

# EU- Datenschutz- grundverordnung

V  
E  
R  
E  
I  
N  
S  
M  
A  
N  
A  
G  
E  
M  
E  
N  
T

# EU-DSGVO

## Die „neue“ EU- Datenschutzgrundverordnung

Am 25.05.2018 trat die neue EU-  
weite Datenschutz-Grundverordnung  
in Kraft. Sie gilt als „nationales“  
Recht und entfaltet daher unmittel-  
bares Recht. Eine Übergangsfrist gibt  
es nicht.

# EU-DSGVO

## Schlechte Nachricht:

**Alle Vereine sind betroffen!**

**Datenschutz ist „Chiefsache“**

(Datenschutzbeauftragter  
berät und unterstützt)

# EU-DSGVO

## Gute Nachricht:

**Alte Informationen gelten fort!**

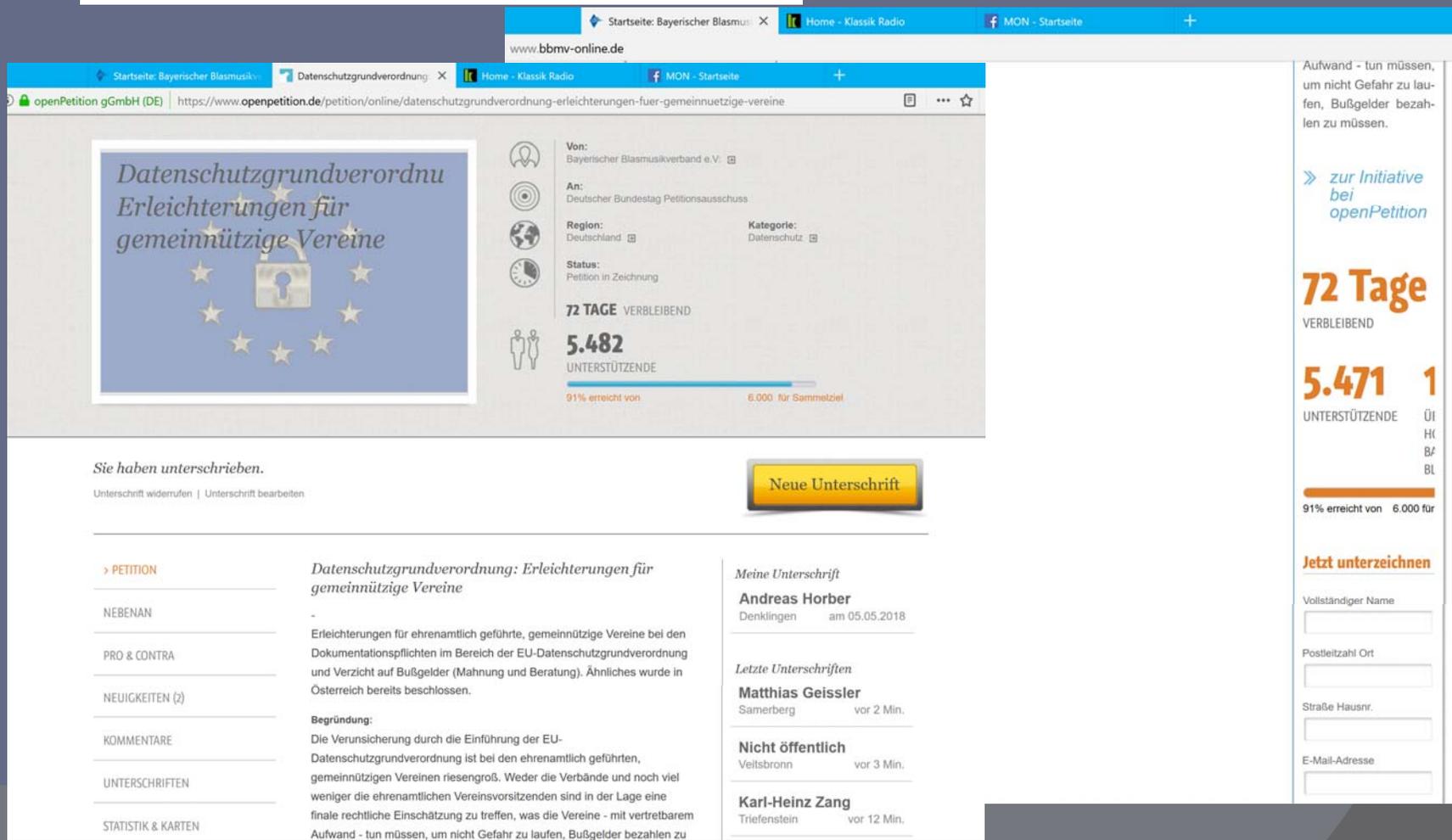
(falls sie bereits einen Hinweis auf  
das Widerrufsrecht enthalten.)

