



Volksbank
Allgäu-Oberschwaben eG

Für die **MENSCHEN**. Für die **HEIMAT**.

Vereinsforum



EU-Datenschutzgrundverordnung

3. Juli 2018



weiter denken...



Marcel Müller

IT-Spezialist (Schwerpunkt
Prüfungsdienst Banken)

Diplom-Kaufmann

Verbandsprüfer

Datenschutzbeauftragter (TÜV)

Certified Compliance-Officer

IT-Sicherheitsmanager (ADG)

10 Jahre tätig in einer Primärbank;

Neuntes Jahr tätig bei einer WP-
Gesellschaft

Aktuelle Tätigkeiten

IT-Revision

Datenschutzbeauftragter in Bank und
Industrie

IT-Sicherheitsbeauftragter in Banken

Compliance-Beauftragter in Banken

Referent

Beteiligung an einem Fachbuch zum
Datenschutz

Vereinszugehörigkeit

Fußballverein – aktiv bei den
„attraktiven“ Herren (AH) und
Jugendtrainer



Agenda

1. Rechtliche Grundlagen und Überblick
2. Schriftliche Regelungen zum Datenschutz
3. Verschwiegenheitsverpflichtung
4. Informationspflicht
5. Betroffenenrechte
6. Datenspeicherung
7. Transparenzpflichten
8. Rechtmäßigkeit der Verarbeitung
9. Umgang mit Fotos
10. Auftragsverarbeitung



Agenda

- 11. IT-Sicherheit
- 12. Verzeichnis Verarbeitungstätigkeiten
- 13. Technisch-organisatorische Maßnahmen
- 14. Datenschutzfolgenabschätzung
- 15. Videoüberwachung
- 16. Compliance-Nachweis
- 17. Verfahren bei Datenschutzverletzungen
- 18. Bußgeldvorschriften
- 19. Tipps für Vereine
- 20. Anhang / Anlagen



Rechtliche Grundlagen und Überblick

Ziele der EU-Datenschutzgrundverordnung (EUDSGVO)

- Harmonisierung der europäischen Datenschutzregelungen.
- Schutz der Persönlichkeitsrechte (Grundrecht)

Ursprüngliche Zielgruppe

- Große international agierende Unternehmen wie google, Facebook und Apple

Zeitliche Anwendung

- Die EUDSGVO gilt für Datenerhebungen ab dem 25. Mai 2018.



Rechtliche Grundlagen und Überblick

Sachlicher Anwendungsbereich

Diese Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

Räumlicher Anwendungsbereich

Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.



Rechtliche Grundlagen und Überblick

Grundsatz „Präventivverbot mit Erlaubnisvorbehalt“

Die Verordnung regelt die **Verarbeitung von personenbezogenen Daten natürlicher Personen**.

Jegliche Form der Datenverarbeitung ist verboten, es sei denn,

1. die Datenverarbeitung ist durch Rechtsvorschrift legitimiert oder
2. der Betroffene hat eingewilligt.



Rechtliche Grundlagen und Überblick

„**Verantwortlicher**“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

„**Auftragsverarbeiter**“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;



Rechtliche Grundlagen und Überblick

„**Personenbezogene Daten**“ sind alle **Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person“) **beziehen**;

- 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.



Rechtliche Grundlagen und Überblick

Rechenschaftspflicht nach Artikel 5 DSGVO

(1) Personenbezogene Daten müssen

- a) ... auf rechtmäßige Weise ... („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“),
- b) ... für festgelegte, eindeutige und legitime Zwecke ... („Zweckbindung“),
- c) ... auf das notwendige Maß beschränkt ... („Datenminimierung“),
- d) ... sachlich richtig ... („Richtigkeit“),
- e) ... erforderlich ... („Speicherbegrenzung“) und mit
- f) ... angemessener Sicherheit ... („Integrität und Vertraulichkeit“)
verarbeitet werden.



Rechtliche Grundlagen und Überblick

Rechenschaftspflicht nach Artikel 5 DSGVO

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

(„Beweislastumkehr“)



Rechtliche Grundlagen und Überblick

Checkliste - Bestellungspflicht Datenschutzbeauftragter

1. Sind mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt?
 - „Ständig beschäftigt“ ist, wer z. B. permanent Mitgliederverwaltung macht – „nicht ständig beschäftigt“ ist dagegen bspw., wer als Übungsleiter nur mit den Namen seiner Mannschaft umgeht.
2. Nimmt der Verein Verarbeitungen vor, die einer Datenschutzfolgenabschätzung unterliegen?
3. Liegt die Kerntätigkeit des Vereins in Verarbeitungsprozessen, welche aufgrund ihrer Art, ihres Umfangs oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Person erforderlich macht?



Rechtliche Grundlagen und Überblick

Checkliste - Bestellungspflicht Datenschutzbeauftragter

4. Besteht die Kerntätigkeit in der Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten?

Besondere Kategorien von Daten sind personenbezogene Daten, aus denen die rassische, ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben und der sexuellen Orientierung.

Als Beispiele kommen die Religionszugehörigkeit, Parteizugehörigkeit sowie Angaben über Krankheiten in Betracht. Hinzukommen muss jedoch auch hier, dass die Kerntätigkeit des Vereins in der Verarbeitung vorgenannter Daten liegt. Dies ist immer dann der Fall, wenn ohne die Verarbeitung dieser Daten der Zweck des Vereins nicht erreicht werden könnte.

Denkbar ist dies etwa bei Selbsthilfegruppen oder Vereinen mit politischer Zielrichtung.

Rechtliche Grundlagen und Überblick

Meldung des Datenschutzbeauftragten

Der Datenschutzbeauftragte ist der zuständigen Aufsichtsbehörde zu melden.

