

DS- GVO

Datenschutz-Grundverordnung VO(EU)2016/679

für Vereine und Verbände

Fassung 2.0. (19.02.2018)

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 330

**PowerPointVorträge, Reden,
Muster auf**

www.maltejoerguffeln.de

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/>

**Aus der
Rechtsprechung des
Bundesverfassungsgerichts**

**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.

....Verschafft der Staat sich Kenntnis von Inhalten der Internetkommunikation auf dem dafür technisch vorgesehenen Weg, so liegt darin nur dann ein Eingriff in Art. 10 Abs. 1 GG, wenn die staatliche Stelle nicht zur Kenntnisnahme autorisiert ist.

Nimmt der Staat im Internet öffentlich zugängliche Kommunikationsinhalte wahr oder beteiligt er sich an öffentlich zugänglichen Kommunikationsvorgängen, greift er grundsätzlich nicht in Grundrechte ein....

Die **LOGIK** des Datenschutzes!

REGEL und Ausnahme(n)...

**VERBOT mit
Erlaubnisvorbehalt**

I.

Ziele der DS- GVO

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

- **Verbraucherschutz**
**„mehr Datensicherheit für
Bürger“**
- **EU- einheitliche Standards**
- **Harmonisierung, Vereinfachung**
- **EU- Behörde beim Datenschutz
für Unternehmen**
- **Kooperation der Behörden**

Durchgriffswirkung der DS- GVO

Art. 288 AEUV

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

II.

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**

III.

DS- GVO

Basiswissen

1.

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

Verbotsprinzip

=

„Verbot mit Erlaubnisvorbehalt“

Art. 6 I 1 DS- GVO

„Einwilligungstrias“

- **Einwilligung**
- **Vertragsdatenverarbeitung**
- **Allgemeine Interessenabwägung**

Zulässigkeit der Datenverarbeitung

Erlaubnistatbestände (enumerativ)

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**

**Datenverwendung ist
erlaubt, wenn dies
erforderlich ist !**

*** Bestandsdaten**

*** Nutzungsdaten**

*** Abrechnungsdaten**

1.1.

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

Einwilligung = vorherige Zustimmung (§ 183 BGB)

„stets vor der Verarbeitung!“

**„unmissverständlich, auch
Mausklick!“**

**(wohl Realakt; geschäftsähnliche
Handlung)**

Wirksamkeitsvoraussetzungen:

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

- (1) Freiwilligkeit und Kopplungsverbot** (nicht erforderliche Daten...)
- (2) Informiertheit (konkreter Fall, Kenntnis der Sachlage)**
- (3) Schriftlich oder elektronisch oder mündlich;**
(konkulent möglich, aber vor dem Hintergrund des Nachweises nicht mehr zu empfehlen!)

MERKE:

- **Nachweis über Einwilligung muss der verantwortliche Datenverarbeiter führen**
- **(Er-)Neu(t)e Einwilligung kann „später“ bei Zweckänderungen erforderlich sein**

(Beispiel: Dachverband verlangt weitere Mitgliederdaten)

- **Betroffener muss Einwilligung jederzeit widerrufen können!**

1.2.

Einwilligung eines Kindes in Bezug auf Dienste in der Informationsgesellschaft (Art. 8 DS- GVO)

Mindesteinwilligungsalter

16 Jahre!

(Art. 8 I DS- GVO)

Kinder unter 16 Jahren ?

Art. 8 I 1 2 DS- GVO

„Träger der elterlichen Verantwortung“

(§§ 1626, 1629 BGB; Beachte § 832 BGB)

Praxis:

Zweistufiges Überprüfungsverfahren!

Stufe 1

Minderjähriger ? „Wie alt bist Du ? “

Ergebnis: minderjähriger Nutzer, dann

Stufe 2:

Verfahren nach Art. 7 DS- GVO

Double- Opt- In Verfahren

2.1. e-mail Adresse der Eltern

2.2. Bestätigungslink... Bestätigung

1.3.

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.

