

# Datenschutz-Grundverordnung für kleine Vereine

  
anstiftung

**WEBINAR**  
**2. Mai 2018**

**Thomas Kranig**, Präsident des Bayer.  
Landesamts für Datenschutzaufsicht

## Ausschreibung der Veranstaltung



Einladung zum Webinar

**Datenschutz-Grundverordnung für kleine Vereine**

2. Mai 2018, 19.00 – 21.00 Uhr



**Schau mer mal** 

Ab dem 25. Mai 2018 ist die Datenschutz-Grundverordnung (DSGVO) anzuwenden, die die Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen regelt und EU-weit vereinheitlicht. Doch was bedeutet das konkret für Vereine und andere ehrenamtliche Gruppen, die Daten von Mitgliedern oder Besucher\*innen erheben?

Das Webinar beschäftigt sich u.a. mit folgenden Fragen:

- Was müssen kleine Vereine konkret machen, um den Anforderungen der Datenschutz Grundverordnung zu genügen?
- Ist es notwendig, dass kleine Vereine eine\*n Datenschutzbeauftragte\*n bestellen?
- Was bedeuten die neuen Informationspflichten konkret?
- Müssen auch kleine Vereine mit Sanktionen rechnen?
- Wo kann man nähere Informationen bekommen?

# Agenda

- 1 Datenschutz – was ist das?
- 2 Datenschutz – was kommt mit der DS-GVO auf uns zu?
- 3 Umgang mit Bildern
- 4 Rolle und Aufgabe der Datenschutzaufsicht
- 5 Empfehlung zum Schluss

# Agenda

- 1** **Datenschutz – was ist das?**
- 2** Datenschutz – was kommt mit der DS-GVO auf uns zu?
- 3** Umgang mit Bildern
- 4** Rolle und Aufgabe der Datenschutzaufsicht
- 5** Empfehlung zum Schluss



# Was ist Datenschutz?

Warum sollte man die DS-GVO beachten?

# Datenschutz ist Grundrechtsschutz



# DATENSCHUTZ

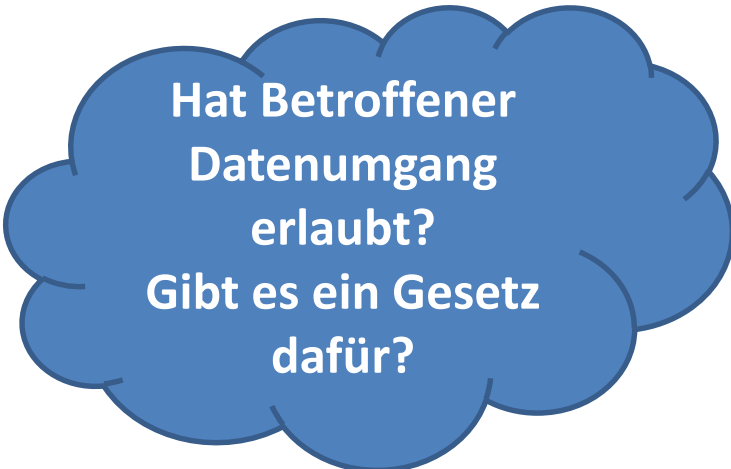
Schutz des Einzelnen vor einer Beeinträchtigung  
des Persönlichkeitsrechts durch den Umgang  
mit seinen personenbezogene Daten

# DATENSICHERHEIT (Safety)

Schutz vor ungewolltem Datenverlust  
(z. B. durch Plattendefekt,  
Feuer, ...)



# Verbot mit Erlaubnisvorbehalt



Hat Betroffener  
Datenumgang  
erlaubt?  
Gibt es ein Gesetz  
dafür?

Die Erhebung, Verarbeitung oder Nutzung **personenbezogener** Daten (Datenumgang) ist zunächst einmal verboten.

Zulässig sind diese Vorgänge nur, wenn eine **Rechtsvorschrift dies erlaubt oder anordnet** oder der Betroffene **eingewilligt** hat.





# Was sind personenbezogene Daten ?

## Definition nach Art. 4 Nr. 1 DS-GVO

„**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 **Merkmale**n, die Ausdruck der **physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen** oder **sozialen Identität** dieser natürlichen Person sind, identifiziert werden kann;



# Welche personenbezogene Daten haben Sportvereine?

## ■ Vereinsmitglieder

- Name
- Adresse
- Telefon
- Sportart
- Kontonummer
- ... (**und vieles mehr**)



## ■ Mitarbeiterdaten

- Name
- Adresse
- Bankverbindung
- Einsatzbereich
- ... (**und vieles mehr**)

## ■ Externe

- Arzt
- Angehörige
- Daten anderer Vereine
- ... (**und vieles mehr**)



Verantwortlicher  
muss prüfen, ob  
er/sie Daten  
verarbeiten darf  
!!



Die Erhebung, Verarbeitung oder  
Nutzung **personenbezogener**  
Daten (Verarbeitung) ist zunächst  
einmal verboten.

Zulässig sind diese Vorgänge nur,  
wenn eine **Rechtsvorschrift dies**  
**erlaubt oder anordnet** oder der  
Betroffene **eingewilligt** hat.



# Agenda

1 Datenschutz – was ist das?

2 **Datenschutz – was kommt mit der DS-GVO auf uns zu?**

3 Umgang mit Bildern

4 Rolle und Aufgabe der Datenschutzaufsicht

5 Empfehlung zum Schluss

# Was kommt auf uns zu?

Amtsblatt  
der Europäischen Union

L 119



Artikel 99

## Inkrafttreten und Anwendung

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union in Kraft.

(2) Sie gilt ab dem 25. Mai 2018.