Meldeportale:

<https://www.baden-wuerttemberg.datenschutz.de/dsb-online-melden/>

<https://www.la-bayern.de/de/dsb-meldung.html>



Rechtliche Grundlagen und Überblick

Aufgaben des Beauftragten für den Datenschutz

Alt- BDSG: Der Beauftragte für den Datenschutz wirkt auf die Einhaltung dieses Gesetzes und anderer Vorschriften über den Datenschutz hin.

Neu-DSGVO: Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben: Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen...



Schriftliche Regelungen zum Datenschutz

Den Verein trifft die Pflicht, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festzulegen.

Entsprechende Datenschutzregelungen können entweder in die **Vereinssatzung** aufgenommen **oder in einem gesonderten Regelwerk** niedergelegt werden.

Es ist empfehlenswert, sich beim Aufbau der Datenschutzregelungen am Weg der Daten von der Erhebung über die Speicherung, Nutzung, Verarbeitung (insbesondere Übermittlung) bis zu ihrer Sperrung und Löschung zu orientieren. (Prozessorientierung)



Schriftliche Regelungen zum Datenschutz

Regelungsinhalte (I)

- Verwendete Daten (z.B. Name, Vorname, Adresse, E-Mailadresse usw.)
- Betroffener Personenkreis (z.B. Vereinsmitglieder, Teilnehmer an Veranstaltungen oder Lehrgängen, Besucher von Veranstaltungen)
- Zweckbindung der Datennutzung

Die bloße Wiedergabe des Wortlauts der Bestimmungen der DS-GVO bzw. des BDSG-neu sind in keinem Fall ausreichend.

Diese Datenschutzordnung sollte von der Mitgliederversammlung beschlossen werden



Schriftliche Regelungen zum Datenschutz

Regelungsinhalte (II)

- Welche Daten werden beim Vereinseintritt für die **Verfolgung des Vereinsziels** und für die **Mitgliederbetreuung und -verwaltung** notwendigerweise erhoben?
- Welche Daten werden für welche **andere Zwecke** des Vereins oder zur Wahrnehmung der **Interessen Dritter** bei den Mitgliedern in Erfahrung gebracht?
- Welche **Daten** werden **von Dritten** erhoben, wobei hier auch der Erhebungszweck festzulegen ist?
- Welche Angaben sind für Leistungen des Vereins erforderlich, die nicht erbracht werden können, wenn der Betroffene nicht die dafür erforderlichen Auskünfte gibt?



Schriftliche Regelungen zum Datenschutz

Regelungsinhalte (III)

- Welcher **Funktionsträger** oder sonstige Dritte hat zu welchen Daten Zugang?
- Zu welchem Zweck darf er Daten von Mitgliedern und Dritten verarbeiten und nutzen?.
- Welche Daten werden zu welchem Zweck im Wege der **Auftragsdatenverarbeitung** verarbeitet?
- Zu welchem Zweck dürfen die Empfänger die erhaltenen Daten nutzen und können sie sie weitergeben?
- Welche Daten werden üblicherweise am „**Schwarzen Brett**“ oder in den **Vereinsnachrichten** offenbart und welche in das Internet oder Intranet eingestellt?



Schriftliche Regelungen zum Datenschutz

Regelungsinhalte (III)

- Ist ein Verein verpflichtet, die Daten seiner Mitglieder regelmäßig einer Dachorganisation - beispielsweise einem Bundes- oder Landesverband - zu übermitteln (etwa in Form von Mitgliederlisten), sollte dies in der Vereinssatzung geregelt werden.



Verschwiegenheitsverpflichtung

Datengeheimnis, Verpflichtung auf den Datenschutz, Unterrichtung

Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen.

Bei nicht öffentlichen Stellen sind die Beschäftigten bei Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu verpflichten.

- Vorstand
- Kassierer
- Beschäftigte...





Informationspflicht

Warum und wann?

Aus Gründen der Transparenz hat der Verein aktiv zum Zeitpunkt der Erhebung (z.B. im Mitgliedsantrag) umfassend die Informationspflichten des Art. 13 DS-GVO zu erfüllen:

Aufklärung wie die personenbezogenen Daten der Mitglieder (oder Dritter) verarbeitet werden.



Informationspflicht

Allgemeine Inhalte (I)

- Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- Kontaktdaten des Datenschutzbeauftragten
- Zwecke und Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen i. S. d. Art. 6 Abs. 1 lit. f) DS-GVO
- Empfänger oder Kategorien von Empfängern
- Absicht von Drittlandtransfer sowie Hinweis auf (Fehlen von) Garantien zur Datensicherheit
- Speicherdauer der personenbezogenen Daten



Informationspflicht

Allgemeine Inhalte (II)

- Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Datenschutz-Aufsichtsbehörde
- Pflicht zur Bereitstellung der Daten
- Automatisierte Entscheidungsfindung einschließlich Profiling





Informationspflicht

Konkrete Inhalte (III)

- Vereinsmitglieder sind bei der Datenerhebung darauf aufmerksam zu machen, welche Angaben für die Mitgliederverwaltung und welche für die Verfolgung des Vereinszwecks bestimmt sind.
- Sollen Daten zum Zwecke der Verfolgung des Vereinsziels oder der Mitgliederverwaltung und -betreuung an andere Stellen übermittelt werden (etwa an einen Dachverband, damit dieser Turniere ausrichten kann, an eine Unfallversicherung oder an die Gemeinde), muss auch darauf hingewiesen werden.



Informationspflicht

Konkrete Inhalte (IV)

- Insbesondere ist das Mitglied darauf hinzuweisen, welche Angaben im Vereinsblatt veröffentlicht oder in das Internet eingestellt werden, etwa im Falle der Wahl als Vorstandsmitglied.
- Kann dem Vereinsmitglied ein bestimmter Vorteil, etwa ein Versicherungsschutz, nur gewährt werden, wenn es dazu bestimmte Angaben macht, muss es darauf aufmerksam gemacht werden, welche Nachteile die Verweigerung dieser Informationen mit sich bringt.



