



Themenbereich

Aktuelle Entwicklungen
zum Datenschutz (Kernbereiche)

Oktober 2019

© RA Richard Didyk

Reiz- Kernthemen zum Datenschutz

- **WhatsApp**
- **Facebook u.a.**
- **Bilder und Videos**
- **Rechtsgrundlage zur Datenverarbeitung**
- **Bestellung eines Datenschutzbeauftragten (§ 38 BDSG/Art. 35; Art. 37 DSGVO)**
- **Datenschutzerklärung bei bestehenden Mitgliedschaften**
- **Datenschutz und Satzungsänderungen**
- **Verarbeitungsverzeichnis**
- **Klagen wegen Wettbewerbsverstoß**

Beispiel Musterverein

Ein kleiner Verein hat 100 Mitglieder, einen ersten Vorstand, einen Kassier sowie einen Schriftführer (Vorstand im Sinne des BGB) sowie fünf Personen, die nach der sog. Übungsleiterpauschale bezahlt werden. Die Mitgliederverwaltung erfolgt durch den Schriftführer selbst. Die Verwaltung der Mitgliedsbeiträge erfolgt dagegen durch den Kassier. Der Verein betreibt zudem eine kleine Webseite, die bei einem Dienstleister gehostet ist, mit Mitgliederfotos.

Wesentliche Verarbeitungstätigkeit im Verein

- Lohnabrechnung über Dritte
- Mitgliederverwaltung
- Betrieb der Webseite
- Veröffentlichung von Mitgliederfotos auf der eigenen Webseite
- Beitragsverwaltung

WhatsApp – Nutzung als (offizielles) vereinsinternes Kommunikationsmittel ?

- ▶ Das Adressbuch eines Nutzers mit allen Kontakten einschließlich E-Mail und Telefonnummern wird an WhatsApp und damit an Facebook übertragen. Damit ist völlig unklar, wohin und zu welchem Zweck diese Daten übertragen und verarbeitet werden.
 - ▶ Der Verein kann daher seinen Mitgliedern gegenüber seinen Informationspflichten nicht nachkommen.
 - ▶ Der Verein kann bei WhatsApp auch nicht erzwingen, dass bei Widerspruch die Daten gelöscht werden.
- ▶ WhatsApp sammelt für den Verein unkontrolliert Metadaten von Nutzern und hat damit Zugriff auf persönliche Identifikatoren, mit welchen Nutzern wann und wie oft und worüber kommuniziert wird und kann damit Benutzerprofile erstellen und verkaufen.
- ▶ Durch die Verwendung von WhatsApp werden Daten in die USA übertragen und damit gegen die DSGVO verstoßen, die eine Übertragung nach außerhalb EU zumindest von einem vergleichbaren Datenschutz abhängig macht.

Alternativen zu WhatsApp

- **SIMSme** ist der Messenger der Deutschen Post, bietet modernste Funktionen und ist gleichzeitig kostenlos und werbefrei, echte Ende-zu-Ende-Verschlüsselung mit Servern nur in Deutschland, Senden von Text- und Sprachnachrichten, Teilen von Videos, Bilder und Standorte, Senden von Dateien beliebigen Formats (pdf, mp3, doc, zip usw.), Gruppen mit bis zu 100 Teilnehmern, mit der SIMSme-ID, kann man anonym kommunizieren, der Dienst ist für die Betriebssysteme Android und iOS verfügbar
- **Briar** kostenloser Messenger bietet den Experten zufolge höchste Sicherheit, weil über das anonyme Tor-Netzwerk kommuniziert wird und bei der Nutzung auch keinerlei Metadaten anfallen. Die Sicherheitsvorkehrungen machen die Anwendung im Alltag aber eher unkomfortabel. Den Messenger gibt es für Android.
- **Kontalk** von Freiwilligen aus aller Welt entwickelt und unterstützt wird, womit etwa ein Interesse an der Auswertung von Nutzerdaten entfällt. Den Messenger gibt es für Android und als Desktop-Version.
- **Signal** Gilt als "Mutter aller Krypto-Messenger". Den von der nichtkommerziellen Organisation Open Whisper Systems betriebenen, kostenlosen Messenger (Android, iOS und Desktop) gibt es schon ein Jahrzehnt – und er war der erste mit Ende-zu-Ende-Verschlüsselung.
- **Threema** Messenger (Android, iOS und Desktop) von Schweizer Entwicklern speichert keine Metadaten, ist bei Bedarf auch anonym nutzbar und genießt einen tadellosen Ruf – auch wenn der Quellcode nicht offenliegt. Die App kostet rund drei Euro.
- **Wire** Hauptsitz des entwickelnden Unternehmens ist in der Schweiz, programmiert wird den Angaben nach in Berlin. Den Experten gefallen unter anderem die vielen Extras sowie die Benutzeroberfläche des Gratis-Messengers (Android, iOS, Desktop und Browser).

