

DS- GVO

Datenschutz-Grundverordnung VO(EU)2016/679

für Vereine und Verbände

Fassung 5.0. (01.05.2018)

Neue Rechtslage ab 25.5.2018

Malte Jörg Uffeln

Mag.rer.publ. Mediator (DAA) MentalTrainer

Lehrbeauftragter

Fortbildung in Krisenpädagogik nach Prof. Dr. Bijan Amini

Rechtsanwalt (Zulassung ruht nach § 47 BRAO)

www.maltejoerguffeln.de

Mein Service für Sie:

Über 350

**Power-Point-Vorträge, Reden,
Muster auf**

www.maltejoerguffeln.de

I.

Sensibilisierung

Warming Up... I

Ein Fall aus der Praxis (Quelle: 45. Tätigkeitsbericht des Hessischen Datenschutzbeauftragten 2016 Ziff. 4.1.1., S. 89)

- HJV (Hessischer Judo-Verband e.V.)

„Videoaufzeichnungssystem“ (Wettkampf zwischen Athleten, keine Löschung der Aufzeichnungen auf dem jeweiligen Laptop nach Ende Wettkampf!“

- Später: **Verwendung der Aufnahmen zu Schulungszwecken** ohne Mitteilung an „Betroffene“

- Kampfrichter nicht vollständig auf Datengeheimnis verpflichtet (§ 5 BDSG)

Warming Up... II

Der Turn- und Sportverein Musterstadt veröffentlicht in seinem Vereinsheim auf dem **Schwarzen Brett** im Februar eines jeden Jahres vor der Mitgliederversammlung alle **Mitglieder, die ihren Beitrag noch nicht gezahlt haben.**

Warming Up... III

87 Prozent der deutschen Firmen hinken bei der Umsetzung der DS- GVO hinterher

Quelle:

<http://meedia.de/newsline-detail/87-prozent-der-deutschen-firmen-hinken-bei-der-umsetzung-der-dsgvo-hinterher/>

- ***„große Verunsicherung“***
- ***„große Menge von Halbwissen“***
- ***„Vollzugsdefizit“***

Eine Meinung zur DS- GVO

Prof.Dr. Thomas Hoeren

**„...eines der schlechtesten
Gesetze des
21.Jahrhunderts...”**

„...hirnlos...”

Quelle:

<https://www.bdsg-externer-datenschutzbeauftragter.de/datenschutz/informationsrechtler-kuert-die-neue-europaeische-datenschutzverordnung-zu-einem-der-schlechtesten-gesetze-des-21-jahrhunderts/>

Warming Up.... IV

**Homepage Prof. Dr. Thomas Hoeren mit
Podcasts zur DS- GVO**

[https://www.uni-
muenster.de/Jura.itm/hoeren/organisation/prof-dr-thomas-
hoeren](https://www.uni-muenster.de/Jura.itm/hoeren/organisation/prof-dr-thomas-hoeren)

Interview Malte Jörg Uffeln zur DS- GVO

<https://www.youtube.com/watch?v=st3BRKNYZxM>

II.

Die Rechtsprechung des Bundesverfassungsgerichts und das Verhältnismäßigkeitsprinzip

**Volkszählungsurteil des
Bundesverfassungsgerichts
(1983)**

***„ Grundrecht auf
informationelle
Selbstbestimmung “***

(Arg. aus Art. 2 I GG)

„Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. [...] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. **Hieraus folgt:**

Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen

Daten voraus. Dieser Schutz ist daher von dem Grundrecht des Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“

„Integritätsgrundrecht“

BVerfG, 1 BvR 370/07 und 1 BvR 595/07

Das allgemeine Persönlichkeitsrecht (Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG) umfasst das
Grundrecht auf Gewährleistung der
Vertraulichkeit und Integrität
informationstechnischer Systeme.

Datenschutz

=

Schutz der Menschen

Datensicherheit

=

Schutz der Daten

Die **LOGIK** des
Datenschutzes:

VERBOT mit
Erlaubnisvorbehalt

Aus der Praxis für die Praxis:

Verwendung von Daten aus öffentlichen Quellen ?

- **Adress- und Telefonbücher**
 - **Öffentliche Register**
 - **Veröffentlichungen**
- **Internet – nicht passwortgeschützt**

Grundsatz der Verhältnismäßigkeit

**verlangt stets eine Güterabwägung
der Rechte des Betroffenen zu den
Zwecken des Vereins**

Rechte des Betroffenen

- ***Recht auf informationelle Selbstbestimmung***
 - ***Schutzgrad personenbezogener Daten***
 - ***Ergänzende Grundrechte/Rechtsgüter***

(bspw. Unverletzlichkeit der Wohnung, Post- und Fernmeldegeheimnis, Sozialdatenschutz

Zwecke des Vereins

- *Auslegung §§ 1,2 der Satzung*
- *Zweckfestlegung und – bindung; Haupt- und Nebenzwecke*
- *technische und organisatorische Maßnahmen nach dem Stand der Technik*
- *Sanktionen (Androhung, Vollstreckung)*

Aus einem Seminar:

***„...Eingehende Daten sind gute Daten
Herausgehende Daten sind schlechte
Daten...”***

III.

**Kurzresümee und
Entwicklungen**

DS- GVO für Vereine und Verbände auf den Punkt gebracht !

1. Zuständigkeit für Datenschutz im Vorstand klären

2. Einwilligungserklärung prüfen/neu fassen

3. Datenschutzklausel in die Satzung/neu fassen

4. ggf. Datenschutzbeauftragter benennen und der Aufsichtsbehörde melden

**5. Anbieterkennzeichnung „Impressum“ prüfen/neu fassen
(Homepage und social media)**

6. Verarbeitungsverzeichnis führen;

DS- GVO-Ordner anlegen !!!! Abläufe dokumentieren!!!

Allgemeine Entwicklungen im Datenschutz 2018 ff.