Informationspflicht

Weitere Anforderungen / Schlussfolgerungen

- Der Datenschutzhinweis ist im Zusammenhang mit der Erhebung von personenbezogenen Daten ab dem 25. Mai 2018 ohne Medienbruch auszugeben.
- Für vorher erhaltene Daten gilt Bestandsschutz (kein Hinweis erforderlich).
- **Ein Hinweis auf die Abrufmöglichkeit genügt nicht.**
- Für den Datenschutzhinweis reicht eine „einseitige“ Ausgabe, eine Unterschrift des Mitglieds ist nicht erforderlich.



Informationspflicht

Weitere Anforderungen / Schlussfolgerungen

- Wird die Beitrittserklärung papierhaft von Hand befüllt, so sind dem Mitglied die Informationen nach Art. 13 DSGVO auch schriftlich auszuhändigen. (Kein Medienbruch)
- Ausgabe Datenschutzhinweis an
 - Vereinsmitglieder
 - Internetauftritt
 - Social Media Fanpage
 - (hauptamtliche) Beschäftigte und Bewerber
 - ...



Informationspflicht

Werden personenbezogene Datei auf andere Weise als bei der betroffenen Person erhoben, so richten sich die Informationspflichten nach Art. 14 Abs. 1 und Abs. 2 DS-GVO.

Zusätzlich zu Art. 13 DSGVO muss der Verein die betroffene Person über die **Kategorie** der verarbeiteten personenbezogenen Daten und über die **Quelle** der erhobenen Daten informieren.

Der Verein muss diese Informationen innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach der Erhebung erteilen.



Informationspflicht Internet

Der für die Verarbeitung Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen, die sich auf die Verarbeitung personenbezogener Daten beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln.

Websites benötigen eine Datenschutzerklärung – an dieser Rechtslage ändert sich nichts. Es sind **künftig mehr Informationen** bereitzustellen.

- Rechtsgrundlagen
- Erforderlichkeit für einen Vertragsabschluss
- ob eine andere Verpflichtung zur Bereitstellung der Daten besteht...



Informationspflicht Internet

Besonderen Wert auf datenschutzkonforme Erklärungen legen!

1. Facebook „Like“-Buttons oder ähnlicher Social-Plugins anderer Anbieter (Twitter, LinkedIn etc.),
2. Webformulare (Kontaktformulare, Newsletter etc.),
3. Cookies (Informationen zu Zweck, Empfänger der Daten etc.)
4. Analyse-Tools (wie Piwik oder etracker) und



Informationspflicht Internet

Fanpage-Betreiber sind mitverantwortlich für Datenschutz

<https://www.golem.de/news/eugh-urteil-fanpage-betreiber-sind-mitverantwortlich-fuer-datenschutz-1806-134772.html>



Muster_Datenschutzhinweis Internet.pdf



Informationspflicht Internet

Die Informationen müssen gem. Art. 13 (1) DS-GVO „bei Erhebung“ der personenbezogenen Daten gegeben werden.

Daher sollte die Datenschutzerklärung – wie bislang – regelmäßig **mit nur einem Klick erreichbar** sein (Artikel–29-Datenschutzgruppe, Working Paper 260, S. 8; zum BDSG a. F. bereits *Wintermeier*, ZD 2013, 21 (23 f.); beim Impressum sind hingegen zwei Klicks ausreichend, BGH, Urt. v. 20. 3. 2006 – I ZR 228/03, MMR 2007, 40). **Dem kann durch die Aufnahme des Links im Header oder Footer neben dem Impressum nachgekommen werden.**

<https://www.datenschutzbeauftragter-info.de/eu-grundverordnung-websitebetreiber-aufgepasst/>





Betroffenenrechte

1. **Recht auf Datenportabilität**

2. **Berichtigungsanspruch**

Neu ist, dass der Verantwortliche, sofern er eine Berichtigung vornimmt, auch Dritte informieren muss, denen er die betroffenen Daten offengelegt hat.

3. **Auskunftsanspruch**

4. **Löschrecht**



Datenspeicherung

Die Löschpflicht gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten **sowie für** die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen.



Datenspeicherung

Artikel 4 Nr. 6 DSGVO konkretisiert das „Dateisystem“ als jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Nach dem „Beckschen“ Kommentar umfasst der Begriff „Dateisystem“ explizit auch manuelle Sammlungen wie z.B. Akten, die gleichartig aufgebaut sind.



Datenspeicherung

Vorgehen - Neu: Löschungen nachweislich durchführen!

1. Verwendete Datenarten identifizieren.
2. Gesetzliche Aufbewahrungsfrist recherchieren.
3. Standardlöschfrist (bei Ablauf der Aufbewahrungsfrist) feststellen.
4. Startzeitpunkt der Löschfrist identifizieren

Schriftgutbezeichnung	Aufbe- wah- rungs- frist in Jahren	zulässige Aufbewah- rungsform*		Anmerkungen
		bild- lich	inhalt- lich	
Mitgliedschaft				Geschäftspolitische Entscheidung, ob Aufbewahrung im Original oder, ob nach Ablauf einer bestimmten Frist elektronisch archiviert und das Original vernichtet wird
- Ausschluss	10 6			Sofern Buchungsbeleg
- Beitritts-/Beteiligungserklärung	3			Die Unterlagen, aufgrund deren die Eintragung in die Mitgliederliste erfolgt, sind drei Jahre aufzubewahren. Die Frist beginnt mit dem Schluss des Kalenderjahres, in dem das Mitglied ausgeschieden ist.
- Kündigung der Mitgliedschaft	10 6			Sofern Buchungsbeleg



Datenspeicherung

Weitere Beispiele:

- Bilanz- und Steuerdaten 10 Jahre
- Handelsbriefe (6 Jahre)
- Spielergebnisse (1 Saison)



Zusammenfassung der Transparenzpflichten

Ziel der DSGVO: Mehr **Transparenz** und **mehr Rechte** für den **Betroffenen** auf drei Ebenen:





Rechtmäßigkeit der Verarbeitung

Prüfschema auf Basis der „Datenschutzhinweis“

Ein Verein darf – auch ohne Einwilligung – solche Daten erheben,

- a) die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind.