**Maßnahmen nur für neue  
Mitglieder!**

# EU-DSGVO



## Petition des BMWV:



Startseite: Bayerischer Blasmusik... Home - Klassik Radio MON - Startseite

www.bbmwv-online.de

Startseite: Bayerischer Blasmusik... Datenschutzgrundverordnung: X Home - Klassik Radio MON - Startseite

openPetition gGmbH (DE) | https://www.openpetition.de/petition/online/datenschutzgrundverordnung-erleichterungen-fuer-gemeinnuetzige-vereine

**Von:** Bayerischer Blasmusikverband e.V.

**An:** Deutscher Bundestag Petitionsausschuss

**Region:** Deutschland **Kategorie:** Datenschutz

**Status:** Petition in Zeichnung

**72 TAGE** VERBLEIBEND

**5.482** UNTERSTÜTZENDE

91% erreicht von 6.000 für Sammelziel

Aufwand - tun müssen, um nicht Gefahr zu laufen, Bußgelder bezahlen zu müssen.

» zur Initiative bei openPetition

**72 Tage** VERBLEIBEND

**5.471** UNTERSTÜTZENDE

91% erreicht von 6.000 für

**Jetzt unterzeichnen**

Vollständiger Name  
Postleitzahl Ort  
Straße Hausnr.  
E-Mail-Adresse

**Sie haben unterschrieben.**  
Unterschrift widerrufen | Unterschrift bearbeiten

**Neue Unterschrift**

> PETITION

NEBENAN

PRO & CONTRA

NEUIGKEITEN (2)

KOMMENTARE

UNTERSCHRIFTEN

STATISTIK & KARTEN

**Datenschutzgrundverordnung: Erleichterungen für gemeinnützige Vereine**

-

Erleichterungen für ehrenamtlich geführte, gemeinnützige Vereine bei den Dokumentationspflichten im Bereich der EU-Datenschutzgrundverordnung und Verzicht auf Bußgelder (Mahnung und Beratung). Ähnliches wurde in Österreich bereits beschlossen.

**Begründung:**  
Die Verunsicherung durch die Einführung der EU-Datenschutzgrundverordnung ist bei den ehrenamtlich geführten, gemeinnützigen Vereinen riesengroß. Weder die Verbände und noch viel weniger die ehrenamtlichen Vereinsvorsitzenden sind in der Lage eine finale rechtliche Einschätzung zu treffen, was die Vereine - mit vertretbarem Aufwand - tun müssen, um nicht Gefahr zu laufen, Bußgelder bezahlen zu

**Meine Unterschrift**

**Andreas Horber**  
Denklingen am 05.05.2018

**Letzte Unterschriften**

**Matthias Geissler**  
Samerberg vor 2 Min.

**Nicht öffentlich**  
Veltsbronn vor 3 Min.

**Karl-Heinz Zang**  
Triefenstein vor 12 Min.

# EU-DSGVO

## Landesamt für Datenschutzaufsicht

V  
E  
R  
E  
I  
N  
S  
M  
A  
N  
A  
G  
E  
M  
E  
N  
T



# Literatur-Hinweise

- „Kleiner Leitfaden für Musikvereine und -verbände“ (BDMV)

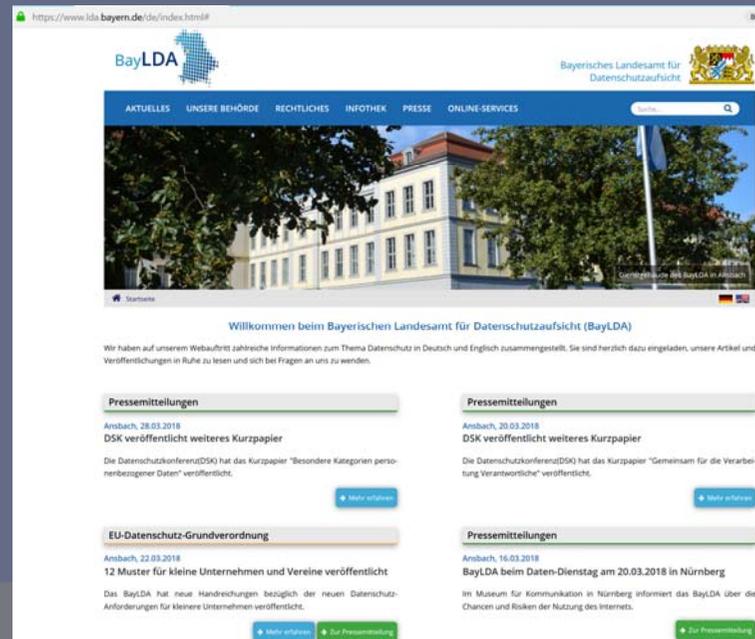
- „Erste Hilfe zur DSGVO“  
C.H.Beck



# Literatur-Hinweise

- Bayerisches Landesamt für  
Datenschutz

[www.ida.bayern.de](http://www.ida.bayern.de)



The screenshot shows the homepage of the Bayerisches Landesamt für Datenschutzaufsicht (BayLDA). The page features a blue header with the BayLDA logo and navigation links: AKTUELLES, UNSERE BEHÖRDE, RECHTLICHES, INFOTHEK, PRESSE, and ONLINE-SERVICES. Below the header is a large photograph of the BayLDA building in Ansbach. The main content area is titled "Willkommen beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)" and includes a welcome message. There are four news sections, each with a title, date, and a "Mehr erfahren" button. The sections are: 1. "DSK veröffentlicht weiteres Kurzpapier" (Ansbach, 28.03.2018), 2. "EU-Datenschutz-Grundverordnung" (Ansbach, 22.03.2018), 3. "DSK veröffentlicht weiteres Kurzpapier" (Ansbach, 20.03.2018), and 4. "BayLDA beim Daten-Dienstag am 20.03.2018 in Nürnberg" (Ansbach, 16.03.2018).