- EU „Ausweitung Verbraucherrechte“
- BUND/HESSEN „Datenschutz- und Informationsfreiheitsgesetz“ (<https://netzpolitik.org/2017/schwarz-gruen-in-hessen-will-schlechtestes-informationsfreiheitsgesetz-deutschlands>)
- Städte/Gemeinden „IT- Audit (Prüfungen)“ ,
§ 131 I Nr. 4 HGO
- Neue Abmahngefahren; Zunahme von Abmahnungen
 - Verstärkung der Kontrollrechte auf EU-Ebene
 - „Mehr“ Bürokratie (Verarbeitungsverzeichnis!)
- Rechtsunsicherheiten bei einheitlicher Auslegungen der DS- GVO

Erwartungen der Datenschutzbehörden

Prüfpunkte: Wo/wie wird hingesehen ?

- ✓ **Bestandsaufnahme der Datenverarbeitungsvorgänge (IST- Analyse)**
 - ✓ **Prüfung der Legitimationen („Einwilligungen“)**
- ✓ **Erfüllung der Informationspflichten (bspw. Datenschutzklausel in der Satzung)**
 - ✓ **Führen eines Verfahrensverzeichnis**

Künftige Prüfungen (ab 25.5.2018) ?

**„Vom situativen Eingreifen zur systematischen
Kontrolle !!!“**

IV.

Ziele der DS- GVO

Art. 288 AEUV

„Die Verordnung hat allgemeine
Geltung. Sie ist in allen ihren Teilen
verbindlich und gilt unmittelbar in jedem
Mitgliedstaat“

Art. 1 DS- GVO

- **Schutz** von Menschen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr der Daten
- **Schutz** der Grundrechte und Grundfreiheiten von Menschen

Nicht geschützt: Verstorbene (Problem bei Chroniken! Aber: postmortales Persönlichkeitsrecht. Beachte § 22 Satz 3,4 KUG)

Künftig sind zu beachten:

➤ DS- GVO

➤ Erwägungsgründe zur DS-GVO

➤ BDSG (alt/neu)

Ausführungsgesetze zur DS-GVO

Ggf. Informationsfreiheitsgesetze

V.

EU- Datenschutz und nationale Rechtsordnungen

Öffentlicher Bereich

Nationale Sonderbestimmungen gelten fort !

Nicht- öffentlicher Bereich

(1)DS- GVO ersetzt BDSG, LDSG's

**(2) Umfangreiche Rechtsbereinigung in
Sondergesetzen wie z.B.: Melderecht, Sozialrecht,
TMG, TKG, BetrVG, UWG**

VI.

DS- GVO

Basiswissen

1.

**Rechtmäßigkeit der
Datenverarbeitung
(Art. 6 DS- GVO)**

Verbotsprinzip

=

„Verbot mit Erlaubnisvorbehalt“

Zulässigkeit der Datenverarbeitung

Erlaubnistatbestände des Art. 6 I DS- GVO

(1) Einwilligung

(2) Vertrag und vorvertragliche Maßnahmen

(3) Rechtliche Verpflichtungen

(4) Lebenswichtige Interessen

(5) Öffentliches Interesse, Ausübung öffentlicher Gewalt

**(6) Berechtigte Interessen eines Verantwortlichen oder
Dritten**

Welche Daten „verarbeiten“ wir ?

➤ Bestandsdaten

(Beispiel: Mitgliederstammdaten)

➤ Nutzungsdaten

(Beispiel: Kauf im Vereinsshop)

➤ Abrechnungsdaten

(Beispiel: Zeitauswertungen, Personalabrechnungen)

1.1.

**Einwilligung
(Art. 7 DS-GVO)**

Einwilligung = vorherige Zustimmung (§ 182 BGB)

- **stets vor der Verarbeitung!**
- **unmissverständlich, auch durch
Mausklick!**

Wirksamkeitsvoraussetzungen:

***Freiwillige, spezifisch informierte
eindeutige Handlung!***

(1) Freiwilligkeit und Kopplungsverbot

(nicht erforderliche Daten dürfen nicht erhoben werden, keine allgemeine Datensammlung)

(2) Informiertheit (konkreter Fall, Kenntnis der Sachlage)

(3) Schriftlich oder elektronisch oder mündlich;

(konkludent möglich, aber vor dem Hintergrund des Nachweises nicht mehr zu empfehlen!)

MERKSÄTZE

1. Nachweis über Einwilligung muss der verantwortliche Datenverarbeiter (Verein, Verband) führen

2. (Er-)neu(t)e Einwilligung kann „später“ bei Zweckänderungen erforderlich sein

(Beispiel: Dachverband verlangt weitere Mitgliederdaten)

3. Der Betroffene muss die Einwilligung jederzeit widerrufen können!

Formen der Einwilligung

- ✓ schriftlich
- ✓ elektronisch
- ✓ mündlich
- ✓ konkludent

Problem: Nachweispflicht !!

„Intellektualität“/Sprache ?

- ✓ **klar und einfach**
- ✓ **keine Verschleierung von Tatsachen**
 - ✓ **Keine Schachtelsätze**
- ✓ **Vermeidung von Fachvokabular**

Der Fall aus der Praxis:

Familienmitgliedschaft im Verein

Wer „willigt“ ein ?

Wer „erklärt“ Vereinsbeitritt ?

Lösungsoptionen

Variante I: Vater und Mutter für sich und Kinder (§§ 1626,1629 BGB)

Variante II: Ein Ehepartner „für“ Familie insgesamt

Variante III: Alle Familienmitglieder „einzeln“ (beachte § 104 BGB)

Problemlagen in der Praxis:

Getrenntleben (§ 1565 BGB)

Fiktive Einwilligung geht nicht!

Widerspruchslösung qua Satzung

Einwilligung wird unterstellt, wenn nicht widersprochen wird, geht nicht!!!

**MUSTER einer
Einwilligungserklärung**

<https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/>

1.2.