Mitgliedsvertrags/Satzung (vgl. schriftliche Regelungen)

- b) wenn er an der Datenverarbeitung ein **überwiegendes berechtigtes Interesse** hat.

(Art. 6 Abs. 1 lit. f) DS-GVO)

Eine Einwilligungserklärung ist erforderlich, wenn beide Fragen verneint werden.



Rechtmäßigkeit der Verarbeitung

Die Interessenabwägung verlangt für die Feststellung der Rechtmäßigkeit der Datenverarbeitung **eine dreistufige Prüfung.**

Bezogen auf den Zweck der vertrieblichen Nutzung ist eine konkrete Werbe- oder Marketingmaßnahme rechtskonform, wenn sich die folgenden drei Kontrollfragen mit „Ja“ beantworten lassen.

- 1.) Besteht ein berechtigtes Interesse des Vereins an der geplanten Datenverarbeitung?
- 2.) Ist die Verarbeitung erforderlich, um dieses Interesse zu wahren?
- 3.) Überwiegt kein den Schutz personenbezogener Daten erforderndes berechtigtes Interesse oder Grundrecht oder keine entsprechende Grundfreiheit der betroffenen Person?



Rechtmäßigkeit der Verarbeitung

Beispiele für Interessenabwägung

- **Ein berechtigtes Interesse besteht grundsätzlich nur an den Daten, die für eine eindeutige Identifizierung erforderlich und ausreichend sind**, d.h. Name, Vorname, Anschrift und Geburtsdatum, nicht jedoch Personalausweis- oder Passnummer.
- So kann es zulässig sein, beim Verkauf von Eintrittskarten etwa für ein Fußballspiel Identifizierungsdaten von dem Verein nicht bekannten Zuschauern zu erheben, um abzuklären, ob gegen sie ein Stadionverbot ausgesprochen worden ist oder ob sie als gewaltbereit anzusehen sind.

.



Rechtmäßigkeit der Verarbeitung

Beispiele für Interessenabwägung

- **Veröffentlichungen in Verbandszeitschriften** und in sonstigen allgemein zugänglichen Publikationen dürfen genauso wie Pressemitteilungen und -auskünfte nur in personenbezogener Form erfolgen, **wenn** es sich um ein **Ereignis von öffentlichem Interesse** handelt.
- Die Übermittlung von Mitgliederdaten an politische Parteien bzw. Gruppierungen oder an Kandidaten bei Wahlen für **Zwecke der Wahlwerbung** ist ohne schriftliche Einwilligung der Betroffenen unzulässig.



Rechtmäßigkeit der Verarbeitung

Beispiele für Interessenabwägung

- Verlangt eine Gemeindeverwaltung, die an einen Verein freiwillige finanzielle Leistungen erbringt, deren Höhe von der Mitgliederzahl oder der Anzahl bestimmter Mitglieder (etwa der Anzahl der Jugendlichen, die in Mannschaften mitspielen) abhängt, **zu Kontrollzwecken die Vorlage von Listen mit den Namen der Betroffenen**, ist der Verein grundsätzlich berechtigt, diese Daten zu übermitteln, weil es sowohl zur Wahrnehmung berechtigter eigener Interessen - nämlich um in den Genuss der Vereinsförderung durch die Gemeinde zu kommen - als auch zur Wahrnehmung berechtigter Interessen eines Dritten - der Gemeinde - erforderlich ist und Interessen oder Grundrechte der betroffenen Vereinsmitglieder einer Datenübermittlung nicht überwiegen.



Rechtmäßigkeit der Verarbeitung

Beispiele für Interessenabwägung

- Vorsicht bei Kindern unter 16 Jahren
- Erkundigungen bei Dritten (etwa als Zuchtverband bei den Käufern von Tieren einer bestimmten Hunderasse) - oder Kontrollen (etwa als Tierschutzverein) bedürfen unbedingt einer Zustimmung, selbst wenn sich die Vereinigung solches zum satzungsmäßigen Ziel gesetzt hat.
- Erfolgt die Informationsausgabe an einen überschaubaren Raum wie das Vereinsheim oder ist es nicht überschau-/kontrollierbar wie das Internet?



Rechtmäßigkeit der Verarbeitung

Beispielhafte Zwecke für erforderliche Einwilligungserklärungen

- Veröffentlichung von Fotos auf der Webseite des Vereins
- Veröffentlichung von Geburtsdaten/Jubiläen im Vereinsblatt/am schwarzen Brett
- Werbung von Dritten
- Datenweitergabe an Dritte

Anders als das BDSG, das für Einwilligungen grundsätzlich die Schriftform vorsieht, ermöglicht die DS-GVO die **Einwilligung schriftlich, elektronisch, mündlich oder sogar konkludent abzugeben.**



Rechtmäßigkeit der Verarbeitung

Voraussetzungen/Anforderungen für die Einwilligungserklärung

- Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen können**, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- Einwilligung **in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache** (informierte Einwilligung; hervorheben).
- **Sachverhalte müssen klar unterschieden und gesondert angekreuzt werden.**
- **Jederzeitiges Widerrufsrecht vereinbaren.** Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
- Die Einwilligung muss **freiwillig** erteilt werden (Kopplungsverbot; Hervorhebung => freie Entscheidung).



Rechtmäßigkeit der Verarbeitung

Vorhandene, die Anforderungen erfüllende Einwilligungserklärungen haben weiterhin für die erfassten Zwecke Bestand.



Muster Einwilligung Internet.pdf



Einwilligung_Verwendung von Fotos.pdf



Rechtmäßigkeit der Verarbeitung

Minderjährige (I)

Kinder und Jugendliche können in die Verarbeitung ihrer personenbezogenen Daten **selbst einwilligen, wenn sie in der Lage sind, die Konsequenzen** der Verwendung ihrer Daten **zu übersehen** und sich deshalb auch verbindlich dazu zu äußern.