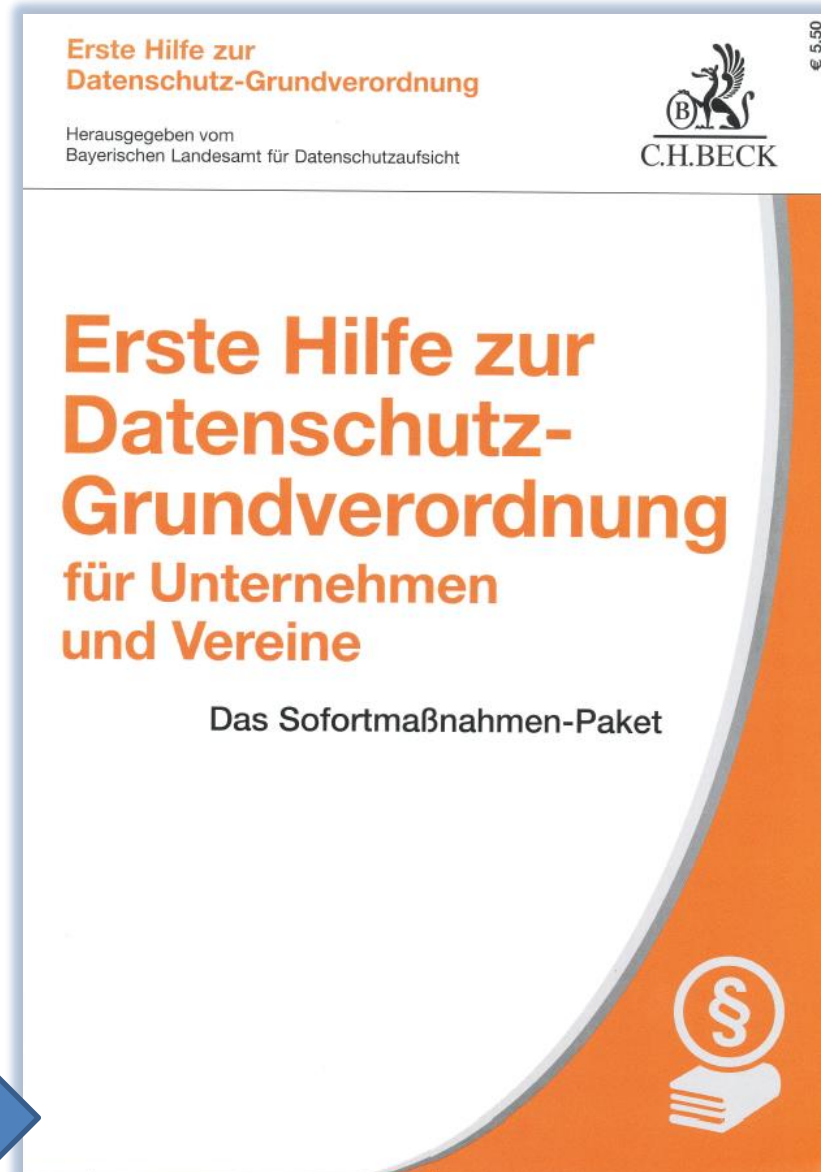
d.h. in  
nur mehr  
**23** Tagen

(<sup>1</sup>) Text von Bedeutung für den EWR

**DE**

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.



**Ehmann / Kranig**

**Erste Hilfe zur  
Datenschutz-  
Grundverordnung**

**Zielgruppe:**

Inhaber kleinerer Unternehmen;  
Vereinsvorsitzende; Datenschutz-  
verantwortliche in kleineren  
Unternehmen und in Vereinen;  
datenschutzinteressierte  
Vereinsmitglieder.

# Datenschutz-Grundverordnung – was kommt da auf uns zu?

Amtsblatt  
der Europäischen Union

L 119



# Datenschutz- Grund-**Verordnung**

verkündet im  
Amtsblatt der Europäischen Union  
vom  
4. Mai 2016

<sup>(\*)</sup> Text von Bedeutung für den EWR

**DE**

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.  
Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.



# Datenschutz-Grundverordnung – was kommt da auf uns zu?

## ■ Rechtsnatur: Verordnung (Art. 288 AEUV)

### KAPITEL 2 RECHTSAKTE DER UNION, ANNAHMEVERFAHREN UND SONSTIGE VORSCHRIFTEN

#### ABSCHNITT 1 DIE RECHTSAKTE DER UNION

#### Artikel 288 (ex-Artikel 249 EGV)

Für die Ausübung der Zuständigkeiten der Union nehmen die Organe Verordnungen, Richtlinien, Beschlüsse, Empfehlungen und Stellungnahmen an.

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

Amtsblatt der Europäischen Union		C 326
Angabe in anderer Sprache	Mitteilungen und Bekanntmachungen	Abkürzung des Gesetzes
Substitutionsnamen	Index	Index
2007/C 093	Konventionen, Protokolle des Vertrags über die Europäische Union und des Vertrags über die Arbeitsweise der Europäischen Union	1
	Vertrag über die Europäische Union (konsolidierte Fassung)	13
	Vertrag über die Arbeitsweise der Europäischen Union (konsolidierte Fassung)	47
	Protokolle	201
	Anträge	211
	Erklärungen zur Schlichter des Streitigkeitsmechanismus, der am 13. Dezember 2007 unterzeichneten Vertrag von Lissabon gegenübersetzt	217
	Charter der Grundrechte	241
2007/C 093	Charta der Grundrechte der Europäischen Union	241
2007/C 093		47

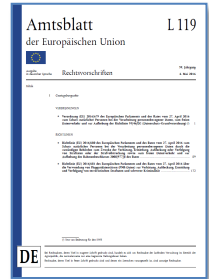


# Für wen gilt die DS-GVO?

# Für wen gilt DS-GVO?

## Artikel 2 DS-GVO: Sachlicher Anwendungsbereich

- (1) 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.

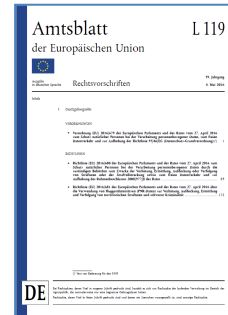


## Artikel 4 Nr. 2 DS-GVO Begriffsbestimmungen

Im Sinne der Verordnung bezeichnet :

„**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

## Für wen gilt DS-GVO?



Auch **Verein** ist „voll und ganz“  
von der neuen Datenschutz-  
Grundverordnung betroffen

... wie auch bisher schon vom Bundesdatenschutzgesetz !!



... und was bedeutet  
das jetzt?

## Wesentliche Anforderungen der DS-GVO

- Anforderungen an die Datenverarbeitung
- Sicherstellung Betroffenenrechte
- Verzeichnis der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten
- Umgang mit Datenschutzverletzungen
- Sanktionen

## Wesentliche Anforderungen der DS-GVO

- **Anforderungen an die Datenverarbeitung**
- Sicherstellung Betroffenenrechte
- Verzeichnis der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten
- Umgang mit Datenschutzverletzungen
- Sanktionen

## Anforderungen an die Datenverarbeitung

- **Rechtmäßigkeit**
- **Transparenz / Informationspflichten**
- **Sicherheit der Verarbeitung**
- **Auftrags(daten)verarbeitung**
- **Rechenschaftspflicht**



## Anforderungen an die Datenverarbeitung

- **Rechtmäßigkeit (Art. 6 ff. DSGVO) bedeutet:**

Im Datenschutzrecht gilt das **Verbot mit Erlaubnisvorbehalt**, d.h. personenbezogene Daten dürfen Sie nur verarbeiten, wenn Sie entweder eine **Rechtsgrundlage** dafür haben (Sozialgesetzbuch, Steuerrecht, Handelsrecht, Vertrag u.a.) oder über eine **Einwilligung** der betroffenen Person verfügen.

Haben Sie das??

## Anforderungen an die Datenverarbeitung

- Rechtmäßigkeit
- **Transparenz / Informationspflichten**
- Sicherheit der Verarbeitung
- Auftrags(daten)verarbeitung
- Rechenschaftspflicht

## Anforderungen an die Datenverarbeitung

### ■ Informationspflichten (Art. 13, 14) beinhalten:

---

- Name (Firmenname) und Kontaktdaten des Verantwortlichen
- Kontaktdaten des Datenschutzbeauftragten (falls vorhanden)
- Zwecke der Datenverarbeitung
- das berechtigte Interesse, sofern die Datenerhebung aufgrund eines berechtigten Interesses erfolgt
- ggf. die Empfänger(kategorien)
- bei Übermittlung in Drittländer: die Arten verwendeter „Garantien“ (z.B. Standarddatenschutzklauseln)
- geplante Speicherdauer
- die Betroffenenrechte (Auskunft, Löschung,...)
- Beschwerderecht bei der Datenschutzaufsichtsbehörde

u.a.

## Anforderungen an die Datenverarbeitung

- **Informationspflichten (Art. 13, 14) beinhalten:**

---

Hier geht es nicht um den Aufbau eines Bürokratiemonsters, sondern um das **berechtigte Interesse der betroffenen Person zu wissen, was mit ihren Daten passiert.**

Je direkter der Kontakt ist, desto geringer sind die Informationspflichten (Bestellung beim Metzger um die Ecke oder Bestellung im Onlineshop).