Besondere Datenkategorien

„Sensible Daten“

(Art. 9 DS- GVO)

Die Regel des Art. 9 I GS- DVO

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.

Ausnahmetatbestand in Art. 9 II lit. d) DS- GVO

Datenverarbeitung im Rahmen des satzungsgemäßen Zwecks

1. “Notwendige“ Mitgliederdaten

2. Interne (Vereins-)Zwecke

TIPP:

Datenschutzklausel in Satzung verankern !!!

2.

Prinzipien der Datenverarbeitung (Art. 5 DS- GVO)

2.1.

**Rechtmäßigkeit, Treu und
Glauben, Transparenz**

Treu und Glauben

(§ 242 BGB)

„Der Schuldner ist verpflichtet, die Leistung so zu bewirken, wie Treu und Glauben mit Rücksicht auf die Verkehrssitte es erfordern.“

Treuwidrig

(Verwendung verborgener Techniken)

- **Heimliche Videoüberwachung**
 - **Spyware**

Der Fall aus der Praxis:

Videoüberwachung des Vereinsheims

- ✓ **Transparenz schaffen: „Hinweisschild“**
 - ✓ **Videoüberwachung ist „ultima ratio“**
- ✓ **Erforderlichkeit ist bzgl. jeder einzelnen Kamera zu prüfen**

2.2.

Zweckbindung

Der ***Zweck des Vereins***
bestimmt über die Zulässigkeit,
Art und Weise und Umfang der
Datenverarbeitung !!!

Stets Satzung prüfen !!!

- **eindeutig, nur rechtlich zulässige Zwecke**
- **Grenzen, Art und Umfang ermitteln über**
Satzungszweck und
dessen Auslegung
- **Verbot der Weiterverarbeitung**

Die personenbezogenen
Daten müssen für den
verfolgten Zweck **„erheblich“**
und **„angemessen“** sein

Erheblichkeit

**Daten müssen für den Zweck
relevant sein**

- ✓ geeignet
- ✓ erforderlich)

Angemessenheit

Nicht erhebliche oder dem Zweck nicht dienende Daten dürfen nicht erhoben werden.

Beachte:

**Grundsatz der Datenminimierung
Satzungen von Dachverbänden**

Welche Daten sind dies ?

- **Name und Anschrift**
 - **Bankverbindung**
 - **Eintrittsdatum**
- **Geburtsjahr (- datum ?)**
- **Kommunikationsverbindungen(?)**
- **Funktionen/Kenntnisse/Fähigkeiten(?)**
 - **Kfz- Kennzeichen(?)**
 - **Kreditkartennummer**

Meine Kernpflichten als Ehrenamtlicher im Umgang mit Daten ?

- ✓ **Vertraulichkeit** der Daten sichern
- ✓ **Integrität** der Daten sichern
(keine Verfälschung/Manipulation)
- ✓ **Verfügbarkeit** sichern
- ✓ **Auskunfts- und Benachrichtigungspflichten**

Text einer Verpflichtungserklärung

***„ Ich verpflichte mich, die
erhaltenen Mitgliederlisten sowie
sonstige personenbezogenen Daten von
Mitgliedern und dritten Personen nur für
satzungsgemäße Zwecke zu verwenden
und nicht unbefugt zu verarbeiten,
bekannt zu geben, zugänglich zu machen
oder sonst zu nutzen.“***

2.3.

Datenminimierung

Datensparsamkeit

Grundsatz der Datenminimierung

(alt: § 3 a BDSG; Datenvermeidung, Datensparsamkeit)

- **Verringerung der Anzahl der verarbeiteten Daten**
- **Verringerung der Anzahl der Nutzungen**
(Rechtswidrigkeit von Mehrfachauswertungen)
- **Verringerung der Anzahl der Betroffenen**
- **Bereitstellung der Daten zum Lesen auf dem Bildschirm ohne Ausdruck**

2.4.

Richtigkeit

- ✓ **Sachlich richtige, aktuelle
Daten**
- ✓ **Vorsorgen für unverzügliche
Löschung**
- ✓ **Unaufgeforderte Berichtigung
unzutreffender Daten**

2.5.

Speicherbegrenzung

**Datenverarbeitung solange, wie
es erforderlich ist !**

Der Fall aus der Praxis :

**Umgang mit Daten von
ausgetretenen, ausgeschiedenen
Mitgliedern ?**

2.6.

Integrität und Vertraulichkeit

Schutzvorkehrungen (IT- Sicherheit) treffen vor

- **unrechtmäßiger Verarbeitung**
 - **zufälligem Verlust**
- **zufälliger Zerstörung und
(Be-)Schädigung**

2.7.

**Rechenschaftspflicht
Informationspflichten**

***Umkehr der Beweislast:
„Der Verantwortliche muss...“***

Verantwortlicher für Datenverarbeitung

- *achtet auf* Einhaltung der Prinzipien
- *weist* Einhaltung der Prinzipien *nach*

Grundsatz des risikobasierten Ansatzes

„geeignete technische und organisatorische
Maßnahmen“ sind zu treffen!

Datenschutzrechtliche Unterrichtung (Art. 13 I, II DS- GVO)

Informationspflichten des Datenverarbeiters

Beachte:

Nichterfüllung der Pflicht ist bußgeldbewehrt!

LINK:

Informationsblätter

<https://www.baden-wuerttemberg.datenschutz.de/orientierungshilfen-merkblatter/>

Hinweispflichten

- Name , Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten
 - Konkrete Zwecke der Verarbeitung
 - Rechtsgrundlage der Verarbeitung
- Berechtigte Interessen (Art. 6 DS- GVO)
- Empfänger/Kategorien von Empfänger der Daten
- Absicht über Drittlandtransfer (Mitgliederverwaltung in einer cloud)
 - Speicherdauer der personenbezogenen Daten
 - Belehrung über Betroffenenrechte
- Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Optionen für datenschutzrechtliche Regelungen im Verein

- **Einwilligungsformular bei Vereinsbeitritt**
 - **Vereinssatzung**
 - **Datenschutzordnung**
(beschlossen von der MGV)
 - **Datenschutzrichtlinie**
- **Datenverarbeitungsrichtlinie**

Aus der Praxis für die Praxis:

**Beispiel für eine
Datenverarbeitungsrichtlinie auf einer
Vereinshomepage**

SV 1988 Aschaffenburg – Damm e.V.

http://www.sv1888damm.de/Richtlinien/Datenschutz_beim_SV1888.pdf

2.8.