# EU-DSGVO

## ○ Prinzipien der Datenverarbeitung

### Prinzipien der Datenverarbeitung nach Art. 5 EU-DSGVO

Allgemeine Grundsätze der Datenverarbeitung – analog den Prinzipien des BDSG

- **Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**
  - Verarbeitung soll auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbare Weise geschehen
- **Zweckbindung**
  - Die Verarbeitung darf nur für im vorhinein festgelegte Zwecke erfolgen und nicht in einer nicht mit diesem Zweck zu vereinbarenden Weise weiterverarbeitet werden
- **Datenminimierung**
  - Verarbeitung muss dem Zweck angemessen und auf das notwendige Maß beschränkt sein
- **Richtigkeit**
  - Daten müssen richtig und auf aktuellem Stand sein. Unrichtige Daten müssen unverzüglich berichtigt oder gelöscht werden
- **Speicherbegrenzung**
  - Daten dürfen nur so lange gespeichert werden, wie es für den betreffenden Zweck erforderlich ist
- **Integrität und Vertraulichkeit**
  - Es muss über ausreichenden Schutz gegen unbefugte oder unrechtmäßige Verarbeitung, Zerstörung oder Schädigung gesorgt werden
- **Rechenschaftspflicht**
  - Einhaltung der o.g. Prinzipien muss durch Verantwortlichen nachgewiesen werden => Erfordernis eines Datenschutz-Management-Systems

# EU-DSGVO

## ○ Erste Schritte

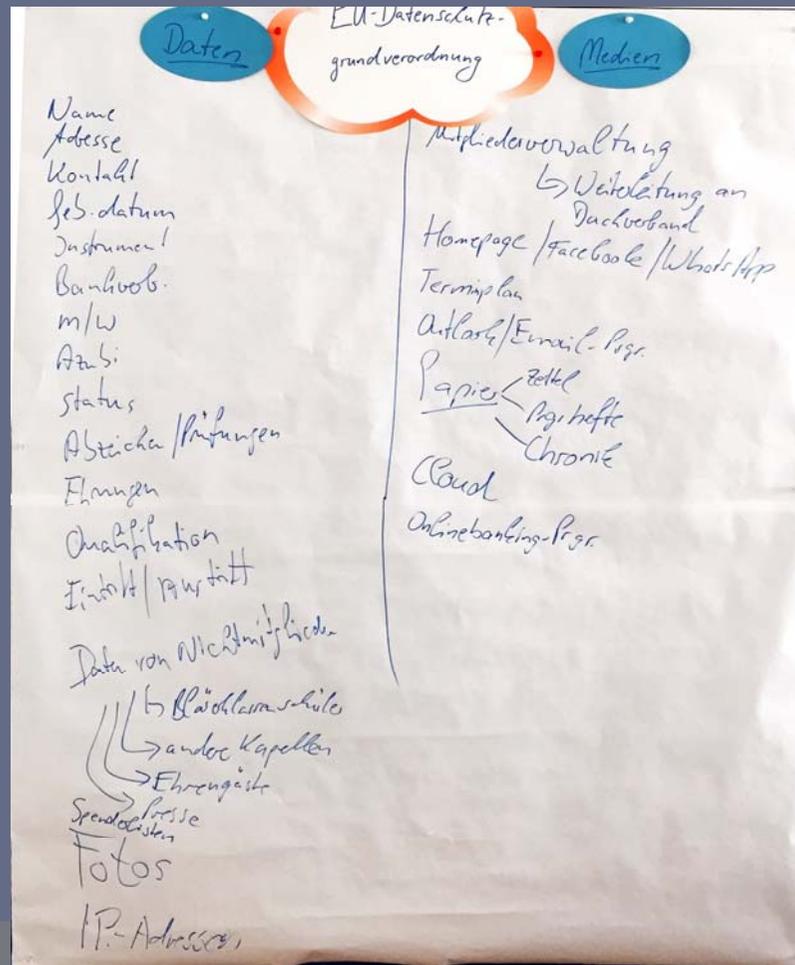
- Bestandsaufnahme, wo im Verein welche Daten verarbeitet werden
- Kritische Punkte in der Sichtbarkeit des Vereins nach außen überprüfen, dass sie nicht augenfällig der neuen DSGVO widersprechen.
  - Impressum & Datenschutz auf Homepage
  - Impressum Social Media
- Erstellung Datenschutzordnung

# EU-DSGVO

- Die DSGVO lenkt den Fokus auf Datenschutz
  - Quer: Thema Sendung 12.4.2018
  - Bayern 1: Thema Morgensendung am 19.4.2018
  - Google: 1.460.000 Suchergebnisse
  - Im MON: Diskussion über Prozesse, die schon seit Jahren/Jahrzehnten problemlos laufen.
    - Täglich neue Unterlagen

# EU-DSGVO

- ◉ Wo im Verein werden welche Daten verarbeitet?