Betroffene Person soll wissen, wer was mit den Daten macht, um auch noch **nein** sagen zu können.

## Anforderungen an die Datenverarbeitung

- Rechtmäßigkeit
- Transparenz/Informationspflichten
- Sicherheit der Verarbeitung
- Auftrags(daten)verarbeitung
- Rechenschaftspflicht

## Anforderungen an die Datenverarbeitung

### ■ Sicherheit der Verarbeitung (Art. 32)

---

- Sind unter Berücksichtigung des **Standes der Technik** ... geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; ...
  - Pseudonymisierung, Verschlüsselung
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit sicherstellen
  - Verfügbarkeit wieder herstellen
  - **Verfahren zur regelmäßigen Überprüfung**, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

## Anforderungen an die Datenverarbeitung

- Rechtmäßigkeit
- Transparenz / Informationspflichten
- Sicherheit der Verarbeitung
- Auftrags(daten)verarbeitung
- Rechenschaftspflicht

## Anforderungen an die Datenverarbeitung

- **Auftrags(daten)verarbeitung, Art 28**

---

Haben Sie eine Überblick, wen Sie mit welchen Aufgaben betraut haben (Cloud Computing, IT-Wartung, usw.)?



## Anforderungen an die Datenverarbeitung

### ■ Auftrags(daten)verarbeitung, Art 28

---

- Ist die Verarbeitung personenbezogener Daten „outgesourct“?
- Wenn Ja, gibt es dafür ausreichende Verträge zur Auftragsdatenverarbeitung (Muster siehe: [www.lida.bayern.de](http://www.lida.bayern.de))

## Anforderungen an die Datenverarbeitung

- Rechtmäßigkeit
- Transparenz / Informationspflichten
- Sicherheit der Verarbeitung
- Auftrags(daten)verarbeitung
- Rechenschaftspflicht

## Anforderungen an die Datenverarbeitung

### Rechenschaftspflicht

#### Artikel 5: Grundsätze für die Verarbeitung

- (1) Personenbezogene Daten müssen
  - a) ... auf rechtmäßige Weise ... („Rechtmäßigkeit 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.]

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

Wie prüfen wir:

**Zeig mal !!**

(„Beweislastumkehr“)

## Wesentliche Anforderungen der DS-GVO

- Anforderungen an die Datenverarbeitung
- **Sicherstellung Betroffenenrechte**
- Verzeichnis der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten
- Umgang mit Datenschutzverletzungen
- Sanktionen

## Sicherstellung der Betroffenenrechte

### Betroffenenrechte (Auszug)

- **Recht auf Auskunft**
- Recht auf Berichtigung
- Recht auf Löschung
- Recht auf Widerruf einer Einwilligung

## Sicherstellung der Betroffenenrechte

- **Auskunft**
  - nicht automatisch, sondern nur auf Antrag (prüfen, ob Antragsteller der ist, der er vorgibt zu sein)
  - Daten aus allen Einrichtungsteilen müssen zusammengeführt werden
  - Abschrift der Daten (schriftlich oder elektronisch)
  - Auskunft ist kostenlos (jedenfalls beim ersten mal)
  - Auskunft muss konkreten Inhalt bezeichnen (Max Mustermann, Hauptstr. 1, 12345 Hauptstadt), nicht nur Kategorien (Name, Adresse ...)

## Sicherstellung der Betroffenenrechte

Können Sie Auskunft geben, über  
welche personenbezogenen  
Daten von betroffenen Personen  
Sie verfügen?

## Wesentliche Anforderungen der DS-GVO

- Anforderungen an die Datenverarbeitung
- Sicherstellung Betroffenenrechte
- **Verzeichnis der Verarbeitungstätigkeiten**
- Bestellung eines Datenschutzbeauftragten
- Umgang mit Datenschutzverletzungen
- Sanktionen



## Verzeichnis der Verarbeitungstätigkeiten

Verpflichtung zur Erstellung eines VVT besteht für

- jeden Verantwortlichen / Auftragsverarbeiter mit mindestens 250 Mitarbeitern
- auch Verantwortliche / Auftragsverarbeiter mit weniger als 250 Mitarbeitern, sofern Verarbeitungen durchgeführt werden, die
  - ein Risiko für Rechte & Freiheiten Betroffener bergen (z.B. Videoüberwachung, Scoring, Betrugsprävention)
  - **oder** nicht nur gelegentlich erfolgen (z.B. regelmäßige Verarbeitung von Kunden- und/oder Beschäftigtendaten)
  - **oder** besondere Datenkategorien gem. Art. 9 Abs. 1 oder Daten über strafrechtliche Verurteilungen / Straftaten betreffen

**Fazit: Die meisten Vereine müssen ein VVT erstellen**, da meistens regelmäßig Kunden- und/oder Beschäftigtendaten verarbeitet werden.

## Verzeichnis der Verarbeitungstätigkeiten

Haben Sie einen Überblick  
darüber, welche  
personenbezogenen Daten in  
Ihrem Verein „verarbeitet“  
werden ??

## Wesentliche Herausforderungen durch die DS-GVO

- Anforderungen an die Datenverarbeitung
- Sicherstellung Betroffenenrechte
- Verzeichnis der Verarbeitungstätigkeiten
- **Bestellung eines Datenschutzbeauftragten**
- Umgang mit Datenschutzverletzungen
- Sanktionen

## Bestellung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter ist zu benennen, wenn

- **Verarbeitung von einer Behörde durchgeführt wird** (d.h. jede Behörde muss immer einen DSB bestellen, Art, 37 Abs. 1 a DSGVO),
- **in der Regel mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind** (§ 38 Abs. 1 Satz 1 BDSG-neu) oder
- Daten verarbeiten, die wegen eines hohen Risikos für die betroffenen Personen eine Datenschutz-Folgenabschätzung erfordern (§ 38 Abs. 1 Satz 2 BDSG-neu – absolute Ausnahme).

## Wesentliche Herausforderungen durch die DS-GVO

- Anforderungen an die Datenverarbeitung
- Sicherstellung Betroffenenrechte
- Verzeichnis der Verarbeitungstätigkeiten
- Bestellung eines Datenschutzbeauftragten
- **Umgang mit Datenschutzverletzungen**
- Sanktionen

## Umgang mit Datenschutzverletzungen

### **„Verletzung des Schutzes personenbezogener Daten“**

ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

# Umgang mit Datenschutzverletzungen

**Beispiele für  
Meldepflicht**



**72 Stunden**

---

**Hacking**

---

**Verlust**

---

**Diebstahl**

---

**Fehlversand**

---

**Softwarefehler**

---

**Schadcode**

---

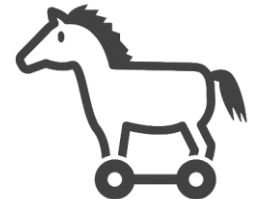
**Fehlentsorgung**

---

**Vernichtung Verlust**

---

**Sonstiges?**



## Umgang mit Datenschutzverletzungen

Sind Sie in der Lage zu erkennen,  
wenn bei Ihnen eine  
Datenschutzverletzung  
eingetreten ist, und ist geklärt,  
wer sich darum kümmert?



## Wesentliche Anforderungen der DS-GVO

- Anforderungen an die Datenverarbeitung
- Sicherstellung Betroffenenrechte
- Verzeichnis der Verarbeitungstätigkeiten
- Umgang mit Datenschutzverletzungen
- **Sanktionen**



... und wenn es  
daneben geht?