Ausnahmetatbestände in Art. 9 II lit.

a) bis j) GS- DVO

u.a. ausdrückliche

Einwilligung, Arbeitsrecht/Sozialrecht

**Schutz lebenswichtiger Interessen
etc.**

WICHTIG:

**Ausnahmetatbestand
in Art. 9 II lit. d)**

**Stiftungen, Vereinigungen, sonstige
gemeinnützige Organisationen**

Datenverarbeitung im Rahmen des satzungsgemäßen Zwecks

- 1. “Notwendige“ Mitgliederdaten**
- 2. Interne Zwecke**

1.4.

**Verarbeitung ohne Zustimmung
des Betroffenen
(Art. 11 DS- GVO)**

Fälle der Pseudonymisierung

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**

Rechtmässig

**(für jeden Datenverarbeitungsvorgang
bedarf es einer Rechtsgrundlage)**

**für den Betroffenen
nachvollziehbar**

2.2.

Zweckbindung

**Zweck des Vereins
bestimmt über die
Zulässigkeit der
Datenverarbeitung !!!**

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 und erforderlich)

Angemessenheit

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

Beachte:

Grundsatz der Datenminimierung

Welche Daten sind dies ?

- * Name und Anschrift**

- * Bankverbindung**

- * Eintrittsdatum**

- * Geburtsjahr (- datum ?)**

- * Kommunikationsverbindungen**

- * Funktionen/Kenntnisse/Fähigkeiten**

Meine Kernpflichten als Ehrenamtlicher ?

- * 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

Zweckabgrenzung/-begrenzung

- **angemessene
Datenverarbeitung**
- **sachlich relevant**
- **begrenzt auf das notwendige
Maß**

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 !**

Praxisproblem:

**Daten von ausgetretenen, ausgeschiedenen
Mitgliedern ?**

2.6.

Integrität und Vertraulichkeit

Schutzvorkehrungen

treffen vor

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

2.7.

Rechenschaftspflicht

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!

2.8.

**Standardfälle aus der
Vereinspraxis**

2.8.1.

**Umgang mit Mitgliederdaten
(Mitgliederliste)**

Herausgabe ?

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

Sonderfall:

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

2.8.2.

**Schwarzes Brett/
Vereinszeitung /Web ?**

In der Regel : NEIN !!!

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**

2.8.7.

Sensible Daten

„Gesundheitsdaten“

**„Treuepflicht“ und „
Verschwiegenheitspflicht“**

=

Schutz der Privatsphäre

(§ 203 StGB Geheimnisträger)

Beispiel:

Medizinischer Bereich

- *die Tatsache, dass ein Behandlungsverhältnis zu einer bestimmten Person bestanden hat,**
- *die Art der Verletzung oder Erkrankung**
- *der Unfallhergang, Krankheitsverlauf etc.,**
- *die Ergebnisse der Untersuchung, die Diagnostik und (Verdachts-)Diagnose**
- *die durchgeführten Maßnahmen sowie**
- *alle übrigen Informationen, die dem Helfer während des Behandlungsverhältnisses bekannt wurden (z. B. Wohn- und Lebenssituation, Sucht, sexuelle Vorlieben, Vermögenslage, körperliche Hygiene).**

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>

Kostenregelung:

Keine Kosten!

Seit 01.08.2013 ist neu, dass die Gebührenbefreiung für ehrenamtlich Tätige unter bestimmten Voraussetzungen gesetzlich verankert ist: Zum 1.8.2013 trat das Zweite Gesetz zur Modernisierung des Kostenrechts (2. Kostenrechtsmodernisierungsgesetz - 2. KostRMoG) in Kraft. Dieses umfangreiche Gesetz fügt nebenbei in das Kostenverzeichnis zum JVKostG, indem die Gebühren geregelt sind, folgende Regelung als Vorbemerkung ein: „Die Gebühren 1130 und 1131 werden nicht erhoben, wenn ein Führungszeugnis zur Ausübung einer ehrenamtlichen Tätigkeit benötigt wird, die für eine gemeinnützige Einrichtung, für eine Behörde oder im Rahmen eines der in § 32 Abs. 4 Nr. 2 Buchstabe d EStG genannten Dienste ausgeübt wird.“

Quellen:

<http://www.dmsj.org/documents/gebuehrenbefreiung-1.pdf>

<http://www.dmsj.org/documents/gebuehrenbefreiung-2.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**

NEU !!!!