Fotografien – DS-GVO contra Kunsturhebergesetz (KUG)

- ▶ Bislang Geltung des KUG soweit es die **Verbreitung** des Bildes betraf
- ▶ Nach Inkrafttreten der DS-GVO finden nunmehr bei der Verarbeitung von Bildaufnahmen (Erstellen, Speichern und Veröffentlichen) die auch sonst geltenden Bestimmungen Anwendung
 - ▶ Erforderlich gesetzliche Rechtsgrundlage (Vertragserfüllung oder Interessenslage) oder
 - ▶ Einwilligung
- ▶ Für die Praxis genügt weitestgehend der gesetzliche Erlaubnistatbestand als Rechtsgrundlage
 - ▶ Aufnahmen und Veröffentlichung von (Einzel-) Bildern anlässlich Vereinsveranstaltungen
 - ▶ Gilt für aktive wie auch passive Teilnehmer, Mitglieder oder Zuschauer und Gäste
 - ▶ Gilt auch für Kinder, allerdings besondere Sorgfalt wegen Kinderschutz

Fotografien - Einwilligung

- ▶ Wenn Einwilligung erforderlich, muss diese nicht schriftlich eingeholt werden. Ausreichend auch mündlich oder stillschweigend.
- ▶ Informationspflicht kommt der Verein nach
 - ▶ mit Datenschutz-Richtlinie
 - ▶ Hinweise auf Einladung
 - ▶ Plakaten zur Veranstaltung
 - ▶ mündliche Informationen zu Beginn der Veranstaltung

Hinweis:

Medienprivileg nach Art. 1 und 38 BayDSG auch für Vereine, wenn Verarbeitung zu journalistischen, künstlerischen oder literarischen Zwecken

Wann dürfen personenbezogene Daten verarbeitet werden?

- Rechtsgrundlage für die Verarbeitung -

Es gilt „**Verbot mit Erlaubnisvorbehalt**“. Danach ist Verarbeitung nur dann rechtmäßig, soweit

- für sie **gesetzliche Berechtigung** greift **o d e r**
- **der Betroffene eingewilligt hat (Art. 6 DSGVO)**.

Gesetzliche Erlaubnistatbestände greifen für Datenverarbeitungen,

- **die zur Vertragserfüllung erforderlich sind** oder
- **für die eine rechtliche Verpflichtung des Verantwortlichen** besteht oder
- **für die es ein berechtigtes Interesse der verantwortlichen Stelle oder eines Dritten gibt** und dem nach Interessensabwägung keine Interessen des Betroffenen entgegenstehen.

Wann dürfen personenbezogene Daten verarbeitet werden? (Einwilligung)

Einwilligung nur erforderlich, wenn nicht gesetzlicher Grund greift und Neuaufnahme oder Erweiterung der Datenverarbeitung, bisherige rechtswirksame Einwilligungen gelten fort !

Anforderungen an die Einwilligung des Betroffenen zur Datenverarbeitung sind

- **Information**, welche Daten zu welchen Zwecken durch welche Stelle,
 - **Freiwilligkeit**
 - Schriftform nicht mehr erforderlich,
 - wenn aber schriftlich, dann in einfacher Sprache
 - Hinweis auf jederzeitige **Widerrufbarkeit**
 - Zustimmung bei **Minderjährigen (< 16. Lebensjahr)**
- und
- **Nachweis** der Einwilligung

Beachte:

- **Gefahr des Widerrufs** mit Folge, dass Daten nicht mehr verwendbar !