**27 Standardfälle aus der
Vereinspraxis**

2.8.1.

**Umgang mit Mitgliederdaten
(Mitgliederliste)**

Herausgabe ?

**Wohl nein, aber Einsicht zur
Wahrung der Mitgliedsrechte
(§ 37 I BGB)**

Sonderfälle:

**Pflege der persönlichen Verbundenheit (???),
Selbsthilfegruppen**

2.8.2.

**Schwarzes Brett/
Vereinszeitung(-blatt) /Web ?**

In der Regel : NEIN !!!

Kritische Fälle

- Hausverbot
- Vereinsstrafe
- Spiellersperre
- Vereinsausschluss

***„Betroffene dürfen n i c h t an den
Pranger gestellt werden!!!“***

Persönliche Nachrichten

- **Eintritt in Verein**
- **Austritt aus dem Verein**
 - **Spenden**
- **Geburtstage, Ehejubiläen**

können veröffentlicht werden !

Sensible Informationen

- **Eheschließung**
- **Geburt von Kindern**
- **Abschluss von Ausbildungen**
- **Private/dienstliche e-Mail-Adresse**

**dürfen nur mit Zustimmung des Betroffenen
veröffentlicht werden.**

2.8.3.

An Sponsoren ?

In der Regel : NEIN !!!

2.8.4.

Spenderliste ?

**Herausgabe und Einsicht :
NEIN !!!**

2.8.5.

Helferliste ?

**Nur mit Einwilligung der Helfer
ist Übersendung an Mitglieder
möglich !!!**

2.8.6.

E-Mail an Mitglieder ?

- **Schriftliche Einwilligung!**
- **BCC – e-mail statt CC – e-mail**

Varianten

➤ „An-Feld“

➤ „CC“ **Carbon Copy** (Alle sehen
Nachricht)

➤ „BCC“ **Blind Carbon Copy**
(Blindkopie)

TIPP:

BCC – e-mail versenden

2.8.7.

Sensible Daten

„Gesundheitsdaten“

**„Treuepflicht“ und „
Verschwiegenheitspflicht“**

=

Schutz der Privatsphäre

(§ 203 StGB Geheimnisträger)

2.8.8.

**Sonderfall Jugendarbeit
(Erweitertes) Führungszeugnis**

§ 72 a SGB VII

Tätigkeitsausschluss einschlägig vorbestrafter Personen

(1) Die Träger der öffentlichen Jugendhilfe dürfen für die Wahrnehmung der Aufgaben in der Kinder- und Jugendhilfe keine Person beschäftigen oder vermitteln, die rechtskräftig wegen einer Straftat nach den §§ 171, 174 bis 174c, 176 bis 180a, 181a, 182 bis 184f, 225, 232 bis 233a, 234, 235 oder 236 des Strafgesetzbuchs verurteilt worden ist. Zu diesem Zweck sollen sie sich bei der Einstellung oder Vermittlung und in regelmäßigen Abständen von den betroffenen Personen ein Führungszeugnis nach § 30 Absatz 5 und § 30a Absatz 1 des Bundeszentralregistergesetzes vorlegen lassen.

Führungszeugnis

FAQ unter

www.bundesjustizamt.de/nn_2051864/DE/.../FAQ__node.html?

Inhalt u.a.

***Jugendstrafen bis zu einer bestimmten Höhe,**

*** erstmalige Geldstrafen, die nicht höher als 90 Tagessätze liegen**

(§ 32 Abs. 2 Nr. 5 BZRG),

***erstmalige Verurteilungen von drogenabhängigen Straftätern, die zwei Jahre Freiheitsstrafe nicht überschreiten und die Vollstreckung der Strafe nach § 35 BtmG zugunsten einer Therapie zurückgestellt, und nach erfolgreicher Therapie nach § 36 BtmG zur Bewährung ausgesetzt wurde, sowie wenn die weiteren diesbezüglichen Bedingungen des § 32 Abs. 2 Nr. 6 BZRG erfüllt sind.**

Erweitertes Führungszeugnis

Mit dem am 1. Mai 2010 in Kraft getretenen 5. Gesetz zur Änderung des Bundeszentralregistergesetzes vom 16. Juli 2009 ist in §§ 30a, 31 Bundeszentralregistergesetz (BZRG) ein „erweitertes Führungszeugnis“ eingeführt worden, welches über Personen erteilt werden kann, die beruflich, ehrenamtlich oder in sonstiger Weise kinder- oder jugendnah tätig sind oder tätig werden sollen.

LINK: <http://www.kinderschutzbund-nrw.de/pdf/ArbeitshilfeFuehrungszeugnis.pdf>

2.8.9.

**Teilnehmerlisten bei
Lehrgängen, WorkShops**

Teilnehmerliste bei Lehrgängen

=

„ Liste der Teilnehmer“

LÖSUNG:

**Umfassende Einwilligungserklärung der
Teilnehmer für die Liste für die
Teilnehmer, den Veranstalter und die
Lehrgangsleitung mit „
Weitergabevermerk“!!!**

2.8.10.

**Datenweitergabe an
Werbepartner**

Finger weg von der Datenweitergabe an **WERBEPARTNER** , auch für Zwecke der Telefon- oder e-mail-Werbung!!!

Möglich ist das aber, wenn

- ✓ **eine spezielle Einwilligung vorliegt**
- ✓ **Einwilligungen sauber dokumentiert sind**
- ✓ **jeder Betroffene das Recht auf Auskunft hat**
jeder Betroffene Löschung verlangen kann

2.8.11.