3.

**Datenportabilität
(Art. 20 DS-GVO)**

**Das 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)**

3.1.

Voraussetzungen des Anspruchs

**(1) Daten des Betroffenen
(Art. 13 DS- GVO) ?**

(2) Verarbeitungsgrundlage

(2.1.) Einwilligung ?

**(2.2.) zur Erfüllung eines
Vertrages ?**

3.2.

Inhalt des Anspruchs

- **Herausgabe aller Daten**
 - **strukturiert**
- **in gängig maschinenlesbarem Format**

Herausgabe an

- **Betroffenen**
- **anderen Verantwortlichen**
 - **(Art. 20 III DS- GVO))**

3.3.

Ausschluss des Anspruchs

(-) kein Rechtsanspruch gegeben

**(-) Beeinträchtigung Rechte
Dritter**

**(-) Untrennbarkeit der Daten
Betroffener vs. Dritter**

**(-) vorgehende Rechte des
Verantwortlichen**

(-) vorgehende Rechte des Verantwortlichen

**-Urheberrechte, gewerbliche Schutzrechte,
Betriebs- und Geschäftsgeheimnisse-**

**(-) kein Recht auf Herausgabe,
wenn dies technisch nicht
machbar ist.**

3.4.

Form der Datenübertragung

FORM

- **strukturiert**
- **gängig, maschinenlesbar**

Nicht vorgeschrieben (!!!)

Interoperabilität, Kompatibilität

**Empfehlung nach
Erwägungsgrund 68 Satz 2 DS-
GVO**

***„ ... Entwicklung interoperabler
Formate“***

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 Vergessenwerden
(Art. 17 Abs. 2 DS- GVO)**

Art. 17 Abs. 1 DS- GVO

„Löschung“

Informationen Anderer über

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

6.

Konkret im Überblick

Die Rechte des Bürgers....

Recht auf

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

IV.

**Datenschutzbeauftragter
(Art. 37 DS- GVO)**

Grundsatz der Selbstkontrolle

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)

Kernbereiche der Tätigkeit

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

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

**Mehr als 10 Menschen
verarbeiten (erheben, speichern,
nutzen...) personenbezogene
Daten** (Argument aus § 4 f BDSG)

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**

V.

**Verarbeitungen,
Prozesssicherheit**

1.

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

Art. 25 DS- GVO

Privacy by Design

**Technische und organisatorische
Maßnahmen**

Privacy by Default

- **Datenminimierung durch entsprechende Voreinstellungen bei Online-Diensten**
 - **Datensparsamkeit**

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**

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**

VI.

Bußgelder, Sanktionen

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

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

1.

Art. 83 DS- GVO

**... wirksam ... verhältnismäßig...
abschreckend**

2.

**Beschwerde bei der
Aufsichtsbehörde**

3.

Verbandsklage

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

4.

Schadenersatz, Strafe

Bußgeld

VII.

Sonderfälle

1.

Website- Compliance

Jetzt handeln:

Datenschutzerklärung anpassen an DSGVO

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

Weiter beachten:

§§ 11 ff. TMG, § 13 TMG

Weitere Informationen:

<https://translate.google.de/translate?hl=de&sl=en&u=https://www.out-law.com/page-5813&prev=search>

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

Weiterführende Informationen:

<https://www.datenschutzbeauftragter-info.de/data-breach-notification-datenpannen-in-der-dsgvo/>

**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**

VIII.

**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

XIX.

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/ch
eckliste.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 _____

X.

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**

Vielen lieben

**Dank für ihre Aufmerksamkeit
und aktive Mitarbeit**

Ihr

Malte Jörg Uffeln

www.maltejoerguffeln.de