Beispiele: Wann dürfen Daten vom Verein veröffentlicht oder weitergegeben werden?

- Datenübermittlung an andere Vereine oder Verbände z.B. wegen Ehrungen, Spielerpässe, Veranstaltungshinweise oder Behörden wegen Zuschüssen

*Zulässig, solange Datenübermittlung erforderlich, um Mitglied die satzungsgemäßen Leistungen bieten zu können (= **Vertragserfüllung**) oder wenn der Verein eigene Interessen an der Datenübermittlung hat z.B. wegen seiner eigenen Mitgliedschaft im Dachverband und Beitragsberechnung (= **Eigenes Interesse**)*

- Datenübermittlung an die Presse wegen Spielergebnissen oder Veranstaltungsberichten

*Zulässig, wenn Verein dabei **eigene Interessen** hat und keine überwiegenden Interessen des Betroffenen, aber Auslegungssache, daher besser pauschale Einwilligungserklärung für solche Fälle, wobei jederzeit Widerruf möglich ist.*

- Veröffentlichung von Mitglieder- oder Spendendaten auf der Vereinshomepage oder in der Mitgliederzeitung

*Zulässig nur auf der Basis einer **Einwilligungserklärung***

- Datenweitergabe aufgrund Outsourcing z.B. bei Versand Mitgliederzeitung, Versicherungen, Beitragseinzug, Mitgliederverwaltung

*Zulässig im Rahmen einer **Auftragsverarbeitung** nach Art. 28 DSGVO*

Muss ein Datenschutzbeauftragter bestellt werden?

Datenschutzbeauftragter

Ein (interner oder externer) Datenschutzbeauftragter **muss** bestellt und an Aufsichtsbehörde **gemeldet** werden, wenn **§ 38 BDSG**

- **in der Regel** mindestens 10 Personen **ständig** mit der **automatisierten** Verarbeitung von personenbezogenen Daten beschäftigt (=befasst) werden,
- gleich ob ehrenamtlich oder entgeltlich,
- z.B. Mitgliederverwaltung, Buchhaltung, Ehrungen, Presse

Meldung an die Aufsichtsbehörde online unter „lda.dsb-meldung.de“

Muss ein Datenschutzbeauftragter bestellt werden?

- **„Automatisierte“ Verarbeitung** liegt vor, wenn im Rahmen der jeweiligen Aufgabenstellung auf die automatisierte Datenverarbeitung des Vereins tatsächlich zugegriffen wird oder zugegriffen werden kann. "Automatisiert" ist danach nicht nur eine Verarbeitung mit Hilfe eines PCs, eines Laptops oder eines sonstigen EDV-Geräts, sondern auch bei Verwendung eines Mobiltelefons, in dessen Adressverzeichnis z.B. Kontaktdaten von Vereinsmitgliedern erfasst sind. Einbezogen in die "Automatisierung" ist auch die Bearbeitung von E-Mails, die beim Verein eingehen.
- Unerheblich ist für das Kriterium **"In der Regel"**, wie häufig oder intensiv auf die Daten zurückgegriffen wird, maßgeblich ist vielmehr, ob es zur regelmäßigen Aufgabenwahrnehmung gehört, personenbezogene Daten automatisiert zu bearbeiten.
- Als **"ständig"** ist die "Beschäftigung" einmal zu verstehen, wenn es sich nicht von vorne herein um eine nur vorübergehende Tätigkeit handelt wie bei der einmaligen Aufgabenstellung eines Vereinsmitarbeiters, z.B. für eine konkrete Einzelveranstaltung Teilnehmerdaten zu erfassen. Zum anderen liegt nach der Auffassung des Landesamts für Datenschutzaufsicht in Bayern eine "ständige" Beschäftigung nur dann vor, wenn die Person, die mit der Datenverarbeitung befasst ist, ihre überwiegende Zeit, die sie für den Verein aufbringt, mit der automatischen Datenverarbeitung zu tun hat.

Muss ein Datenschutzbeauftragter bestellt werden?