**Werbung durch Verein für
Verein, Spendenaufrufe**

**Ja, zur Erreichung der Zwecke
und Ziele !!!**

2.8.12. Cloud- Mitgliederverwaltungsdienst

✓ **Machbar**

✓ **Empfehlung:**

Klare Satzungsregelung

2.8.13.

**Mitgliederdaten an
Versicherungen/
Gruppenversicherer**

- ✓ **Ja, zur Erfüllung des Vereins/-
Verbandszwecks bei Einwilligung Mitglied**
- ✓ **Nein, wenn rein freiwillig (Werbung etc.)**

2.8.14.

**Veröffentlichung von Daten im
WWW.**

Social Media

- ✓ **Ja, mit Einwilligung des
Mitglieds**

2.8.15.

**Veröffentlichung von
Wettkampfergebnisse**

✓ **Ja, auch ohne Einwilligung
des Mitglieds**

(Spielergebnisse, persönliche Leistungen, Mannschaftsaufstellungen,
Ranglisten, Torschützen)

2.8.16.

Veröffentlichung von Daten im Intranet (passwortgeschützt)

- ✓ **Ja auf der Basis
„Einwilligung“ oder
Satzungsklausel**

2.8.17.

Veröffentlichung von Daten in Presse/Massenmedien

**✓ Ja, nur unbedingt
notwendige persönliche
Daten**

2.8.18.

Veröffentlichung von Daten zu Zwecken der Wahlwerbung

- **NEIN!**

2.8.19.

Übermittlung von Daten an Behörden

**✓ Ja, bei Wahrnehmung
berechtigter Interessen**

**(bspw. Abrechnung von Zuschüssen, Beantragung von Zuwendungen,
Bestandsmeldungen, Statistiken)**

2.8.20.

Übermittlung von Daten an Arbeitgeber von Mitgliedern

- ✓ Ja im Falle des § 67 a SGB X
(Regress)**

2.8.21.

Daten in einem Vereinsarchiv ?

- ✓ **Ja, wenn Nutzerkreis „ klein“
gehalten wird!**

2.8.22.

Whatsapp- Gruppen

NEIN „im“ Verein

- **Machbar für „Gruppenkommunikation“
(Sportgruppe, Vorstand etc.)**
- **In der Regel nicht nutzbar für Einladungen etc.**
 - **Trennung klar stellen: Verein vs. Private
Kommunikation**

Alternative zu WhatsApp:

Threema

(<https://threema.ch/de>)

***Threema* ist so konzipiert, dass keine Datenspur entsteht. Gruppen und Kontaktlisten werden auf Ihrem Gerät verwaltet, nicht auf dem Server. Nachrichten werden sofort nach Zustellung gelöscht. So entstehen möglichst keine Metadaten. Beste Verschlüsselung**

2.8.23.

Datenabgleich mit Abteilungen

- ✓ **Ja, zulässig zur Datenbestandsfeststellung und – pflege**
- ✓ **Abteilung muss Daten dem Vorstand nach § 26 BGB zur Verfügung stellen**

2.8.24.

SEPA- Lastschrift

- ✓ **SEPA- Lastschriftinzugsermächtigung in Eintritts-,/Beitrittsformular**
- ✓ **Pre-Notifikation bei „erstmaligem Einzug“**

(<http://single-euro-payments-area.de/vorabinformation-pre-notification>)

gilt auch für Folgeeinzüge, wenn kein Widerspruch

2.8.25.

Mitgliederverwaltung auf Privat- PC

- ✓ **Ja, bei Zugangssicherung**
- ✓ **Trennung von privater und Vereins-
Datenverarbeitung**
- ✓ **Empfehlung: Beschluss Vorstand zur
Zulässigkeit, ggf.
Datenverarbeitungsrichtlinien**

2.8.26.

Mitgliederverwaltung auf Dienst- PC, der privat genutzt werden darf

- ✓ Ist **n i c h t** zu empfehlen
- ✓ Trennung von privater und Vereins-
Datenverarbeitung
- ✓ Empfehlung: Beschluss Vorstand zur
Zulässigkeit, ggf.
Datenverarbeitungsrichtlinien

2.8.27.

Recht auf Datenmitnahme

- In der „Einwilligung“ bei Vereinseintritt klären
- „Vor“ der Löschung Anschreiben an „ehemaliges Mitglied“
 - „Reproduzierbarkeit von Daten “ ?

(Fall: Ehrungen, Auszeichnungen...; Fall: Blogs und Mitglieder-Chats)

3.

Datenportabilität

(Art. 20 DS-GVO)

**Der Bürger hat ein Recht auf
Datenübertragbarkeit!**

Rechtsanspruch

(Herausgabeanspruch) auf Erhalt eigener
personenbezogener Daten und
auf Übertragung in
Verarbeitungssystem eines
anderen Verantwortlichen

(selbst oder mittelbar von Verantwortlichem zu
Verantwortlichem)

***„Grundsatz der Interoperabilität, Übertragung in ein
gängiges Format“***

4.

**Recht auf Einschränkung der
Verarbeitung**

(Art. 18 DS- GVO)

„ Sperrung “(alt: § 35 II BDSG)

Fälle:

- 1. Bestrittene Richtigkeit der Daten**
- 2. Unrechtmässige Verarbeitung**
- 3. Wegfall der Verarbeitungsnotwendigkeit**
- 4. Widerspruch gegen die Verarbeitung nach
Art. 21 Abs. 1 DS-GVO**

5.