Maßgeblich ist der jeweilige Verwendungszusammenhang der Daten und der **Reifegrad bzw. die Lebenserfahrung** des Betroffenen.

Bei Kindern unter 13 Jahren ist regelmäßig davon auszugehen, dass sie die Konsequenzen der Verwendung ihrer Daten **nicht** übersehen können.



Rechtmäßigkeit der Verarbeitung

Minderjährige (II)

Ist die Einsichtsfähigkeit zu verneinen, ist die Verarbeitung seiner personenbezogenen Daten nur mit Einwilligung aller Sorgeberechtigten zulässig. Empfehlung Rücklaufkontrolle!

<https://www.datenschutzbeauftragter-info.de/dsgvo-informationspflicht-interessenabwaegung-bei-daten-von-kindern/>



Rechtmäßigkeit der Verarbeitung

Beschäftigtendatenschutz für **Personen in einem abhängigen hauptamtlichen Verhältnis** (§ 26 BDSG-neu).

Danach dürfen **personenbezogene Daten von Beschäftigten** für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.

Sofern der Verein eigene Beschäftigte hat, müssen deren Personaldaten getrennt von den sonstigen Daten, insbesondere den Mitgliederdaten, gespeichert werden. (Trennungsprinzip)



Rechtmäßigkeit der Verarbeitung

Veröffentlichung im Internet (I)

Veröffentlichung personenbezogener Daten durch einen Verein im Internet **grundsätzlich unzulässig, wenn sich der Betroffene nicht ausdrücklich damit einverstanden erklärt hat.**

Ausnahmen:

- **Funktionsträger eines Vereins** dürfen auch ohne ausdrückliche Einwilligung mit ihrer „dienstlichen“ Erreichbarkeit in das Internet auf der Homepage des Vereins eingestellt werden.
- Die von einem Verein oder Verband **ausgerichteten Veranstaltungen** (z. B. Spiele in der Bezirksklasse) sind öffentlich. Die Namen und die Ergebnisse werden im Rahmen solcher Veranstaltungen üblicherweise öffentlich bekannt gegeben.



Rechtmäßigkeit der Verarbeitung

Veröffentlichung im Internet (II)

- **Informationen über Vereinsmitglieder** (z.B. Spielergebnisse und persönliche Leistungen, Mannschaftsaufstellungen, Ranglisten, Torschützen usw.) **oder Dritte** (z.B. Spielergebnisse externer Teilnehmer an einem Wettkampf) *können ausnahmsweise auch ohne Einwilligung kurzzeitig ins Internet eingestellt werden, wenn die Betroffenen darüber informiert sind und keine schutzwürdigen Interessen oder Grundrechte und Grundfreiheiten der Veröffentlichung im Einzelfall überwiegen.*



Rechtmäßigkeit der Verarbeitung

Veröffentlichung im Internet (III)

Um den Eingriff in das Persönlichkeitsrecht in Grenzen zu halten, dürfen bei derartigen Veröffentlichungen jedoch **allenfalls Nachname, Vorname, Vereinszugehörigkeit und eventuell in begründeten Ausnahmefällen der Geburtsjahrgang** aufgeführt werden.

Bei einer Veröffentlichung eines Fotos, des vollen Geburtsdatums (Tag, Monat und Jahr), der privaten Anschrift oder der Bankverbindung des Betroffenen überwiegen dessen Interessen oder Grundrechts oder Grundfreiheiten berechnigte Vereins oder Verbandes; sie wäre daher nur mit ausdrücklicher Einwilligung der Betroffenen zulässig.

Ergänzend muss - wie oben aufgeführt - sichergestellt sein, dass die Daten nach angemessener Zeit gelöscht werden.



Rechtmäßigkeit der Verarbeitung

Veröffentlichungen im Intranet (IV)

Wenn ein Verein seinen Mitgliedern und Funktionsträgern Informationen über das Internet **in passwortgeschützten Bereichen** (Intranet) zur Verfügung stellt, können über die Vergabe von Benutzerkennungen und Passwörtern individuelle Zugriffsberechtigungen eingerichtet werden.



Umgang mit Fotos im Internet

- Technische Maßnahmen reichen in keinem Fall aus, um das **Persönlichkeitsrecht** bei Bildern auch nur annähernd sicher zu schützen.
- Bei Filmen kommt es nicht darauf an, wie lange der Betroffene zu sehen ist.
- Nach § 22 KUG dürfen Bildnisse grundsätzlich nur mit schriftlicher Einwilligung des Abgebildeten verbreitet und veröffentlicht werden.
- Praxistipp: Sammeleinwilligung per Namensliste. Dabei sollte der Verwendungszweck sehr genau beschrieben sein.



Umgang mit Fotos im Internet

- **Ausnahmen von der Zustimmungspflicht nach § 23 KUG**
 - Bildnisse aus dem Bereich der Zeitgeschichte
 - Bilder, bei denen Personen nur Beiwerk von Landschaften o.ä. sind.
 - Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die Personen teilgenommen haben.
 - „Kunst“



Umgang mit Fotos im Internet

▪ Beispiele

- Jährlicher Faschingsumzug = Versammlung (keine Einwilligung)
- Foto von einem Fußballspiel = Versammlung (keine Einwilligung)
- Besuch eines Staatssekretärs = Person der Zeitgeschichte (keine Einwilligung)
- Foto einer vollbesetzten Zuschauertribüne = Personen sind Beiwerk (keine Einwilligung), sofern nicht einzelne Personen herangezoomt wurden.
- Hose/Trikot zerreißt, Genitalien sind zu sehen = Veröffentlichung ausgeschlossen.