Im Verein können daher ohne Weiteres auch mehr als 10 Personen regelmäßig Zugriff auf die automatisierten Datenbestände der Vereinsmitglieder nehmen,

- ▶ beispielsweise zur Organisation von wöchentlichen Proben, Trainingseinheiten, Spielen oder Veranstaltungen, ohne dass deshalb ein Datenschutzbeauftragter bestellt werden müsste,
- ▶ da hier zwar eine wiederkehrende und häufige, aber keine ständige Datenverarbeitung vorliegt, der zeitliche Aufwand für die Datenverarbeitung vielmehr im Verhältnis zur Gesamtzeit, die für den Verein aufgebracht wird, weniger als die Hälfte ausmacht.

Nachdem das neue BDSG entgegen der bisherigen Fassung bei den Erfordernissen zur Bestellung eines Datenschutzbeauftragten ausdrücklich nur noch auf eine ständige Beschäftigung mit einer "automatisierten Verarbeitung" abstellt, ist davon auszugehen,

- ▶ dass beispielsweise Übungsleiter oder Kursleiter, denen für ihren Bereich lediglich ausgedruckte Teilnehmerlisten zur Verfügung gestellt werden, damit nicht zu dem Personenkreis zählen, die es für die Bestellung eines Datenschutzbeauftragten zu berücksichtigen gilt.
- ▶ Anders dagegen beim Schriftführer oder Kassier

Welche formalen Datenschutzvorgaben müssen im Verein beachtet werden? (Auftragsverarbeitung)

Sobald Verantwortliche (z.B. des Vereins) Dienstleistungen in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag von anderen Unternehmen verarbeiten zu lassen, besteht die Pflicht, dazu einen **schriftlichen Vertrag** zur Auftragsverarbeitung abzuschließen. **Wesentlich** für die Auftragsverarbeitung ist, dass die Verantwortung zum Datenschutz beim (ursprünglich) Verantwortlichen verbleibt und diesem die Verarbeitung durch den Auftragsverarbeiter zugerechnet wird.

Merke:

Die Entscheidung

- über die Verarbeitungsmittel und -zwecke bleibt beim Verantwortlichen,
- über die technisch-organisatorischen Fragen der Verarbeitung wird sie auf den Auftragsverarbeiter delegiert.

Welche formalen Datenschutzvorgaben müssen im Verein beachtet werden? (Auftragsverarbeitung - Beispiele)

Auftragsverarbeitung - ja

- Externe Lohn- und Gehaltsabrechnungen
- Outsourcing personenbezogener Daten auf Clouds
- Wartung und Fernzugriffe, wenn dabei Zugriff auf Daten möglich
- Hosting von Webseiten auf Fremdserver (Bilder !), solange nicht nur rein statistische Daten
- Betreuung von Kontaktformularen oder Anfragen, ohne dass inhaltliche Betreuung erforderlich
- Auslagerung von Datenspeicherungen

Auftragsverarbeitung – nein

- Inanspruchnahme fremder Fachleistungen bei eigenständiger Verantwortung
 - Berufsgeheimnisträger wie Steuerberater, Rechtsanwälte, Betriebsärzte, WP
 - Bankinstitute für Geldtransfer
 - Postdienste für Brieftransport
 - Schulungsleiter oder Tagungshotel

Datenschutzerklärung

- Folgen aus der rechtmäßigen Datenverarbeitung -

Worum geht es ?

Die DSGVO verlangt zusätzliche Angaben in der Datenschutzerklärung des Vereins, wenn er **erstmalig** personenbezogene Daten erfasst, u.a. auf welcher Rechtsgrundlage der Verein zur Datenverarbeitung berechtigt ist oder dass die Betroffenen verschiedene Rechte zur Schutz ihrer Daten haben.

Worauf ist zu achten ?

Befassen Sie sich mit den rechtlichen Grundlagen zu den bestehenden Hinweispflichten gegenüber den Betroffenen.

Problem:

„zum Zeitpunkt der Erhebung“ ./.. Verweis auf Homepage
(wohl unzulässig bei Medienbruch)

Klausel im Aufnahmeantrag (Muster)

„Die im Aufnahmeantrag angegebenen personenbezogenen Daten, insbesondere Name, Anschrift, Telefonnummer, Bankdaten, sind allein zum Zwecke der Durchführung des entstehenden Mitgliedschaftsverhältnisses notwendig und erforderlich und werden auf Grundlage gesetzlicher Berechtigungen erhoben.