# Sanktionen **morgen**

## Art. 83 DS-GVO



bis **10.000.000** EUR oder 2 % Weltjahresumsatz  
(„formelle Verstöße“)

bis **20.000.000** EUR oder 4 % Weltjahresumsatz  
(„materielle Verstöße“)

- *Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen ... in jedem Einzelfall **wirksam, verhältnismäßig und abschreckend** ist. (Art. 83 Abs. 1 DS-GVO)*

# Agenda

- 1 Datenschutz – was ist das?
- 2 Datenschutz – was kommt mit der DS-GVO auf uns zu?
- 3 **Umgang mit Bildern**
- 4 Rolle und Aufgabe der Datenschutzaufsicht
- 5 Empfehlung zum Schluss

## Umgang mit Bildern

### Grundsatz:

Erforderlich ist die Erlaubnis des Fotografen bzw. Urhebers, sein Bild verwenden und veröffentlichen zu dürfen

**und**

bei Fotos oder Filmen von Personen die grundsätzlich Erlaubnis der abgebildeten Person.

# Umgang mit Bildern

## Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie

KunstUrhG – KUG vom 9. Januar 1907 (kein Schreibfehler !!)

### § 22 KUG

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. Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige im Sinne dieses Gesetzes sind der überlebende Ehegatte oder Lebenspartner und die Kinder des Abgebildeten und, wenn weder ein Ehegatte oder Lebenspartner noch Kinder vorhanden sind, die Eltern des Abgebildeten.

# Umgang mit Bildern

- **Einwilligung:** konkludente Einwilligung reicht
- **verbreitet oder öffentlich zur Schau stellen** = Weitergabe des Originals oder von Kopien, die das Risiko einer nicht mehr zu kontrollierenden Kenntnisnahme in sich birgt, egal, ob in Zeitschrift, Buch, Postkarte, Foto oder Film; Möglichkeit der Kenntnisnahme reicht; Aushang im Schaukasten oder Museum reicht;
- Die **Einwilligung gilt im Zweifel als erteilt**, wenn der Abgebildete dafür, dass er sich abbilden ließ, eine Entlohnung erhielt.
- Nach dem Tode des Abgebildeten bedarf es bis zum Ablaufe von 10 Jahren der Einwilligung der Angehörigen des Abgebildeten. Angehörige sind ...

# Umgang mit Bildern

## § 23 KUG

- (1) **Ohne** die nach § 22 erforderliche **Einwilligung** dürfen verbreitet und zur Schau gestellt werden:
1. Bildnisse aus dem Bereiche der **Zeitgeschichte**;
  2. Bilder, auf denen die Personen nur als **Beiwerk** neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;
  3. Bilder von **Versammlungen, Aufzügen und ähnlichen Vorgängen**, an denen die dargestellten Personen teilgenommen haben;
  4. Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem **höheren Interesse der Kunst** dient.
- (2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schau-  
stellung, durch die ein **berechtigtes Interesse des Abgebildeten** oder, falls  
dieser verstorben ist, seiner Angehörigen verletzt wird.



# Handlungsempfehlungen: Einwilligung einholen



## TIPP

Folgender Ratschlag völlig unjuristischer Art hat in der Praxis schon viel Ärger verhindert: Wenn Ihnen Ihr Bauchgefühl sagt, dass etwas nicht gut ist, ist es meistens auch nicht gut! Oder anders gesagt: 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.



Bayerisches Landesamt für  
Datenschutzaufsicht



**Info-Kompakt**

**Fotos im Internet**

Stand: Januar 2016

Ich möchte Fotos, auf denen Personen zu sehen sind, auf einer Homepage veröffentlichen. Unternehmen und Vereine haben ein legitimes Interesse daran, ihren Internetauftritt möglichst ansprechend und lebendig zu gestalten. Daher liegt es nahe, die eigene Darstellung im Internet mit Bildern vom Tag der offenen Tür, dem Vereinsausflug usw. zu ergänzen. Die gesetzlichen Rahmenbedingungen für eine Veröffentlichung von Fotos im Internet finden sich in den Rechtsvorschriften des Kunsturheberrechtsgesetzes (KUG), das als speziellere Regelung den Vorschriften des Bundesdatenschutzgesetzes vorgeht.

**Was genau sehen die Regelungen des Kunsturheberrechtsgesetzes (KUG) vor?**

Das KUG sieht vor, dass das Veröffentlichung von Fotos im offenen Internet, auf denen Personen abgebildet sind, grundsätzlich deren Einwilligung bedarf. Ausnahmen von diesem Grundsatz, d. h. eine zulässige Veröffentlichung ohne Einwilligung der abgebildeten Person, sieht das Gesetz beispielsweise dann vor, wenn die Personen „nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen“ oder es sich um Fotos von „Versammlungen, Aufzügen und ähnlichen Vorgängen“ handelt. Stehen bei Fotos daher nicht einzelne Personen im Vordergrund, sondern soll lediglich ein Eindruck vom Tag der offenen Tür oder der Vereinsfeier vermittelt werden, kann eine Veröffentlichung von Fotos auch ohne Einwilligung der betroffenen Personen zulässig sein.

**Ich bin mir unsicher, ob ich die Einwilligung brauche**

Nicht umsonst mussten bereits zahlreiche Einzelfälle zu dieser Thematik vor Zivilgerichten entschieden werden, da subjektiv unterschiedliche Sichtweisen existieren, ob und wann eine abgebildete Person als „Beiwerk“ auf einem Foto erscheint oder das Foto wirklich den Charakter einer Veranstaltung wiedergibt und nicht einzelne Personen im Fokus stehen. Eine Empfehlung kann daher nur lauten, im Zweifelsfall eine Einwilligung der abgebildeten Person einzuholen oder von einer Veröffentlichung des Fotos abzusehen.

**Wie muss eine Einwilligung eingeholt werden?**

Eine besondere Form für die Einwilligung sieht das KUG nicht vor, so dass sich die Einwilligung einer Person auch aus deren konkludentem Verhalten ergeben kann. Dafür genügt es allerdings nicht, wenn sich die Person „einfach fotografieren lässt“ oder sogar dafür „posiert“. Sie muss dies vor allem auch in dem Bewusstsein tun, dass das Foto ins Internet gestellt wird.

Herausgeber:  
Bayerisches Landesamt für Datenschutzaufsicht  
Promenade 27 (Schloss)  
91522 Andechs

Tel.: 0981/53-1300 | Fax: 0981/53-5300  
poststelle@lda.bayern.de  
www.lda.bayern.de



**f) Muster einer Einwilligungserklärung**

Muster 5: Einwilligung mit genauer Beschreibung des Verwendungszwecks (Veröffentlichung von Fotos im Intranet/Internet)

**Einwilligung zu Fotoaufnahmen**

Das/der .....  
(genaue Bezeichnung des Unternehmens)

beabsichtigt, im Rahmen von .....  
(Benennung der Veranstaltung, z. B. „bei der Weihnachtsfeier/beim Tag der offenen Tür/beim Firmenjubiläum)

Fotos anfertigen zu lassen.  
Diese Fotos sollen an folgender Stelle im Internet/Intranet veröffentlicht werden:

.....  
(Benennung der Adresse der Homepage, auf der die Veröffentlichung erfolgt)

Die Veröffentlichung soll auf unbestimmte Zeit erfolgen.  
Es wird darauf hingewiesen, dass Fotos im Internet von beliebigen Personen abgerufen werden können. Es kann nicht ausgeschlossen werden, dass solche Personen die Fotos weiterverwenden oder an andere Personen weitergeben.