Umgang mit Fotos im Internet

- **Beispiel Mannschaftsfoto:**
 - Mitwirken = stillschweigende Einwilligung darin, das Foto zu machen, **aber** nicht dass es auch im Internet veröffentlicht werden darf.
=> Unterschriftenliste zur Zustimmung der Veröffentlichung im Internet, sofern kein Teamentscheid.
=> Vorsicht: Stillschweigen ist hier nicht gleichbedeutend mit einer Zustimmung!



Umgang mit Fotos im Internet

- **Minderjährige**
 - Spielszenen bei Mannschaftsspielen und vom Training nicht ohne Einwilligung aller Sorgeberechtigten.
 - Kein Problem beim Besuch einer Person der Zeitgeschichte.



Umgang mit Fotos im Internet

- **Praxistipp**
 - Fragen Sie sich vor der Veröffentlichung des Fotos einer anderen Person, ob Sie es auch dann im Internet veröffentlichen würden, wenn Sie selbst auf dem Foto zu sehen wären.
 - Holen Sie schriftliche Einwilligungserklärungen ein.

Umgang mit Fotos bei Veranstaltungen

■ Praxistipp

- Allgemeine Hinweise, dass Fotos gemacht werden und dass beabsichtigt ist, diese auf der Homepage einzustellen.
- Damit eröffnen Sie erst Möglichkeiten zum Widerspruch.
- Der Hinweis ersetzt keine Einwilligung.



Auftragsverarbeitung

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit **Auftragsverarbeitern**, die hinreichend **Garantien** dafür bieten, **dass geeignete technische und organisatorische Maßnahmen** so **durchgeführt werden**, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Die Verarbeitung durch einen Auftragsverarbeiter erfolgt auf der Grundlage eines unbedingt zu erneuernden Vertrags!



Auftragsverarbeitung

Beispiel

- Datenhosting, z.B. Mitgliederlisten bei einem übergeordneten Verband oder Drittdienstleister, Spielberichtsbögen...



Muster_Verein_AVV.pdf

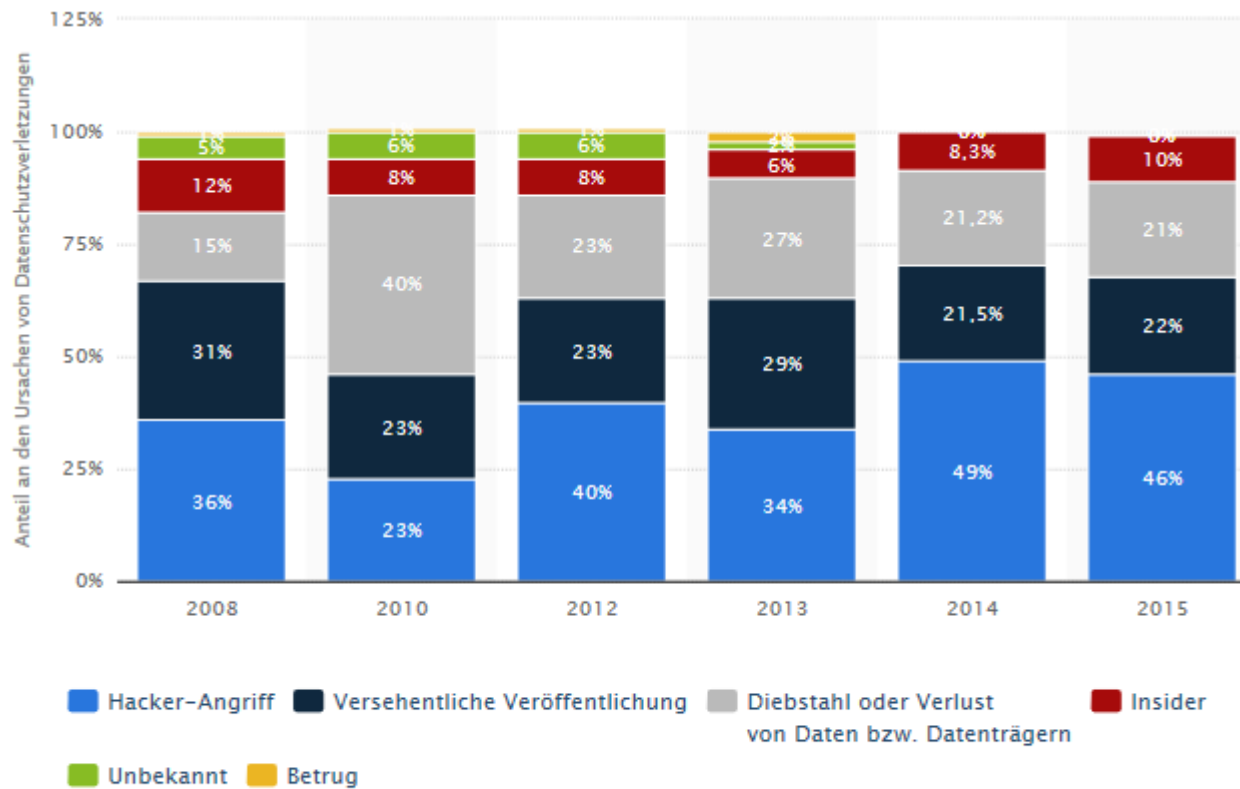


IT-Sicherheit

1. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen
2. Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert.



IT-Sicherheit





IT-Sicherheit

Von Bedeutung ist künftig ein risikobasierter Ansatz, d.h. die Ausrichtung der erforderlichen Maßnahmen an der Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken.

Dabei sind insbesondere folgende Risiken in den Blick zu nehmen:

1. unbeabsichtigte/unrechtmäßige Vernichtung und Veränderung,
2. unbeabsichtigter/unrechtmäßiger Verlust,
3. unbefugte Offenlegung,
4. unbefugter Zugang zu personenbezogenen Daten.