Die Datenschutz-Informationen gemäß Art. 12 ff DSGVO sind dem beigefügten Merkblatt zu entnehmen.“

Achtung: Kein Medienbruch!

Datenschutzrichtlinie statt Merkblatt

Muster zur Information bei Datenerhebung (Datenschutzerklärung)

Name und Kontaktdaten des Verantwortlichen	
Name und Kontaktdaten des Datenschutzbeauftragten	
Zweck der Datenverarbeitung	Mitgliederverwaltung,
Rechtsgrundlage für die Verarbeitung	Vertragserfüllung, Interesse, Einwilligung
Berechtigte Interessen an der Verarbeitung	Interne Verwaltung, Verbandsmitgliedschaft, Ehrungen, Vereinszeitschrift, Versicherungsschutz
Kategorien der Daten, die verarbeitet werden	Name, Adresse, Geburtsdatum, Konto
Quelle, aus denen die Daten stammen	Betroffener selbst /Dritter
Empfänger der Daten (intern/extern)	
Dauer der Speicherung	Solange Zweck zu erfüllen ist, gesetzliche Aufbewahrungsfristen
Rechte der Betroffenen	Recht auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Datenübertragbarkeit, Widerspruch, Beschwerderecht



Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lida.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf abrufbar.

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:
TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@waldermuehler-tsv.de	02.03.2018	<ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern 	Beschäftigte	<ul style="list-style-type: none"> Name und Adressen der Beschäftigten ggf. Religionszugehörigkeit Eindeutige Kennzahlen zur Steuer/ Sozialabgaben 	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@waldermuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	<ul style="list-style-type: none"> Name und Adressen Eintrittsdatum Sportbereiche 	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@waldermuehler-tsv.de	28.02.2018	Außendarstellung	<ul style="list-style-type: none"> Mitglieder Webseitenbesucher 	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@waldermuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@waldermuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenschanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Wer überwacht die Einhaltung des Datenschutzes im Verein?

Von staatlicher Seite kontrolliert die Datenschutz-Aufsichtsbehörde. Diese darf Informationen anfordern , Datenschutzprüfungen vornehmen, den Zugang zu Informationen fordern und **Bußgelder** verhängen.

Zuständig für Vereine:

Datenschutzaufsichtsbehörde in Bayern
für den nicht-öffentlichen Bereich

Adresse:

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27, 91522 Ansbach
Telefon: 0981 53-1300

www.lida.bayern.de

Hilfestellungen unter

<https://www.lida.bayern.de/de/kleine-unternehmen.html>

Checkliste für Vereine

Datenschutzbeauftragter

Muss ein DSB bestellt werden?

- Ja
- Nein (weniger als 10 Personen ständig im regelmäßigen Umgang mit personenbezogenen Daten)

Verzeichnis von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

- Ja (wegen regelmäßiger Verarbeitung von personenbezogenen Daten)
- Nein

Datenschutzverpflichtung von Beschäftigten

Ist eine solche Verpflichtung durchzuführen?

- Ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
- Nein

Informations- und Auskunftspflichten

Bestehen Informationspflichten?

- Ja (Antrag, Anhang, Website)
- Nein

Checkliste für Vereine

Löschen von Daten

Gibt es Anforderungen zur Datenlöschung?

- Ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
- Nein

Sicherheit

Müssen Daten besonders gesichert werden?

- Ja
- Nein (etablierte Standardmaßnahmen ausreichend)

Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

- Ja (sowohl mit dem Webanbieter als auch mit externem Lohnabrechner)
- Nein

Datenschutzverletzungen

Müssen bestimmte Vorfälle gemeldet werden?

- Ja (aber nur bei relevanten Risiken, per Online beim BayLBDA)
- Nein

Datenschutz-Folgeabschätzung

Muss eine DSFA durchgeführt werden?

- Ja
- Nein (da kein hohes Risiko besteht)

Bild urheberrechtlich geschützt



Vielen Dank

und

viel Erfolg bei
Ihrer Arbeit

RA Richard Didyk, München
kanzlei.didyk@t-online.de