- Diese Einwilligungserklärung gilt ab dem Datum der Unterschrift (Zutreffendes bitte ankreuzen)
- bis zu dem Zeitpunkt, zu dem das Arbeitsverhältnis endet. Nach Beendigung des Arbeitsverhältnisses werden die Fotos, auf denen der Arbeitnehmer zu erkennen ist, gelöscht.
  - und auch über die Beendigung des Arbeitsverhältnisses hinaus. Der Arbeitnehmer kann die Einwilligung nach Beendigung des Arbeitsverhältnisses nur dann widerrufen, wenn er nachweist, dass dies erforderlich ist, um seine berechtigten Interessen zu schützen.

.....  
Datum, Ort und Unterschrift des Arbeitnehmers



... wer kümmert sich  
darum und wer  
kontrolliert?

## Wer ist verantwortlich und wer kontrolliert die Einhaltung der DS-GV?

### Art. 4 Nr. 7: Begriffsbestimmungen

„**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; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

**Wer ist verantwortlich** und wer kontrolliert die Einhaltung der DS-GV?

## Art. 4 Nr. 7: Begriffsbestimmungen

„**Verantwortlicher**“

ist der (im Vereinsregister eingetragene)  
Vorstand

**Wer ist verantwortlich** und wer kontrolliert die Einhaltung der DS-GV?

## Datenschutzbeauftragte/r

... dient der internen Kontrolle. Er/Sie ist nicht dafür verantwortlich, was in Unternehmen bzw. Verein mit den Daten passiert.

**„Verantwortlicher“**

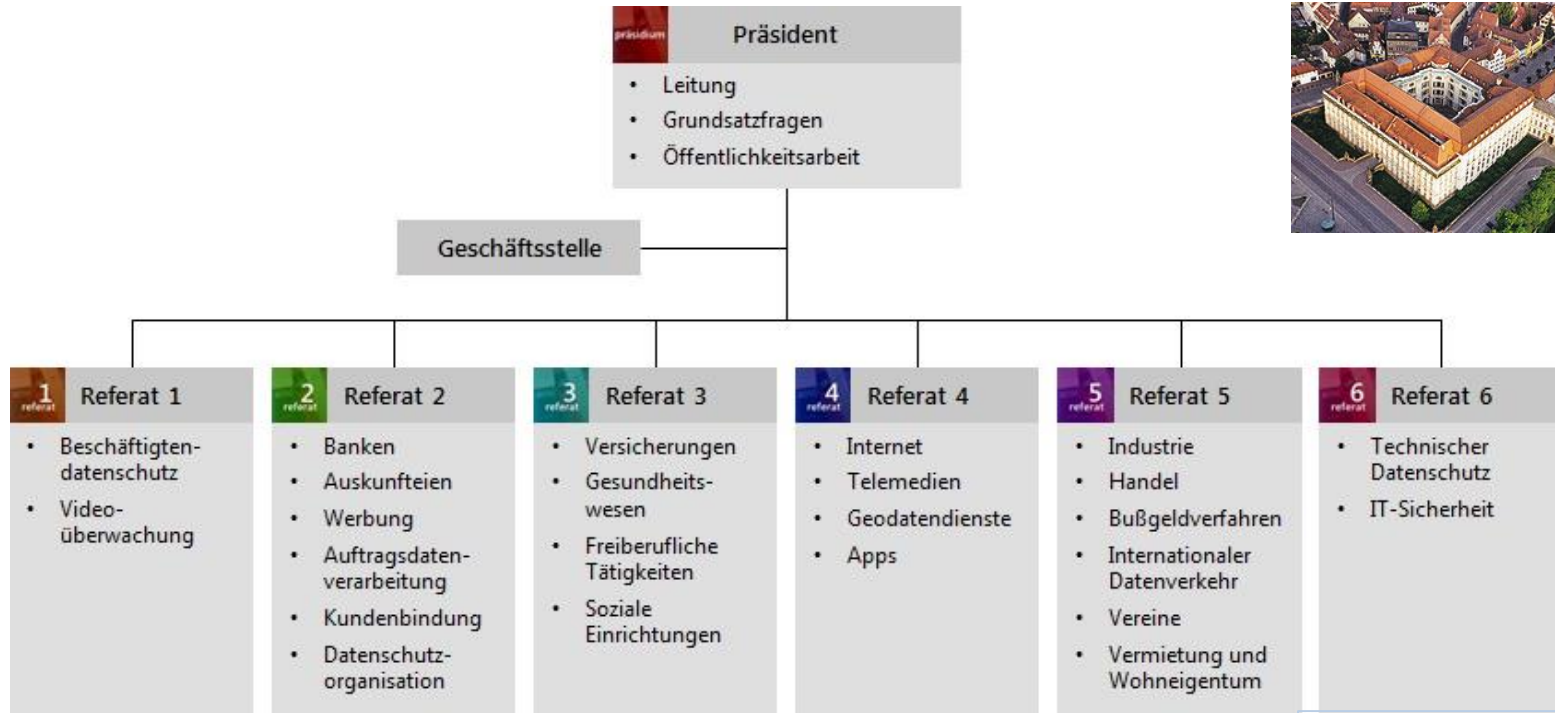
ist der (im Vereinsregister eingetragene) Vorstand. Er ist und bleibt verantwortlich.

# Agenda

- 1 Datenschutz – was ist das?
- 2 Datenschutz – was kommt mit der DS-GVO auf uns zu?
- 3 Umgang mit Bildern
- 4 **Rolle und Aufgabe der Datenschutzaufsicht**
- 5 Empfehlung zum Schluss