Dies begründet die Notwendigkeit einer stärker als bislang **formalisierten Risikoanalyse.**



IT-Sicherheit

1. Neu sind die Anforderung, ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Sicherheitsmaßnahmen zu etablieren ([Datenschutzmanagement](#)), sowie ein **Sicherheitskonzept**, das die getroffenen Maßnahmen darstellt.
2. Für die Risikoanalyse sowie die Datenschutzfolgeabschätzung sollte auf das von der Konferenz der unabhängigen Datenschutzbehörden entwickelte [Standard-Datenschutzmodell](#) zurückgegriffen werden.

<https://www.datenschutz.rlp.de/de/themenfelder-themen/standard-datenschutzmodell/>

BSI – B(austein) 1.5 Datenschutz



Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 DS-GVO hat jeder Verantwortliche ein Verzeichnis aller Verarbeitungstätigkeiten zu führen.

Ein Verein hat ein Verzeichnis zu führen, wenn mindestens eine der folgenden Eigenschaften vorliegt, auch wenn weniger als 250 Mitarbeiter beschäftigt werden:

- fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend,
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend oder
- ständig oder **regelmäßig stattfindend** (für kleine und Kleinvereine relevant)

Aktualisierung Mitgliederliste, Versand von Nachrichten an Mitglieder, Einzug von Mitgliedsbeiträgen, Anmeldung zu Wettkämpfen etc.)



Verzeichnis von Verarbeitungstätigkeiten

Muster



Muster_Verein_VVT.pdf



Muster_Verein_VVT Formblatt.pdf



Technisch-organisatorische Maßnahmen

Pseudonymisierung	<ul style="list-style-type: none">§ Zur internen Zuordnung werden Kundennummern verwendet, die nicht der Kontonummer entsprechen§ Die Verwaltung des Personals erfolgt nach Möglichkeit anhand der Personal- oder Benutzernummer
Verschlüsselung	<ul style="list-style-type: none">§ Verschlüsselungsmethoden werden stets auf dem aktuellem Stand der Technik gehalten§ Mobilgeräte kommunizieren mit dem internen Netzwerk ausschließlich über eine verschlüsselte VPN-Verbindung§ E-Mails mit sensiblem Inhalt werden stets verschlüsselt§ Hochvertrauliche Daten werden nach Möglichkeit in verschlüsselter Form gespeichert§ Mobile Datenträger werden auf dem Transportweg stets verschlüsselt§ Öffentlich zugängliche Webseiten verfügen stets über eine ausreichend starke https-Verschlüsselung§ Mobile BankingApps verfügen über eine ausreichend starke Verschlüsselung
Vertraulichkeit	<ul style="list-style-type: none">§ Es besteht ein Prozess für die Vergabe, Änderung und den Entzug von IT-Berechtigungen§ Für alle relevanten Anwendungen bestehen Berechtigungskonzepte, die nach dem Need-to-Know-Prinzip erstellt wurden§ Berechtigungen werden jährlich, kritische Berechtigungen werden halbjährlich auf deren Erforderlichkeit hin überprüft§ Es existieren abgestufte Schließkreise mit unterschiedlichen Zutrittsberechtigungen§ Es besteht ein Prozess zur Vergabe, Veränderung und zum Entzug von Schließberechtigungen§ Sensible Bereiche werden videoüberwacht§ Das Gebäude Linkenheim-Hochstetten wird durch eine Einbruchmeldeanlage gesichert§ Zugriffsmöglichkeiten auf Daten werden auf das erforderliche Maß beschränkt§ Es bestehen Vorgaben für Länge und Komplexität von Kennwörtern, die nach Möglichkeit technisch erzwungen werden§ Für hochvertrauliche Anwendungen ist eine Authentifikation ausschließlich mittels zweier voneinander unabhängigen Faktoren möglich



Technisch-organisatorische Maßnahmen

Integrität	<ul style="list-style-type: none">§ Dokumente und Vorlagen werden stets unter Angabe der vorgenommenen Änderungen versioniert§ Änderungen an Daten und Dokumenten werden protokolliert
Verfügbarkeit	<ul style="list-style-type: none">§ Virenschutz und Firewallsysteme werden stets aktuell gehalten§ Daten werden täglich inkrementell und monatlich vollumfänglich gesichert§ Es werden regelmäßig Rücksicherungstests durchgeführt§ Veränderungen an IT-Systemen durchlaufen stets einen standardisierten IT-Change- und Releasemanagement-Prozess
Belastbarkeit	<ul style="list-style-type: none">§ Für wichtige IT-Systeme werden ausreichend Ressourcen zur Verfügung gestellt
Physischer oder technischer Zwischenfall	<ul style="list-style-type: none">§ Es bestehen Datensicherungskonzepte§ Für zeitkritische Geschäftsprozesse existieren entsprechende Notfallkonzepte§ Für zeitkritische Geschäftsprozesse werden regelmäßig K-Fall-Tests durchgeführt§ Ein Prozess für den Umgang mit Stör- und IT-Sicherheitsvorfällen ist definiert§ Es besteht ein Konzept zum Umgang mit Datenpannen



Technisch-organisatorische Maßnahmen

Verfahren zur Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM	§ ISB und DSB sind bestellt
	§ Der Schutzbedarf der Geschäftsprozesse wird jährlich überprüft
	§ Das Schutzniveau der Anwendungen wird jährlich überprüft
	§ Abweichungen und Risikobewertungen werden vierteljährlich kommuniziert
	§ Vorab definierte Soll-Schutz-Maßnahmen werden regelmäßig überprüft
	§ Es finden in regelmäßigen Abständen interne Auditierungen statt
	§ Datenschutzvorfälle werden stets dokumentiert und ausgewertet
§ Es existiert ein angemessenes Informationssicherheits-Risikomanagement	



Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden.

Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

Das Ergebnis der Vorabprüfung und die zugrunde gelegten Einschätzungen der im Zuge der Verarbeitungstätigkeit möglicherweise auftretenden Schäden sowie die resultierende Schwere und Eintrittswahrscheinlichkeit der Risiken sind zu dokumentieren.