# EU-DSGVO

## ○ Umsetzung

- Festlegung der Rechtsgrundlagen
- Einwilligungen einholen
- Prüfung, ob Daten zur Verarbeitung nach außen gegeben werden (Auftragsverarbeitung)
- Informationspflichten gegenüber den Betroffenen und Auskunftsrechte vorbereiten
- Vorsorge für Datenschutz durch Technik und Organisation treffen

# EU-DSGVO

## Übersicht der EU – DSGVO

- **Allgemeine Bestimmungen**
  - **Rechtmäßigkeit der Verarbeitung (Art. 6)**
  - **Einwilligung zur Verarbeitung (Art. 7)**
- **Rechte der betroffenen Personen**
  - **Informationspflicht bei Erhebung der Daten beim Betroffenen (Art. 13)**
  - Informationspflicht bei Erhebung der Daten bei Dritten (Art. 14)
  - **Auskunftsrecht des Betroffenen (Art. 15)**
  - Sonstige Rechte (Berichtigung, Löschung) (Art. 16, 17), (Einschränkung, Datenübertragung) (Art. 18, 20)
  - Recht auf Beschwerde bei der Aufsichtsbehörde (Art. 77),
- **Widerspruchsrecht im Einzelfall**
- **Handlungspflichten des Verantwortlichen**
  - Informationspflicht bei Erhebung der Daten (Art. 13)
  - Sicherheit der Verarbeitung (Risikoeinschätzung) (Art. 32)
  - Meldung bei Verletzungen an Aufsichtsbehörde (Art. 33)
- **Verantwortung für die Verarbeitung**
  - **Generelle Verantwortung des Verantwortlichen (Art. 24),**
  - **Datenschutz durch Technikgestaltung und Organisation (Art. 25, 26),**
  - Auftragsverarbeitung (Art. 28, 29)
  - **Verzeichnis der Verarbeitungstätigkeiten (Art. 30)**
  - Zusammenarbeit auf Anfrage der Aufsichtsbehörde (Art. 31)
- **Datenschutzbeauftragter**
  - **Benennung eines Datenschutzbeauftragten (Art. 37, § 38 BDSG),**
  - Stellung des Datenschutzbeauftragten (Art. 38),
  - Aufgaben des Datenschutzbeauftragten (Art. 39)
- **Aufsichtsbehörden**
  - Aufsichtsbehörde (Art. 51 ff)
  - **Sanktionen, Bußgelder Art. 83, §§ 41, 43 BDSG**

# EU-DSGVO

- Welche Vereine sind betroffen?  
Alle Vereine, die personenbezogene Daten verarbeiten, unabhängig
  - wie groß der Verein ist.
  - wie viele Personen mit den Daten arbeiten.
  - ob die Verarbeitung über EDV oder mit Karteikarten erfolgt.

=> also eigentlich IMMER !

# EU-DSGVO

- Beispiele für Datenverarbeitung
  - Speicherung von Mitgliedsdaten
  - Weitergabe von Daten an Dachverbände
  - Veröffentlichung von Daten auf der Homepage und bei Facebook
  - Veröffentlichung von Daten in der Vereinszeitschrift
  - Aushänge am Schwarzen Brett

# EU-DSGVO

- Was sind personenbezogene Daten?
  - Name, Vorname, Adressen, Kontaktdaten, Bankverbindungen
  - Daten von Kunden und Geschäftspartnern (soweit nicht juristische Personen)
  - Daten von Ehrenamtlichen und Mitarbeitern
  - IP-Adressen (!?!?)

# EU-DSGVO

- Hinweis „besondere Arten von personenbezogenen Daten“
    - Familienstand
    - Religionszugehörigkeit / Ethnische Herkunft / Politische Meinung
    - Gesundheitsdaten
- => Pflicht Datenschutzbeauftragter

Tipp:

Keine „besonderen Daten“ speichern!

# EU-DSGVO

- Wann muss ein Datenschutzbeauftragter benannt werden?
    - i.d.R. wenn mind. 10 Personen ständig mit der automatisierten Datenverarbeitung betraut sind
    - Egal, ob ehrenamtlich oder beruflich
    - Bei „besonderen“ Daten!
- => Verarbeitungstätigkeiten auf weniger als 10 Personen eingrenzen!

# EU-DSGVO

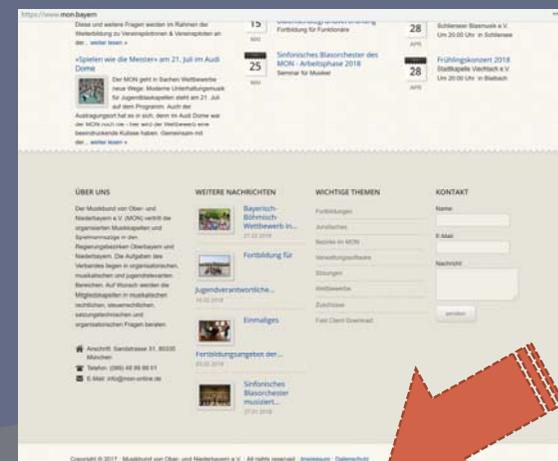
- Wann muss ein Datenschutzbeauftragter benannt werden?
  - Achtung: Instrumentallehrer zählen zu den Personen, die regelmäßig Daten verarbeiten, wenn die Ausbildung über den Verein läuft und eine rechtliche Beziehung zwischen Verein und Lehrer besteht!  
=> Daten in Listenform übergeben  
(nicht automatisiert)