# Bayerisches Landesamt für Datenschutzaufsicht



Der Freistaat  
Bayern hat

**12,7 Mio.**  
Einwohner



**20/24 Planstellen**

Der Freistaat  
Bayern hat

**ca. 700.000**  
Unternehmen

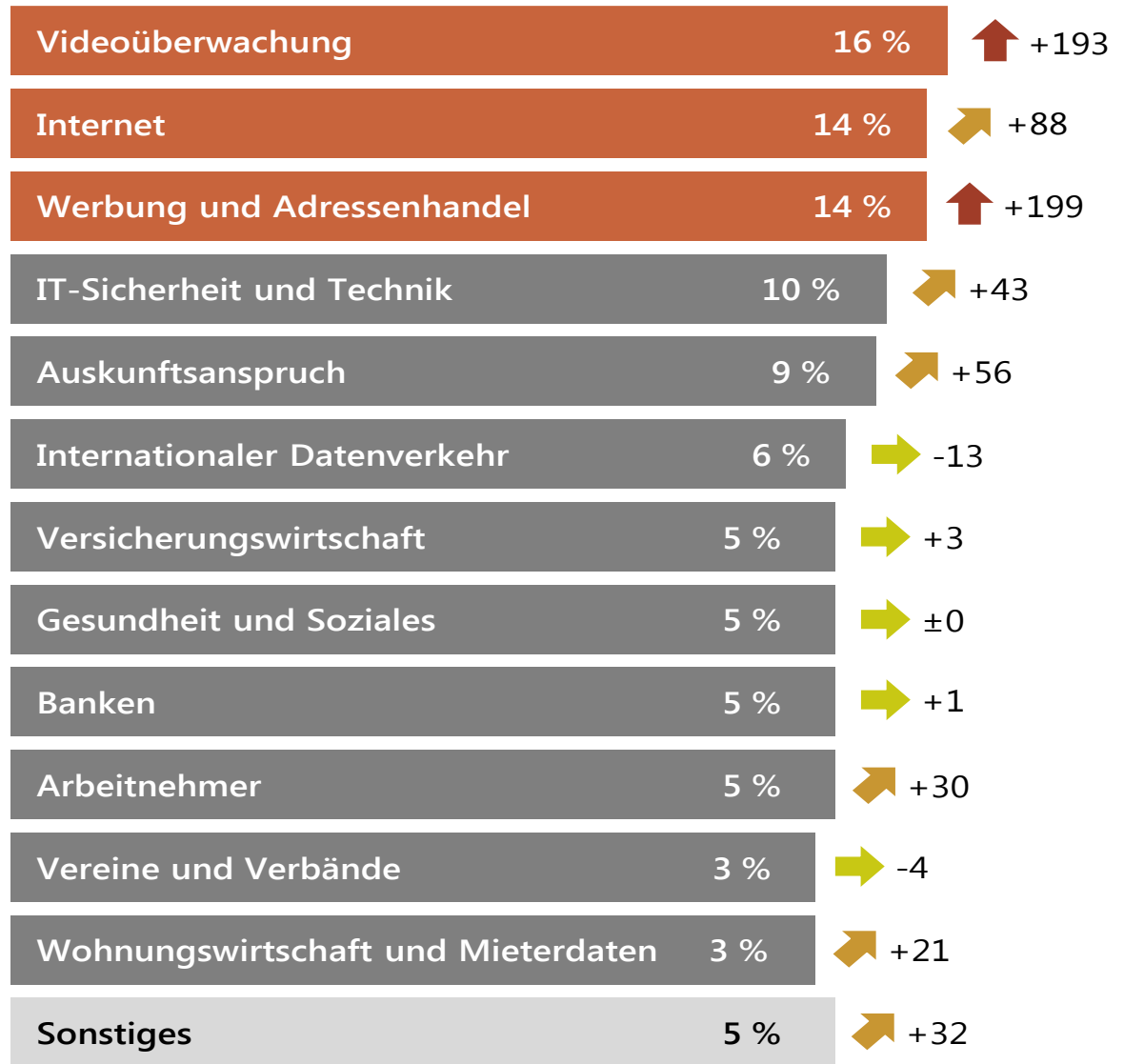


# Rolle und Aufgabe der Datenschutzaufsicht

	2013	2014	2015	2016	Tendenz
Beschwerden	925	953	1103	1424	↑
Beratungen Bürger	799	991	877	1065	↔
Beratungen Unternehmen	1733	1821	1850	2003	↑
Bußgeldverfahren	53	64	94	79	↔
Datenpannen	32	21	28	85	↑



**Beschwerden**





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



Dienstgebäude des BayLDA in Ansbach

 Startseite



## Willkommen beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Wir haben auf unserem Webauftritt zahlreiche Informationen zum Thema Datenschutz in Deutsch und Englisch zusammengestellt. Sie sind herzlich dazu eingeladen, unsere Artikel und Veröffentlichungen in Ruhe zu lesen und sich bei Fragen an uns zu wenden.

### Pressemitteilungen

Ansbach, 28.03.2018

#### DSK veröffentlicht weiteres Kurzpapier

Die Datenschutzkonferenz(DSK) hat das Kurzpapier "Besondere Kategorien personenbezogener Daten" veröffentlicht.

[→ Mehr erfahren](#)

### Pressemitteilungen

Ansbach, 20.03.2018

#### DSK veröffentlicht weiteres Kurzpapier

Die Datenschutzkonferenz(DSK) hat das Kurzpapier "Gemeinsam für die Verarbeitung Verantwortliche" veröffentlicht.

[→ Mehr erfahren](#)

### EU-Datenschutz-Grundverordnung

Ansbach, 22.03.2018

#### 12 Muster für kleine Unternehmen und Vereine veröffentlicht

Das BayLDA hat neue Handreichungen bezüglich der neuen Datenschutzanforderungen für kleinere Unternehmen veröffentlicht.

[→ Mehr erfahren](#)

[→ Zur Pressemitteilung](#)

### Pressemitteilungen

Ansbach, 16.03.2018

#### BayLDA beim Daten-Dienstag am 20.03.2018 in Nürnberg

Im Museum für Kommunikation in Nürnberg informiert das BayLDA über die Chancen und Risiken der Nutzung des Internets.

[→ Zur Pressemitteilung](#)

# Wesentliche Anforderungen für den Einzelhändler

## EU-Datenschutz-Grundverordnung

Ansbach, 22.03.2018

### 12 Muster für kleine Unternehmen und Vereine veröffentlicht

Das BayLDA hat neue Handreichungen bezüglich der neuen Datenschutz-Anforderungen für kleinere Unternehmen veröffentlicht.

→ Mehr erfahren

→ Zur Pressemitteilung



# Wesentliche Anforderungen für einen Verein

## Unsere Handreichungen



... geht doch !!

The screenshot shows the BayLDA website interface. At the top, there is a navigation bar with links for 'AKTUELLES', 'UNSERE BEHÖRDE', 'RECHTLICHES', 'INFOTHEK', 'PRESSE', and 'ONLINE-SERVICES'. Below this is a search bar and a main banner image with various icons representing business and technology. The main content area is titled 'Handreichungen für kleine Unternehmen und Vereine' and contains a list of links for 'Anforderungen für Vereine', 'Musterverzeichnis der Verarbeitungstätigkeiten für Vereine', 'Kfz-Werkstatt', and 'Musterverzeichnis der Verarbeitungstätigkeiten für Werkstätten'.

The document is titled 'Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.' and is labeled 'Muster 1: Verein'. It is published by the 'Bayerisches Landesamt für Datenschutzaufsicht'. The document includes a 'Hinweis' section, a 'Kurzbeschreibung des Vereins' section, and a checklist of 'Wesentliche DS-GVO-Anforderungen für den Verein'. The checklist items are as follows:

- A** Datenschutzbeauftragter (DSB)
  - Muss ein DSB vom Verein benannt werden?
    - ja
    - nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)
- B** Verzeichnis von Verarbeitungstätigkeiten
  - Ist ein solches Verzeichnis erforderlich?
    - ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
    - nein
- C** Datenschutz-Vereinbarung von Beschäftigten
  - Ist eine solche Vereinbarung durchzuführen?
    - ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
    - nein
- D** Information- und Auskunftspflichten
  - Bestehen irgendwelche Informationspflichten?
    - ja (insb. in der Vereinssatzung sowie auf der Webseite in der Datenschutzerklärung)
    - nein
- E** Löschen von Daten
  - Gibt es eine Anforderung zur Datenlöschung?
    - ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
    - nein
- F** Sicherheit
  - Müssen die Daten besonders gesichert werden?
    - ja
    - nein (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)
- G** Auftragsverarbeitung
  - Ist ein Vertrag zur Auftragsverarbeitung notwendig?
    - ja (sowohl mit dem Hosting-Anbieter als auch mit dem externen Lohnabrechner)
    - nein
- H** Datenschutzverletzungen
  - Müssen bestimmte Vorfälle gemeldet werden?
    - ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
    - nein
- I** Datenschutz-Folgeabschätzung (DSFA)
  - Muss eine DSFA vom Verein durchgeführt werden?
    - ja
    - nein (da kein hohes Risiko bei der Datenverarbeitung im Verein besteht)
- J** Videoüberwachung (VÜ)
  - Besteht eine Ausschuldungspflicht bezüglich VÜ?
    - ja
    - nein (da keine Videoüberwachung im Verein durchgeführt wird)

# Wesentliche Anforderungen für einen Verein

## ☑ Wesentliche DS-GVO-Anforderungen für den Verein

### A Datenschutzbeauftragter (DSB)

Muss ein DSB vom Verein benannt werden?