Videoüberwachung

Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.



Videoüberwachung

Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt [erkennbar zu machen](#) (Hinweispflicht nach BDSG-neu).



Videoüberwachung

Nach § 4 Absatz 5 BDSG-neu sind die **Daten der Videoüberwachung unverzüglich zu löschen**, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Das ist der Fall, wenn eine Gefahr nicht weiter abgewendet werden muss oder eine Beweissicherung nicht notwendig ist.

Das bedeutet, dass Videoaufzeichnungen **regelmäßig nach 48 bis 72 Stunden, spätestens aber nach sieben Tagen zu löschen** sind. Da sich die gesetzliche Speicherdauer am Aufzeichnungszweck orientiert, kann der Zeitpunkt der Löschpflicht aber je nach Einzelfall variieren.



Compliance-Nachweis

Dokumentieren Sie die Rechtskonformität der Datenverarbeitungen sowie die Erfüllung der Informations- und anderer Pflichten, um im Fall der Fälle der Rechenschaftspflicht nach Art. 5 Abs. 2 DS-GVO gerecht werden zu können.



Verfahren bei Datenschutzverletzungen

Differenziertes Verfahren bei Datenschutzverletzungen

1. **Meldepflicht ggü. Aufsicht** ohne unangemessene Verzögerung, jedoch höchstens 72 Stunden nach Bekanntwerden.
2. **Meldepflicht ggü. dem Betroffenen** bei hohem Risiko für seine Rechte, ohne unangemessene Verzögerung in einfacher Sprache.

Die Meldeadresse ist

<https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/>



Bußgeldvorschriften, Art. 83 Abs. 4-6



<ul style="list-style-type: none">○ Bis zu 10.000.000 EUR oder im Fall eines Unternehmens bis zu 2 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist	<p>Pflichten gemäß den Artikeln 8, 11, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 42 und 43;</p> <p>42, 43</p> <p>41 Abs. 4</p>	<p>Verantwortliche; Auftragsverarbeiter</p>
<ul style="list-style-type: none">○ Bis zu 20.000.000 EUR oder im Fall eines Unternehmens bis zu 4 % seines weltweiten Jahresumsatzes, je nach dem, was höher ist	<p>Verstöße gegen die folgenden Bestimmungen: Artikel 5, 6, 7 und 9, 12-22, 44-49, 58 Abs. 1, 2,</p>	<p>Zertifizierungsstelle Überwachungsstelle</p> <p>Verantwortliche, Auftragsverarbeiter</p>

Berücksichtigung erschwerender und erleichternder
(z. B. Zertifizierung) Tatsachen aber:
In jedem Fall

“wirksam, verhältnismäßig und abschreckend”



DSGVO – 10 Tipps für Vereine (Checkliste)

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Rheinland-Pfalz hat einen Ratgeber für Vereine herausgebracht. Mit den zehn wichtigsten Hinweisen zur Datenschutzgrundverordnung (DSGVO) möchte die Datenschutzaufsicht Vereinsvorständen wichtige Tipps im Umgang mit der DSGVO geben.

Die Hinweise im Überblick

1. Erstellen Sie ein Verzeichnis der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO.



DSGVO – 10 Tipps für Vereine (Checkliste)

2. Erheben, speichern und verarbeiten Sie personenbezogene Daten nur, wenn Sie eine Rechtsgrundlage hierfür haben. Bei Vereinen dürfte der Vertrag über die Mitgliedschaft in Verbindung mit der Vereinssatzung in den meisten Fällen als Rechtsgrundlage dienen. Für einen Newsletterversand u.ä. braucht es eine Einwilligung.
3. Mitglieder müssen über die Datenverarbeitungsvorgänge informiert werden. Insbesondere ist darüber zu informieren, welche personenbezogenen Daten zu welchem Zweck und auf welcher Rechtsgrundlage über welchen Zeitraum verarbeitet werden.



DSGVO – 10 Tipps für Vereine (Checkliste)

4. Erheben, speichern und verarbeiten Sie nur die personenbezogenen Daten, die für den jeweiligen Zweck erforderlich sind und speichern Sie diese auch nur so lange, wie sie für die Erfüllung des Zwecks erforderlich sind (Achtung: Gesetzliche Aufbewahrungsfristen beachten).
5. Stellen Sie organisatorisch und technisch sicher, dass nur diejenigen Personen personenbezogene Daten einsehen und verarbeiten können, die dies auch rechtlich dürfen bzw. müssen.
6. Betroffene haben verschiedene Betroffenenrechte wie z. B. das Auskunftsrecht oder das Recht auf Datenlöschung. Stellen Sie sicher, dass Sie diesen Rechten zeitnah nachkommen können.



DSGVO – 10 Tipps für Vereine (Checkliste)

7. Prüfen Sie, ob Sie einen Vertrag zur Auftragsverarbeitung benötigen.
8. Prüfen Sie, ob Sie eine Datenschutzfolgenabschätzung durchführen müssen. Diese ist immer dann durchzuführen, wenn ein hohes Risiko bei der Datenverarbeitung im Verein besteht.
9. Sind zehn oder mehr Personen mit der automatischen Verarbeitung personenbezogener Daten beschäftigt, muss ein Datenschutzbeauftragter benannt werden.
10. Dokumentieren Sie wie sie Daten verarbeiten und wie Sie Ihren Pflichten nachkommen.



weiter denken...



Informationsquellen u.a.

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

<https://www.datenschutz.rlp.de/de/themenfelder-themen/datenschutz-grundverordnung/kurzpapiere-zur-auslegung-der-ds-gvo/>



Wir bleiben in Verbindung

Ihre Kontaktdaten:

Marcel Müller
Audit WPG
Heilbronner Straße 41
70191 Stuttgart



Fon 0173 / 928 1744
Fax 0711 22213 - 1722

marcel.mueller@audit-wpg.com
www.audit-wpg.com