# EU-DSGVO

- Homepage/ Facebook: Impressum / Datenschutz
  - Korrekte und an DSGVO angepasstes Impressum (und Datenschutz) ist Pflicht, da von außen einsehbar !!!
  - Impressum-Generatoren, z.B.  
[www.e-recht24.de](http://www.e-recht24.de) (kostenpflichtig)  
[www.ratgeberrecht.eu/leistungen/muster-datenschutzerklaerung.html#Generator](http://www.ratgeberrecht.eu/leistungen/muster-datenschutzerklaerung.html#Generator)

# EU-DSGVO

- Homepage/ Facebook: Impressum / Datenschutz
  - Impressum muss auch so benannt sein
  - Impressum muss als „Seite“ vorhanden sein (nicht als pdf zum Download)
  - Impressum muss gut lesbar sein
  - Zwei-Klick-Regel



# EU-DSGVO

- Homepage / Datenschutzerklärung
  - Eine Datenschutzerklärung ist nach DSGVO aufzunehmen, wenn personenbezogene Daten verarbeitet werden:  
Kontaktformulare, Newsletter-Anmeldungen, Tools zum Benutzerverhalten wie zB Google-Analytics

# EU-DSGVO

- Wann dürfen Daten verarbeitet werden?
  - Grundsatz:  
„Verbot mit Erlaubnisvorbehalt“

Entweder

- Gesetzliche Grundlage
- Einwilligung des Betroffenen

# EU-DSGVO

- Gesetzliche Grundlagen:
  - Rechtliche Verpflichtung  
z.B. Aufbewahrung von Buchhaltungs-  
unterlagen
  - Zur Vertragserfüllung notwendig  
z.B. Mitgliedschaft = Vertrag
  - Interesse des Vereins  
z.B. Datenübermittlung an
    - Dachverbände, GEMA, Versicherung
    - Lohnbuchhaltung, Homepage etc. im  
Rahmen einer Auftragsdatenverarbeitung

# EU-DSGVO

## ⊙ Einwilligung

- z.B. Nutzung von Fotos, z.T. Veröffentlichung von Daten im Internet etc.
- z.B. Weitergabe von Schülerdaten an Instrumentaltrainer
- Möglichst im Aufnahmeantrag
- Auch wenn Datenschutz in Satzung oder als Ordnung.

# EU-DSGVO

- Was muss in Einwilligung?
  - Freiwillige Entscheidung
  - Welche Daten gespeichert werden?  
Bezogen auf eine bestimmte Verarbeitung.
  - Zu welchen Zwecken?  
Bezogen auf einen bestimmten Zweck.
  - Hinweis auf Widerrufmöglichkeit
  - Möglichst schriftlich!
- TIPP: analog und digital, weil nachweisbar

# EU-DSGVO

- Verarbeitungsverzeichnis 

„Kein Verzeichnis

=

Bußgeld“



# EU-DSGVO

- Auftragsdatenverarbeitung
  - Auftragsdatenverarbeitung ist die Datenverarbeitung im Auftrag durch einen Dritten, bei der die Verantwortung für die ordnungsgemäße Datenverarbeitung beim Auftraggeber verbleibt.
  - Der Auftragnehmer (Dienstleister) wird in diesen Konstellation nur unterstützend tätig und ist bildlich als verlängerter Arm des Auftraggebers anzusehen.
  - Eine Weitergabe von Daten im Rahmen einer Auftragsdatenverarbeitung stellt keine Übermittlung von Daten dar und ist daher unter erleichterten Voraussetzungen möglich.

# EU-DSGVO

## ○ Auftragsdatenverarbeitung

- Klassische Bereiche der Auftragsdatenverarbeitung sind beispielsweise:
    - Externe Lohn- bzw. Gehaltsabrechnung
    - Homepage-Hosting
    - Ausgelagerte Rechenzentren (Clouds)
    - Wartung und Fernzugriffe, wenn Datenzugriff
    - Dienstleisterverträge zur Datenträgerentsorgung
- => Verträge von Firmen einfordern!

# EU-DSGVO

- Auftragsdatenverarbeitung
  - Keine Auftragsdatenverarbeitung sind beispielsweise:
    - Berufsgeheimnisträger wie Steuerberater, Rechtsanwälte
    - Kreditinstitute
    - Postdienste

# EU-DSGVO

## ○ Auftragsdatenverarbeitung

Nichtamtliches Inhaltsverzeichnis

### Bundesdatenschutzgesetz (BDSG)

#### § 11 Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag

(1) Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich. Die in den §§ 6, 7 und 8 genannten Rechte sind ihm gegenüber geltend zu machen.

(2) Der Auftragnehmer ist unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Der Auftrag ist schriftlich zu erteilen, wobei insbesondere im Einzelnen festzulegen sind:

1. der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Er kann bei öffentlichen Stellen auch durch die Fachaufsichtsbehörde erteilt werden. Der Auftraggeber hat sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.