- ja  
 nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

### B Verzeichnis von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

- ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)  
 nein

### C Datenschutz-Verpflichtung von Beschäftigten

Ist eine solche Verpflichtung durchzuführen?

- ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)  
 nein

### D Information- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

- ja (insb. in der Vereinssatzung sowie auf der Webseite in der Datenschutzerklärung)  
 nein

### E Löschen von Daten

Gibt es eine Anforderung zur Datenlöschung?

- ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)  
 nein

### F Sicherheit

Müssen die Daten besonders gesichert werden?

- ja  
 nein (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)

### G Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

- ja (sowohl mit dem Hosting-Anbieter als auch mit dem externen Lohnabrechner)  
 nein

### H Datenschutzverletzungen

Müssen bestimmte Vorfälle gemeldet werden?

- ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)  
 nein

### I Datenschutz-Folgeabschätzung (DSFA)

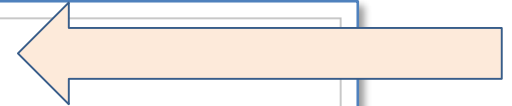
Muss eine DSFA vom Verein durchgeführt werden?

- ja  
 nein (da kein hohes Risiko bei der Datenverarbeitung im Verein besteht)

### J Videoüberwachung (VÜ)

Besteht eine Ausschilderungspflicht bezüglich VÜ?

- ja  
 nein (da keine Videoüberwachung im Verein durchgeführt wird)






# Wesentliche Anforderungen für einen Verein

## Unsere Handreichungen



... geht doch !!

Rückseite

Bayerisches Landesamt für  
Datenschutzaufsicht 

**① Erläuterungen zu den Anforderungen**

**A** **Datenschutzbeauftragter (DSB)**  
In aller Regel ist nur dann ein DSB zu benennen, wenn mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. „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.  
→ DSK-Kurzpapier Nr. 12: [www.lida.boymern.de/media/dsk\\_kprnr\\_12\\_datenschutzbeauftragter.pdf](http://www.lida.boymern.de/media/dsk_kprnr_12_datenschutzbeauftragter.pdf)

**B** **Verzeichnis von Verarbeitungstätigkeiten**  
Vereine, die regelmäßige Mitgliederverwaltung und Beitragsabrechnung machen, müssen ein – vom Umfang her sehr überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.  
→ BayLDA Muster-Verzeichnis für kleine Vereine: [www.lida.boymern.de/media/muster\\_1\\_veerein\\_verzeichnis.pdf](http://www.lida.boymern.de/media/muster_1_veerein_verzeichnis.pdf)  
→ DSK-Kurzpapier Nr. 1: [www.lida.boymern.de/media/dsk\\_kprnr\\_1\\_verzeichnis\\_verarbeitungstatigkeiten.pdf](http://www.lida.boymern.de/media/dsk_kprnr_1_verzeichnis_verarbeitungstatigkeiten.pdf)  
→ DSK-Muster-Verzeichnis allgemein: [www.lida.boymern.de/media/dsk\\_muster\\_vov\\_verantwortlicher.pdf](http://www.lida.boymern.de/media/dsk_muster_vov_verantwortlicher.pdf)

**C** **Datenschutz-Vereinbarung mit Beschäftigten**  
Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.  
→ BayLDA Info-Blatt zur Verpflichtung: [www.lida.boymern.de/media/info\\_verpflichtung\\_beschaeftigte\\_ds-gvo.pdf](http://www.lida.boymern.de/media/info_verpflichtung_beschaeftigte_ds-gvo.pdf)

**D** **Informations- und Auskunftspflichten**  
Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Ein Verein muss bspw. Informationen auf der Homepage und der Satzung leicht zugänglich bereithalten. Die betroffenen Personen (z. B. Vereinsmitglieder) haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.  
→ DSK-Kurzpapier Nr. 6: [www.lida.boymern.de/media/dsk\\_kprnr\\_6\\_auskunftsrecht.pdf](http://www.lida.boymern.de/media/dsk_kprnr_6_auskunftsrecht.pdf)  
→ DSK-Kurzpapier Nr. 10: [www.lida.boymern.de/media/dsk\\_kprnr\\_10\\_informationspflichten.pdf](http://www.lida.boymern.de/media/dsk_kprnr_10_informationspflichten.pdf)

**E** **Löschen von Daten**  
Sobald keine gesetzliche Grundlage (z. B. steuerliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. In der Regel ist dies bspw. erst der Fall nach Ausscheiden eines Vereinsmitglieds.  
→ DSK-Kurzpapier Nr. 11: [www.lida.boymern.de/media/dsk\\_kprnr\\_11\\_vergessenwerden.pdf](http://www.lida.boymern.de/media/dsk_kprnr_11_vergessenwerden.pdf)

**F** **Sicherheit**  
Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virens Scanner und Benutzerrechte. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können.  
→ BayLDA-Kurzpapier Nr. 1: [www.lida.boymern.de/media/baylda\\_ds-gvo\\_1\\_security.pdf](http://www.lida.boymern.de/media/baylda_ds-gvo_1_security.pdf)

**G** **Auftragsverarbeitung**  
Sobald Verantwortliche Dienstleistungen (z. B. Buchhaltung) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.  
→ DSK-Kurzpapier Nr. 13: [www.lida.boymern.de/media/dsk\\_kprnr\\_13\\_auftragsverarbeitung.pdf](http://www.lida.boymern.de/media/dsk_kprnr_13_auftragsverarbeitung.pdf)  
→ BayLDA-Formulierungshilfe zum Vertrag: [www.lida.boymern.de/media/muster\\_adv.pdf](http://www.lida.boymern.de/media/muster_adv.pdf)

**H** **Datenschutzverletzungen**  
Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Vereinsdaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.  
→ BayLDA-Kurzpapier Nr. 8: [www.lida.boymern.de/media/baylda\\_ds-gvo\\_8\\_data\\_breach\\_notification.pdf](http://www.lida.boymern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf)  
→ BayLDA-Online-Service zur Meldung: [www.lida.boymern.de/de/datenpanne.html](http://www.lida.boymern.de/de/datenpanne.html)

**I** **Datenschutz-Folgeabschätzung (DSFA)**  
Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgeabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.  
→ DSK-Kurzpapier Nr. 5: [www.lida.boymern.de/media/dsk\\_kprnr\\_5\\_dafa.pdf](http://www.lida.boymern.de/media/dsk_kprnr_5_dafa.pdf)

**J** **Videoüberwachung**  
Führt ein Verantwortlicher eine Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoaufnahmen zu informieren.  
→ DSK-Kurzpapier Nr. 15: [www.lida.boymern.de/media/dsk\\_kprnr\\_15\\_videoueberwachung.pdf](http://www.lida.boymern.de/media/dsk_kprnr_15_videoueberwachung.pdf)