**Recht auf Vergessen werden
(Art. 17 Abs. 2 DS- GVO)**

„Der digitale Radiergummi!“

Hintergrund:

**Entscheidung des EuGH vom
13.5.2014 C 131/12**

„Google Spain“

**Der Betroffene hat ein Recht auf
Vergessen werden im Internet**

Quelle:

<http://curia.europa.eu/juris/liste.jsf?language=de&num=C-131/12>

Art. 17 Abs. 1 DS- GVO

„Löschung“

Informationen Anderer über

- **alle Links**
- **Kopien und Replikationen**

Exkurs:

Löschfristen Arbeitsrecht

- **§ 17 Antidiskriminierungsgesetz: 6 Monate
(abgelehnte Bewerber)**
- **Unterlagen nach AZG, MuSchG: 2 Jahre**
- **§§ 28 f SGB IV (Entgeltunterlagen;
Unterlagen für Jahresabschluss, bspw.
Lohnbuchhaltung. Zehn Jahre
(§§ 257,147 AO)**

6.

Im Überblick

Die Rechte des Bürgers....

Recht auf

- **Auskunft**
- **Löschung**
- **Berichtigung**
- **Widerruf und Widerspruch**
 - **Einschränkung**
 - **Datenmitnahme**
 - **Protokollierung**
- **Beschwerde bei der Aufsichtsbehörde**
 - **Schadenersatz**

VII.

Datenschutzbeauftragter

(Art. 37 DS- GVO; § 38 BDSG)

„Unabhängig“, „weisungsfrei“

Grundsatz der Selbstkontrolle

Das System der Datenschutzkontrolle

➤ **Selbstkontrolle** (Betroffene)

➤ **Eigenkontrolle**

(Datenschutzbeauftragte)

➤ **Fremdkontrolle**

(Aufsichtsbehörden)

Variante I

„verpflichtend“ für Unternehmen

(Art. 37 Abs. 1 DS- GVO)

Variante II

„freiwillig“ in anderen Fällen

(... Verbänden, Vereinigungen...)

(Art. 37 Abs. 4 DS GVO, § 38 BDSG)

Kernbereiche der Tätigkeit

- **Sicherstellung des Datenschutzes**
- **Hinwirkung auf Einhaltung des Datenschutzes**
- **Überwachung der Organisation**

**Wann brauchen wir im Verein
einen Datenschutzbeauftragten ?**

Mehr als 9 Menschen(mind.10)

**beschäftigen sich ständig mit
der automatisierten (PC)- auch nicht
automatisierten(Papierakte) Verarbeitung
personenbezogener Daten**

(Argument aus § 4 f BDSG; § 38 BDSG, Art. 37 DS-GVO)

Plath(Hrsg.),Kommentar zum BDSG,
2013, S. 203)

„ Der ***Begriff ständig***

bedeutet nicht notwendig dauernd, verlangt
aber, dass die Tätigkeit auf Dauer angelegt ist
und die betreffende Person immer dann tätig
wird, wenn es notwendig ist, selbst wenn die
Tätigkeit nur in zeitlichen Abständen (z.B.
monatlich) anfällt.

Bestellungsoptionen

Variante 1

Interner Datenschutzbeauftragter

Variante 2

Externer Datenschutzbeauftragter

**in Vollzeit und Teilzeit, je nach Größe des
Unternehmens!**

Qualifikationen ?

Keine Regelung in der DS- GVO

Empfehlungen(!)

- **Fachwissen im Datenschutzrecht und der Datenschutzpraxis**
- **Technisches und organisatorisches Fachwissen**
 - **Kommunikationsfähigkeit**

Information und Transparenz

- **Bestellung ggf. durch Beschluss des Vorstandes**
 - **Namentliche Meldung an die Aufsichtsbehörde**
- **Mitteilung der Anschrift auf der Homepage des Vereins**

Praxis des Datenschutzbeauftragten

- ✓ **Beraten und unterrichten**
- ✓ **Überwachen und sanktionieren**
- ✓ **Datenschutzfolgen abschätzen und beraten**
- ✓ **Ansprechpartner zur Datenschutzaufsicht**
- ✓ **Zusammenarbeiten mit Vorstand und Datenschutzaufsicht**
- ✓ **Risikoabwägung**
- ✓ **Beraten lassen durch Datenschutzaufsicht**

Der Fall aus der Praxis:

**Kann ein „Vereinsring“ für alle Vereine
einen Datenschutzbeauftragten
bestellen ?**

- **Machbar**
- **Klare Beschlüsse aller Vereine**

VIII.

**Verarbeitungen,
Prozesssicherheit**

1.

**Datenschutz durch
Technikgestaltung (Privacy by Design)
und datenschutzfreundliche
Voreinstellung (Privacy by Default)**

Art. 25 DS- GVO

2.

**Datenschutz-Folgenabschätzung
(Art. 35 DS- GVO)**

Mögliche Vorgehensweise:

- 1. Erforderlichkeit ? (Prozess und Ergebnis festhalten)**
- 2. Mögliche Vorgaben der Aufsichtsbehörden**
- 3. Prozessbeschreibung**
- 4. „Vorherige Konsultation“ (der Aufsichtsbehörde) klären**

3.

**Sicherheit der Verarbeitung
(Art. 32 DS- GVO)**

Angemessene Sicherheitsvorkehrungen

IT- Sicherheitsziele

- **Vertraulichkeit**
 - **Integrität**
 - **Verfügbarkeit**
- **Sicherheitsmanagement**

Exkurs:

**Datensicherung digitaler und
analoger Daten**

3.1.

Digitale Daten

- ✓ **Passwortzugang für PC, Laptop**
 - ✓ **Passwortschutz für mobile Datenträger (USB Stick, Festplatten)**
- ✓ **Sicherung auf einem externen Server**
- ✓ **Verschlüsselte Datenübermittlung**

3.2.

Analoge Daten

- ✓ **Lagerung in abgeschlossenen Räumen**
- ✓ **Lagerung in abschließbaren Schränken**
- ✓ **Digitalisieren(Scannen) und Integration in Software**
- ✓ **Schutz vor fremdem Zugriff
(nicht rumliegen lassen)**

4.