(3) Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers erheben, verarbeiten oder nutzen. Ist er der Ansicht, dass eine Weisung des Auftraggebers gegen dieses Gesetz oder andere Vorschriften über den Datenschutz verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

(4) Für den Auftragnehmer gelten neben den §§ 5, 9, 43 Abs. 1 Nr. 2, 10 und 11, Abs. 2 Nr. 1 bis 3 und Abs. 3 sowie § 44 nur die Vorschriften über die Datenschutzkontrolle oder die Aufsicht, und zwar für

1. a) öffentliche Stellen,  
b) nicht-öffentliche Stellen, bei denen der öffentlichen Hand die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist,  
die §§ 18, 24 bis 26 oder die entsprechenden Vorschriften der Datenschutzgesetze der Länder,
2. die übrigen nicht-öffentlichen Stellen, soweit sie personenbezogene Daten im Auftrag als Dienstleistungsunternehmen geschäftsmäßig erheben, verarbeiten oder nutzen, die §§ 4f, 4g und 38.

(5) Die Absätze 1 bis 4 gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann.

# EU-DSGVO

- Technischer & organisatorischer Datenschutz
  - Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personentreffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem *Risiko angemessenes Schutzniveau zu gewährleisten*; [...]

# EU-DSGVO

- Technischer & organisatorischer Datenschutz
  - PC und LapTop mit Passwort schützen
  - Sichere Passwörter & regelmäßig ändern
  - Firewall und Antiviren-Programm (Virens Scanner)
  - Datensicherung auf externe Festplatte (Festplatte mit Passwort schützen oder wegsperren)
  - Verschlüsselung von Servern und LapTops
  - Updates von Betriebssystem & Browser

# EU-DSGVO

- Tipp für sichere Passwörter
  - "Kombinieren Sie ein Masterpasswort mit einem seitenspezifischen Passwort.  
"DasMasterpasswort - zum Beispiel Hc84#  
- ergänzen Sie mit einer für jede Website einzigartigen Zeichenkette.
  - Lange Passwörter mit Eselsbrücken, z.B.  
„Musik spielen mit einem Blasinstrument  
macht schlau, besonders mich!“  
=> MsmeBms,bm-\_\_ (Kürzel des  
Programms) => M\$meBm\$,bm-\_\_

# EU-DSGVO

- Technischer & organisatorischer Datenschutz
  - Sperren von PC/LapTop bei Abwesenheit
  - Bewusste Nutzung von Cloud-Speichern
  - Vertrauliche Daten in Papierform wegsperren
  - Personenbezogene Daten auf Papier nicht in den Papierkorb => Aktenvernichter
  - Email-Versand: max. 1 Email in „An“ bzw. „CC“ ansonsten „BCC“

# EU-DSGVO

- Technischer & organisatorischer Datenschutz
  - Sicherheitskonzept für alle „Mitarbeiter“ (Ehrenamtliche)
  - Verpflichtungserklärung für alle Personen, die mit personenbezogenen Daten arbeiten

# EU-DSGVO

## Datenschutzverpflichtung Ehrenamtliche

*Sie verarbeiten in Ihrer Funktion als ..... im ehrenamtlichen Bereich personenbezogene Daten auf Ihrem PC und sind daher verantwortlich für die Einhaltung der gesetzlichen Datenschutzbestimmungen. Bitte beachten Sie daher als notwendige Mindestmaßnahmen und Regeln:*

- 1. Daten dürfen nur im zwingend erforderlichen Rahmen erfasst werden.*
- 2. Anwesenheitslisten sind über Namen, Vornamen und Funktion ohne weitere Informationen anzulegen.*
- 3. Der Zugang zum Vereinsbereich ist durch ein sicheres Passwort zu sichern.*
- 4. Bei Internetanschluss sind Virenschutzprogramm und Software-Firewall unerlässlich.*
- 5. Datensicherungen sind regelmäßig durchzuführen, Speichermedien sind sicher aufzubewahren.*
- 6. Bei Beendigung des Ehrenamts sind alle Daten an den Nachfolger zu übergeben und auf Ihrem PC zu löschen.*
- 7. Daten auf Papier sind vollständig zu übergeben, nicht mehr benötigte Dokumente zu vernichten.*

# EU-DSGVO

- Betroffenenrechte
  - Recht auf Auskunft
  - Recht auf Berichtigung
  - Recht auf Löschung
  - Recht auf Einschränkung der Verarbeitung
  - Recht auf Datenübertragbarkeit
  - Widerspruchsrecht

# EU-DSGVO

- Betroffenenrechte: Recht auf Auskunft
  - Jeder Betroffene kann vom Verein eine Auskunft verlangen, ob und welche Daten über ihn gespeichert sind. Auskunft ist innerhalb eines Monats zu erteilen:
    - die Zwecke, weshalb der Verein Daten über ihn verarbeitet,
    - die Kategorien der über ihn gespeicherten Daten,
    - evtl. Empfänger, wenn Daten weiter gegeben werden,
    - die Speicherdauer