# Wesentliche Anforderungen für einen Verein

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

Bayerisches Landesamt für  
Datenschutzaufsicht



## Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

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

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

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

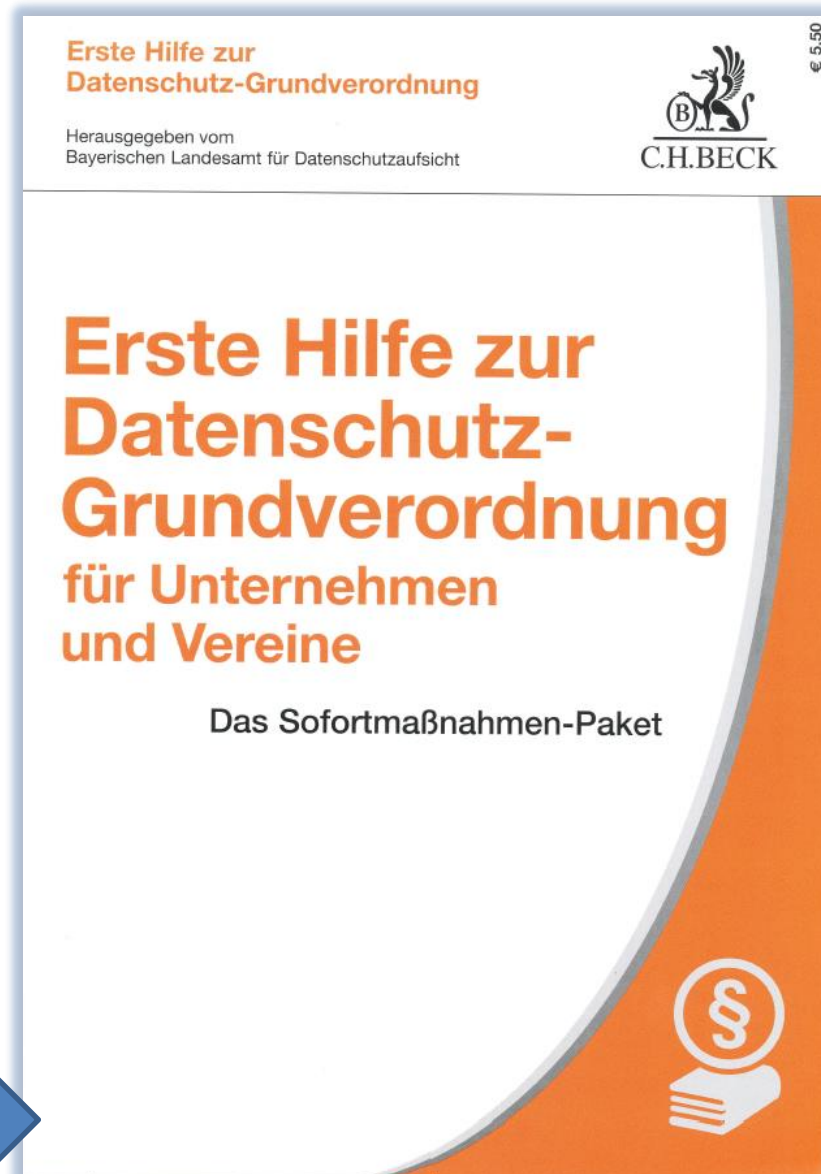
Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer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

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

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

# Agenda

- 1 Datenschutz – was ist das?
- 2 Datenschutz – was kommt mit der DS-GVO auf uns zu?
- 3 Umgang mit Bildern
- 4 Rolle und Aufgabe der Datenschutzaufsicht
- 5 **Empfehlung zum Schluss**



**Ehmann / Kranig**

**Erste Hilfe zur  
Datenschutz-  
Grundverordnung**


**Zielgruppe:**

Inhaber kleinerer Unternehmen;  
Vereinsvorsitzende; Datenschutz-  
verantwortliche in kleineren  
Unternehmen und in Vereinen;  
datenschutzinteressierte  
Vereinsmitglieder.

# Empfehlung aus Sicht der Datenschutzaufsicht

BAYERISCHES LANDESAMT FÜR  
DATENSCHUTZAUFICHT



- **Datenschutz ist Chefsache** (sowohl beim Vorbeugen und Entscheiden als auch bei Sanktionen)
- **Datenschutz geht alle an** (und geht nur, wenn alle mitmachen)
- **Datenschutz gilt von Anfang an** („privacy by design“ – beziehen Sie den Datenschutz immer mit ein)
- **Schaffen Sie sich einen Überblick über Ihre aktuelle Situation** (Erstellen Sie ganz schnell Ihr Verarbeitungsverzeichnis nach Art. 30 DS-GVO, wenn Sie es nicht schon haben)
- **Sprechen Sie mit Ihrer Aufsichtsbehörde** (sie kann [muss] Sie beraten – und schafft Ihnen Rechtssicherheit)
- **Haben Sie einen Plan**  **... sonst werden Sie verplant.**



Dienstgebäude des BayLDA in Ansbach

## Willkommen beim Bayerischen Landesamt für Datenschutzaufsicht (BayLDA)

Wir haben auf unserem Webauftritt zahlreiche Informationen zum Thema Datenschutz in Deutsch und Englisch zusammengestellt. Sie sind herzlich dazu eingeladen, unsere Artikel und Veröffentlichungen in Ruhe zu lesen und sich bei Fragen an uns zu wenden.

# Vielen Dank für Ihre Aufmerksamkeit

Thomas Kranig, Bayer. Landesamt für Datenschutzaufsicht

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



ITIL  
IT-GRUNDSCHUTZ  
ISO 27001  
SPIONAGE  
FACEBOOK  
CLOUD  
RSA  
EXPLOIT  
STARTTLS  
BEDROHUNGSLAGE  
XSS  
BYOD  
AES-256  
SCHWACHSTELLE  
SQL INJECTION  
AWARENESS  
ANDROID  
FIREWALL  
FORWARD SECRECY  
PHISHING  
IPV6  
ZERO-DAY EXPLOIT  
AUTHENTIFIZIERUNG  
BDSG  
HTTPS  
CSRF  
DDOS  
PGP  
BSI  
DIEBSTAHL  
CRIME  
ENISA  
BEAST  
TOMS  
ROOTKIT  
AKTENVERNICHTUNG  
MD5  
DARKNET  
JAVA  
S/MIME  
WINDOWS XP  
AUTORISIERUNG  
PDKDF2  
MIMM

NOTFALLKONZEPT  
TLS 1.2  
BSI GRUNDSCHUTZ  
HACKER  
PRISM  
WAF  
TROJANER  
BOTNETZ  
VPN  
DATENSCHUTZ  
BACKDOOR  
SPOOFING  
MITM  
HYDRA  
MDM  
SPAM  
QUANTENCOMPUTER

BCRYPT  
METASPLOIT  
W3AF  
IOS  
IPV4  
DLP  
HACKTIVISMUS  
DMZ  
APT  
IDS  
NSA  
FIPS  
IPS  
OSCP  
EV-ZERTIFIKAT  
CYBERSÖLDNER  
APPS  
GOOGLE  
WATERHOLE ATTACK  
NMAP

W3AF  
IOS  
IPV4  
DLP  
HACKER  
PRISM  
WAF  
TROJANER  
BOTNETZ  
VPN  
DATENSCHUTZ  
BACKDOOR  
SPOOFING  
MITM  
HYDRA  
MDM  
SPAM  
QUANTENCOMPUTER