener Daten
- Zweck und Rechtsgrundlage, für die die personenbezogenen Daten verarbeitet werden
- Dauer der Verarbeitung
- Löschungsfristen
- technische und organisatorische Schutzmaßnahmen

→ Erläuterung und Musterbeispiel: Verarbeitungsverzeichnis für Vereine

VII. Auftragsverarbeitung, Art. 28 DS-GVO, Art. 4 Nr. 8 DS-GVO

Sofern Sie sich externer Dienstleister (IT-Wartung, Cloud-Dienste, Webhosting, Aktenvernichtung, etc.) bedienen, welche personenbezogene Daten in Ihrem Auftrag weisungsgebunden verarbeiten, liegt ein Fall der sogenannten Auftragsverarbeitung vor:

1. Auswahl des Auftragsverarbeiters

Bei der Auswahl des Auftragsverarbeiters ist sicherzustellen, dass dieser hinreichend Garantien dafür bietet, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Bestimmungen erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

2. Abschluss eines Vertrages

Darüber hinaus ist mit dem Auftragsverarbeiter ein Vertrag zur Auftragsverarbeitung abzuschließen.

Darin ist insbesonder*e* zu regeln,

- dass der Auftragsverarbeiter die personenbezogenen Daten nur auf dokumentierte Weisung des Verantwortlichen verarbeitet,
- dass geeignete technische und organisatorische Sicherheitsmaßnahmen zu treffen sind,
- dass sich die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichten müssen,
- dass nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten gelöscht oder zurückgegeben werden.

Beispiel: Der Verein hat eine Vereinshomepage. Diese wird über die 123-Internet AG gehostet, welche den Speicherplatz für die Vereinshomepage und für die dazugehörige E-Mail-Kommunikation bereithält.

→ Erläuterung und Musterbeispiel: Auftragsverarbeitung

VIII. Sicherheit der Verarbeitung, Art. 32 DS-GVO

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürliche Personen muss der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Vertraulichkeit:

- Personenbezogene Daten sind so zu schützen, dass keine unberechtigten Personen darauf Zugriff nehmen können.

Integrität:

- Personenbezogene Daten sind vor Manipulationen (etwa durch Schadprogramme, Computerviren, etc.) zu schützen.

Verfügbarkeit:

- Es sind Maßnahmen zu treffen, damit personenbezogenen Daten jederzeit nutzbar sind und es nicht zu Ausfällen kommt (Back-Up Systeme, etc.).

→ **Beispiele zur IT-Sicherheit (im Vortrag)**

IX. Notwendigkeit der Benennung eines Datenschutzbeauftragten, Art. 37 ff. DS-GVO, § 38 BDSG-neu

Dies ist *insbesondere* dann der Fall, soweit im Verein in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, vgl. § 38 BDSG n.F.

➔ Benennung eines Datenschutzbeauftragten, Veröffentlichung der Kontaktdaten und Mitteilung an die Aufsichtsbehörde

Gemäß Art. 39 DS-GVO erstrecken sich die Aufgaben des Datenschutzbeauftragten insbesondere auf:

- die Unterrichtung und Beratung des Verantwortlichen, der Auftragsverarbeiter und Beschäftigten.
- Überwachung der datenschutzrechtlichen Vorschriften