# EU-DSGVO

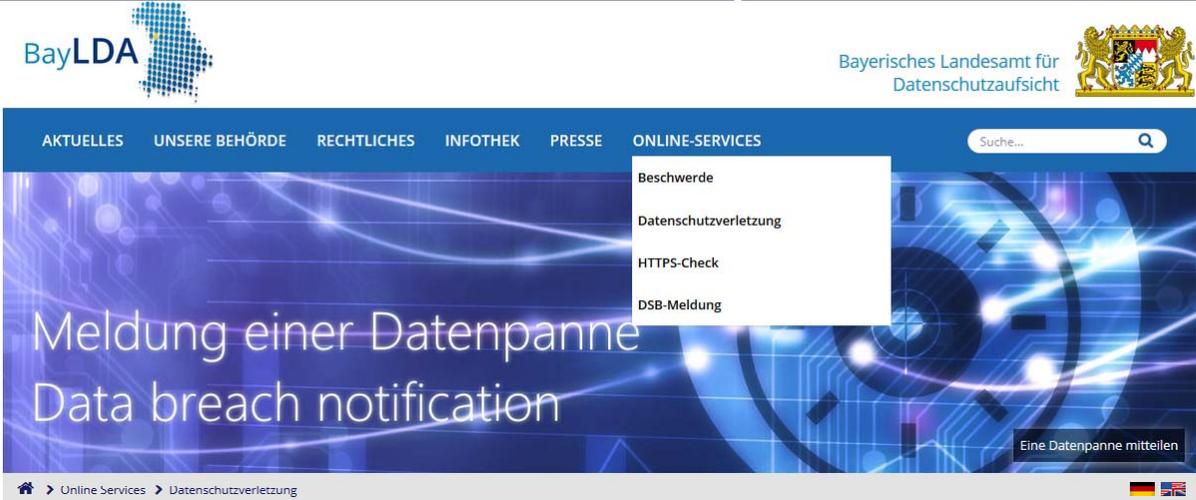
- Betroffenenrechte: Recht auf Löschung
  - Eine Löschung muss durchgeführt werden, wenn
    - die Daten nicht mehr benötigt werden, weil der Zweck entfallen ist,
    - die Daten unrechtmäßig verarbeitet wurden,
    - der Betroffene seine Einwilligung widerrufen hat,
    - der Betroffene im Einzelfall Widerspruch eingelegt hat und der Widerspruch berechtigt ist.

# EU-DSGVO

- Verhalten bei Datenpannen
  - Begriff der „Datenpanne“ ist weitgefasst – vom Falschversand von Emails bis zum Hackerangriff
  - Meldepflichten gegenüber Behörden und Betroffenen innerhalb von i.d.R. 72 Stunden

# EU-DSGVO

## ○ Verhalten bei Datenpannen



**BayLDA** Bayerisches Landesamt für Datenschutzaufsicht

AKTUELLES UNSERE BEHÖRDE RECHTLICHES INFOTHEK PRESSE ONLINE-SERVICES

Suche...

Beschwerde  
Datenschutzverletzung  
HTTPS-Check  
DSB-Meldung

Meldung einer Datenpanne  
Data breach notification

Eine Datenpanne mitteilen

Online Services > Datenschutzverletzung

**Meldung einer Datenpanne - online & sicher**

Auf dieser Seite bieten wir die einfache Möglichkeit an, eine Meldung von Verletzungen des Schutzes personenbezogener Daten, umgangssprachlich Datenpannen genannt, durchzuführen. Die Meldung erfolgt dabei über ein Online-Formular, das eine verschlüsselte Übertragung Ihrer Angaben gewährleistet. Sollten Sie Fragen zu den Hintergründen bei Datenpannen haben, können Sie unser [Infoblatt](#) in Ruhe zu lesen.

**! Online-Meldung einer Datenpanne**

1. SCHRITT: WER MELDET UNS EINEN VORFALL?

Name  
Ihr Name

Straße und Hausnummer  
Ihre Straße und Hausnr.

PLZ

# EU-DSGVO

- Wer überwacht den Datenschutz im Verein

Bayerisches Landesamt für  
Datenschutzaufsicht

Promenade 27

91522 Ansbach

Telefon: 0981/53-1300

[www.lida.bayern.de](http://www.lida.bayern.de)

# EU-DSGVO

## ○ Bußgelder

### Bußgelder und Sanktionen

Bußgeldbewährte Verstöße in Höhe von bis zu 10 Mio. sowie in Höhe von bis zu 20 Mio. Euro

▪ **Bis 10 Mio. EUR / 2% d. weltweiten Jahresumsatz**

nach Art. 83 Abs. 4 DSGVO

- Einwilligung von Kindern (Art. 8 DSGVO)
- ADV (auch gg. Auftragnehmer! - Art. 29 DSGVO)
- Unzureichende Dokumentation (Art. 30 DSGVO)
- Zusammenarbeit mit der Aufsichtsbehörde (Art. 31 DSGVO)
- Unzureichende TOMs (bisher nicht bußgeldbewehrt - Art. 32 DSGVO)
- Meldung von Datenschutzverstößen an Aufsicht und betroffene Personen (Art. 33,34 DSGVO)
- Nicht durchgeführte DS-Folgenabschätzung bzw. Konsultation der Aufsicht (Art. 35, 36 DSGVO)
- Benennung, Stellung und Aufgaben des DSB (Art. 37, 38, 39 DSGVO)
- Pflichten der Überwachungs- und Zertifizierungsstellen (Art. 41,42,43 DSGVO)

▪ **Bis 20 Mio. / 4% d. weltweiten Jahresumsatzes**

(je nachdem was höher ist)