**Verarbeitungsverzeichnis
(Art. 30 DS- GVO)**

Verantwortlicher:

**Aufzeichnung aller
Verarbeitungstätigkeiten**

Auftragnehmer:

**Aufzeichnung der durchgeführten
Tätigkeiten**

**Weitere Dokumentationspflichten aus anderen
Rechtvorschriften!!!**

5.

Dokumentations- und Nachweispflichten

5.1. Dokumentationspflichten

- **Dokumentierte Weisungen**
- **Verzeichnete Verarbeitungstätigkeiten**
 - **Verletzungen des Schutzes personenbezogener Daten**
 - **Abwägungen**

5.2. Nachweispflichten

- **Einhaltung der Verarbeitungsprozesse**
 - **Einwilligungen**
 - **Unbegründetheit von Anträgen**
 - **Erfassung der Verarbeitung**
 - **Einhaltung der DS- GVO**
 - **Kontrolle**

IX.

Bußgelder, Sanktionen

- ✓ **Wirksam**
- ✓ **verhältnismäßig**
- ✓ **abschreckend**

**Bußgeld bis zu
10.000.000,00 €
20.000.000,00 €**

**Unternehmen:
bis zu 2% des weltweiten
Umsatzes**

Maßstäbe, Kriterien I

✓ **Art**

✓ **Schwere**

✓ **Dauer**

✓ **Anzahl der Betroffenen**

Maßstäbe, Kriterien II

- ✓ Vorsatz oder Fahrlässigkeit des Verstoßes (*verschärfend*)
- ✓ Maßnahmen zur Minderung des Schadens (*mildernd*)

1.

**Beschwerde bei der
Aufsichtsbehörde**

2.

Verbandsklage

**Vertretung eines „Betroffenen“
durch einen Verband
(s.a. nationales Recht;
UKlaG)**

3.

Schadenersatz, Strafe

Bußgeld

X.

Sonderfälle

1.

Website- Compliance

Jetzt handeln:

**Datenschutzerklärung anpassen an
DS- GVO**

**ePrivacy-Verordnung der EU betreffend
Informationspflichten und Einwilligung
bei der Nutzung von Cookies auf
Webseiten umsetzen.**

Weiter beachten:

§§ 11 ff. TMG, § 13 TMG

2.

Videoüberwachung

Nicht explizit geregelt in der DS- GVO !

Prüfung nach Art. 6 Abs. 1 Satz 1 lit f. DS- GVO

Grundsätzliche Anforderungen

- **Beschränkung auf das unbedingt notwendige Maß**
- **Intensität der Überwachung darf nicht außer Verhältnis zum verfolgten – präventiven- Zweck stehen !**

Ergo:

Verhältnismäßigkeitsprinzip

3.

Data Breach Notification

(Datenpannen... Was ist zu tun?)

Datenpannen

1.Datenschutzverletzung muss innerhalb von 72 Stunden der Aufsichtsbehörde gemeldet werden.

2.Meldung an die Betroffenen

3.Dokumentation

**Notwendigkeit einer
Cyberversicherung ?**

Cyber-Versicherung I

Vielfältige Begrifflichkeit:

**Data Protect, Datenschutz-Versicherung, Data-Risk,
Cyber-Deckung, Hacker- Versicherung, ergänzend:
Elektronikversicherung, Datenträgerversicherung**

Ziel:

Schutz vor Hacker- Angriffen und Cyberkriminalität

Cyber-Versicherung II

Versicherungsumfang

- **Drittschäden (Datenrechtsverletzung durch VN)**
- **Eigenschäden (bspw. Hacker-Angriff, DoS-Attacke-Dienstverweigerung-)**

Cyber-Versicherung III

Kostenersatz:

- **Wiederherstellung, Reparatur der IT-Systeme**
- **Kosten für Computer-Forensik-Analysten**
 - **Fachanwälte für IT- Recht**
 - **Krisenmanagement und PR**
 - **Kreditschutz/-überwachung**
- **Interner Strafrechtsschutz (Strafverteidigung)**
- **Mehrkosten zur Fortführung des Betriebes**

Cyber-Versicherung IV

Mögliche Ergänzungen:

- Betriebsunterbrechungsversicherung
- Ertragsausfallversicherung (Umsatzausfälle!)

4.

Datenschutzmanagementsystem

Verpflichtend für Unternehmen!

Vereine und Verbände: Empfehlung!

Weiterführender Link:

Leitfaden für die betriebliche Praxis

<https://www.datenschutzbeauftragter-info.de/datenschutzmanagement-nach-der-dsgvo-leitfaden-fuer-die-praxis/>

Der Datenschutzmanager

(DSM)

nach VdS 10010

**(VdS Richtlinien zur Umsetzung der
DSGVO)**

- **implementiert ein Datenschutzmanagementsystem**
 - **erarbeitet Verbesserungsvorschläge**
 - **Unterstützt Vorstand nach § 26 BGB**
 - **prüft und passt DS- Richtlinien jährlich an**
- **untersucht datenschutzrelevante Ereignisse**
 - **ist Ansprechpartner bei Projekten**
- **berichtet jährlich an den Datenschutzbeauftragten**
 - **ist Ansprechpartner, wenn kein Datenschutzbeauftragter bestellt ist**

5.

**Verzeichnis der
Verarbeitungstätigkeiten
(Art. 30 DS- GVO)**

Inhalt

- **Name und Kontaktdaten des Verantwortlichen**
 - **Zwecke der Verarbeitung**
- **Beschreibung der Kategorien betroffener Personen und Daten**
 - **Angaben über Drittlandtransfer**
 - **Ggf. Fristen für Löschung**
 - **Ggf. Beschreibung technischer und organisatorischer Maßnahmen**

XI.