- Verstöße gegen Grundsätze nach Art. 5 DSGVO
- Verstoß gegen Rechtmäßigkeit der Verarbeitung (Art. 6 DSGVO)
- Verarbeitung ohne Einwilligung (Art. 7 DSGVO)
- Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)
- Verstöße bei Beachtung der Rechte betroffener Personen (Art. 12-22 DSGVO)
- Verstöße bei Drittlandsübermittlungen (z.B. in die USA - Art. 44-49 DSGVO)
- Verstöße gegen Vorschriften der Mitgliedsstaaten in besonderen Verarbeitungssituationen nach Kapitel IX DSGVO
- Verstöße bei der Zusammenarbeit mit der Aufsichtsbehörde
- Verstöße gegen Anordnungen der Aufsichtsbehörde

# EU-DSGVO

- Facebook als Kommunikationsmittel:
  - Sowohl die Nutzung einer Facebook-Fanpage bzw. –Seite als auch
  - die Nutzung von Social-Media-PlugIns auf der Vereinshomepage ist DSGVO-mäßig problematisch und kaum sicher hinzukommen.

TIPP:

Social-Medias aus Homepage entfernen  
bzw. Shariff-/2-Klick-Lösung anwenden

# EU-DSGVO

- WhatsApp als Kommunikationsmittel:
    - Kontaktdaten aus dem „Adressbuch“ werden an WhatsApp und damit Facebook in die USA übertragen.
    - WhatsApp sammelt unkontrolliert Metadaten von Nutzern (welche Nutzer wann mit wem, wie oft und worüber kommuniziert haben) zur Erstellung von Nutzerprofilen
- => Verstoß gegen EU-DSGVO

# EU-DSGVO

- WhatsApp-Gruppe:
    - entspricht nicht den Datenschutzbestimmungen der EU-DSGVO, da der Verein den ihm auferlegten Informationspflichten gegenüber den Betroffenen nicht nachkommen kann
    - egal ob die Betroffenen eingewilligt haben oder nicht!!!
- => Nur private Gruppenbildung unter Mitgliedern möglich!

# EU-DSGVO

- Nutzung von Fotos
  - Nicht DSGVO, sondern KUG
  - Fotos, die Personen abbilden, enthalten personenbezogene Daten (auch ohne die Angabe der Namen).
  - Bildnisse dürfen nur mit Einwilligung des Abgebildeten verbreitet oder öffentlich zur Schau gestellt werden.  
Die Einwilligung gilt im Zweifel als erteilt, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt.

# EU-DSGVO

- Nutzung von Fotos
  - Grundsätzlich Einwilligung.
  - Ausnahmen:
    - Bildnis aus dem Bereich der Zeitgeschichte
    - Bilder auf denen die Personen nur Beiwerk von Landschaften oder Örtlichkeiten sind
    - Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben. (Menschenansammlungen)

# EU-DSGVO

- Nutzung von Fotos
  - „Menschenansammlungen“  
Wer an öffentlichen Veranstaltungen teilnimmt, muss damit rechnen, abgebildet zu werden und muss dies in gewissen Grenzen akzeptieren. Die Vorschrift erfasst Veranstaltungen aller Art, wie öffentliche Demonstrationen, Karneval-Umzüge, Sportveranstaltungen, Konzerte und Kongresse.

# EU-DSGVO

- Nutzung von Fotos - Beispiele
  - Festzug  
Fotos dürfen ohne Einwilligung verbreitet werden, auch im Internet
  - Politiker-Besuch  
Politiker sind Personen der Zeitgeschichte. Die sonstigen Personen sind Beiwerk.
  - Musikverein will Konzertbesuch dokumentieren. Auf Fotos sind Gesichter einzelner Zuhörer erkennbar. Fotos ohne Einwilligung zulässig (Versammlung)

# EU-DSGVO

- Nutzung von Fotos => Fazit
  - Besser Einwilligung!
  - Einwilligung von Mitgliedern:  
Vorbeugende, allgemeine Einwilligung  
rechtlich nicht gültig.  
Denkbar ist eine Regelung, die auf  
konkrete Situationen bezogen ist, in der  
Satzung oder der Beitrittserklärung zum  
Verein.
  - Besonderes Augenmerk auf Fotos von  
Minderjährigen!

# EU-DSGVO

- Zusammenfassung DSGVO
  - Bestandsaufnahme machen
  - Rechtsgrundlagen der Datenspeicherung prüfen bzw. festlegen
  - Homepage: Impressum und Datenschutz
  - Dokumentation erstellen (Datenschutzordnung, Verarbeitungsverzeichnis)
  - Einwilligungen neu formulieren

# EU-DSGVO

- Zusammenfassung
  - Datenschutz durch Technik und Organisation
  - Auftragsdatenverarbeitung: Verträge machen
  - Melde- und Kontrollpflichten gegenüber Aufsichtsbehörden umsetzen
  - Betroffenenrechte und Informationspflichten umsetzen

# EU-DSGVO

Also fangen Sie an!

Es ist auf jeden Fall besser, mit dem Projekt DSGVO halb fertig zu sein, als – im Fall der Fälle - zugeben zu müssen, dass man noch nicht einmal begonnen hat.