**Datenschutz bei Werbung und
Marketing unseres Vereins**

MERKSÄTZE
zum
Datenschutz
bei Werbung und
Marketing

- * Datenübermittlung an DRITTE (Partner des Vereins) ist nur mit ausdrücklicher Einwilligung der Betroffenen zulässig**
- *Verein/Verband bleibt immer „ verantwortliche Stelle“ der Datenverarbeitung**
- * Verein/Verband bleibt in der Verantwortung**

*** Keine Weitergabe von Adressen
Minderjähriger – auch bei Einwilligung der
Eltern-**

*** „ BILDER“ (Porträts) dürfen nur bei
spezieller Einwilligung genutzt werden**

*** „ MASSEN- Photos“ dürfen in der Regel
genutzt werden (Aber: Kinder !!!)**

(Beachte: TRICHTERPRINZIP !)

CHECKLISTE

**Werbung mit der Post oder
per e-mail**

1. Einwilligung zur Datenerhebung besorgen

(von Brief/Mail zu Brief/Mail; Zweckvermerk !!!)

2. Adresssammlung über Web-Site § 13 TMG

2.1. Datenschutzerklärung

2.2. Zwangs-Opt-In und Protokoll

2.3. Datenübertragung an Server

3. „Post“

(unsubscribe-Möglichkeit muss geschaffen werden)

4. „e-mail“

4.1. Begrüssungs-Mail

4.2. unsubscribe - Möglichkeit

XII.

Was müssen wir jetzt tun ?

Brennpunkte in der Vereinspraxis
Checkliste

LINK:

**Fragebogen zur Umsetzung der
DS- GVO vom 25.5.2018**

Papiere zur DS- GVO

**[https://www.ida.bayern.de/media/
dsgvo_fragebogen.pdf](https://www.ida.bayern.de/media/dsgvo_fragebogen.pdf)**

Checkliste

Unsere Fragen an uns ?!

Weiterführender Link:

<http://ds-gvo.gesundheitsdatenschutz.org/html/checkliste.php>

I. Der aktuelle IST- Zustand

- 1. Welche Daten verarbeiten wir ?**
- 2. Wozu verarbeiten wir die Daten ?**
- 3. Wie werden die Daten verarbeitet ?**
- 4. Rechtsgrundlagen der Verarbeitung ?**

5. Liegen Einwilligungen vor ?

5.1. schriftlich von den Betroffenen ?

5.2. Satzungsklausel ?

5.3. BDSG, DS- GVO

6. Unser Umgang mit den Rechten der Betroffenen ?

6.1. Verarbeitung

6.2. Sperrung

6.3. Löschung

7. Kritische Fälle aus der Vergangenheit ?

**8. Haben wir einen
Datenschutzbeauftragten ?**

**9. Welche internen Beschlüsse,
Richtlinien etc. gibt es ?**

**10. Sicherheit unserer
Datenverarbeitung ?**

11. Datensensibilität unter Mitgliedern ?

12. Anforderungen des(r) Dachverbände?

II.

**Der ab 25.5.2018 geforderte
SOLL- Zustand nach DS- GVO**

III.

**Vergleich IST- Zustand zu
SOLL- Zustand**

IV.

Handeln, Umsetzen, Machen

1. Zeitplanung D- Day 25.5.2018

Was? Wann ? Wie ?

1. Budgetplanung

2. Notwendige Maßnahmen

3.1. Einwilligungserklärungen neu fassen

3.2. Datenschutzklausel in der Satzung ändern

3.3. Verantwortlichkeiten im Verein klarstellen

3.4. Homepage checken

3.5. Änderungen in der e-mail-Korrespondenz ?

3.6. Mitarbeiter schulen

3.7.....

4. Compliance- System ?

5. Sanktionen ?

6. Offene Punkte _____

XIII.

Prozessevaluierungen

über den

25.5.2018 hinaus

Dokumentieren und

Risikoanalyse

Dokumentieren

- 1. Datenschutzdokumentation**
- 2. Transparenz**
- 3. Datenschutzfolgenabschätzung**
- 4. Beschwerdemanagementsystem**
- 5. Vertragsmanagement**
- 6. Einwilligungsmanagement**

Weitere hilfreiche LINKs:

<https://www.datenschutz-nord-gruppe.de/>

[**http://ds-gvo.gesundheitsdatenschutz.org/html/checkliste.php**](http://ds-gvo.gesundheitsdatenschutz.org/html/checkliste.php)

[**http://www.hlfp.de/dokumente/blog/HLFP-Checkliste-DSGVO-DE.pdf**](http://www.hlfp.de/dokumente/blog/HLFP-Checkliste-DSGVO-DE.pdf)

[**https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/160909-EU-DS-GVO-FAQ-03.pdf**](https://www.bitkom.org/Presse/Anhaenge-an-PIs/2016/160909-EU-DS-GVO-FAQ-03.pdf)

[**https://www.it-zoom.de/it-mittelstand/e/checkliste-geruestet-fuer-den-eu-datenschutz-13730/**](https://www.it-zoom.de/it-mittelstand/e/checkliste-geruestet-fuer-den-eu-datenschutz-13730/)

Bereich der Risikoanalyse I

- **Zugangskontrolle**
- **Datenträgerkontrolle**
- **Speicherkontrolle**
- **Benutzerkontrolle**
- **Zugriffskontrolle**
- **Übertragungskontrolle**

Bereich der Risikoanalyse II

- **Eingabekontrolle**
- **Transportkontrolle**
- **Wiederherstellbarkeit**
 - **Zuverlässigkeit**
 - **Datenintegrität**
- **Auftragskontrolle**
- **Verfügbarkeitskontrolle**
 - **Trennbarkeit**

Hilfreiche Literatur:

**Erste Hilfe zur Datenschutzgrundverordnung,
Das Sofortmaßnahmen- Paket, ISBN 978-3-
406-71662-1 € 5,50**

**Georg F. Schröder, Datenschutzrecht für die
Praxis, Beck im dtV , ISBN 978-3-423-51202-2
€ 20,50**

Vielen lieben

**Dank für ihre Aufmerksamkeit
und aktive Mitarbeit**

Ihr

Malte Jörg Uffeln

www.maltejoerguffeln.de