

# Herbstvollversammlung des KJR Neumarkt – Handout zum Thema DS-GVO

---

Neumarkt, 22. November 2018



## Zur Person

- 48 Jahre
- Rechtsanwalt (seit 1998)
- Zertifizierter Datenschutzbeauftragter DSB-TÜV
- Zertifizierter Datenschutzauditor DSA-TÜV
- Zertifizierter Informationssicherheitsbeauftragter (BVS)
- Behördlicher und Externer Datenschutzbeauftragter
- Lehrbeauftragter der Hochschule Ansbach
- Technisches Webdesign
- 3. Bürgermeister a.D., Stadt- und Kreirat a.D.
- 13 Jahre Vorsitzender eines kleinen Sportvereins





# Hilfreiche Webseiten



The screenshot shows the homepage of the Bayerisches Landesamt für Datenschutzaufsicht (BayLDA). The header is blue with a navigation menu: BayLDA, Aktuelles, Online-Services, Themen, Veröffentlichungen, and Unsere Behörde. A search bar is on the right. Below the header, there's a section titled 'Hotline' with a paragraph explaining the service. A large light blue box contains the 'Hotline für Vereine und ehrenamtlich Tätige in Bayern' information, including the phone number 0981-53-1810 and service hours. At the bottom of this box are two buttons: 'Pressemitteilung des BayLDA' and 'Pressemitteilung des StMI'.

Bayerisches Landesamt für  
Datenschutzaufsicht

BayLDA Aktuelles Online-Services Themen Veröffentlichungen Unsere Behörde

Suche...

Home > Hotline

## Hotline

Mit einer neu eingerichteten Telefonhotline unterstützt das BayLDA Vereine und Ehrenamtliche in Bayern bei der Umsetzung des neuen europäischen Datenschutzrechts. Ab 9. Juli 2018 können unter einer bestimmten Telefonnummer Fragen rund um die DS-GVO an geschultes Personal adressiert werden. Die Fragen sollen rasch und unkompliziert beantwortet werden. In regelmäßigen Abständen veröffentlichen wir unter der Rubrik "Häufig gefragt" die meistgestellten Fragen mit den dazugehörigen Antworten.

### Hotline für Vereine und ehrenamtlich Tätige in Bayern

**Telefonnummer: 0981-53-1810**  
Servicezeit von Montag bis Freitag von 08:00 Uhr bis 19:00 Uhr

Für den Fall, dass einzelne Fragen nicht durch die Hotline oder unser Informationsangebot auf der Website gelöst werden können, steht ein zusätzlicher E-Mail-Kontakt für bayerische Vereine und Ehrenamtliche bereit: [vereine@lda.bayern.de](mailto:vereine@lda.bayern.de). Wir bitten jedoch darum, primär die eigens eingerichtete Telefonhotline für Fragestellungen zu nutzen.

Pressemitteilung des BayLDA

Pressemitteilung des StMI

3/50

Quelle: <https://www.lda.bayern.de/de/hotline.html>



# Hilfreiche Webseiten

## Häufig gefragt - FAQ für Vereine

Im Folgenden beantwortet das BayLDA 10 Fragen zur Umsetzung der DS-GVO bei Vereinen und Ehrenamtlichen, die in der letzten Woche der unter der Nummer 0981-531810 erreichbaren [Hotline](#) des BayLDA am häufigsten gestellt wurden.

- #1 Ist es erforderlich, von allen (aktiven und passiven) Vereinsmitgliedern eine schriftliche Einwilligungserklärung zur Datenverarbeitung einzuholen?
- #2 Müssen Informationen zum Datenschutz dem Aufnahmeantrag beigelegt werden oder reicht ein Hinweis auf die Veröffentlichung auf der Homepage bzw. Auslage im Vereinsheim?
- #3 Muss mein Verein einen Datenschutzbeauftragten benennen?
- #4 Brauche ich als Verein ein "Verzeichnis der Verarbeitungstätigkeiten"?
- #5 Darf mein Verein noch Mannschaftsfotos auf der eigenen Vereinshomepage veröffentlichen?
- #6 kann es sein, dass auf einer Webseite zwei Datenschutzerklärungen stehen?
- #7 Welche Maßnahmen der Datensicherheit sind zwingend erforderlich?
- #8 Dürfen unsere Spieler untereinander mit einem Messenger-Dienst kommunizieren?
- #9 Darf mein Verein Bilder von Spielszenen eines Fußballspiels ohne weitere Voraussetzungen veröffentlichen?
- #10 Darf mein Verein noch Vereinsinformationen per E-Mail an die Mitglieder versenden?



4/50

Quelle: <https://www.lida.bayern.de/de/faq.html>



# Hilfreiche Webseiten



## DSGVO für Vereine: Fragen und Antworten

Schritt für Schritt zum neuen Datenschutz: Praxisnah, einfach und leicht verständlich geben wir Ihnen als Vereinsmitglied die wichtigsten Antworten rund um die DSGVO.

Überfordern Sie Ihren Vorstand nicht, was Sie zur DSGVO als Vereinsmitglied wissen müssen.


Quelle: <https://www.dsgvo-verstehen-bayern.de/vereine/>







# Hilfreiche Webseiten



Bayerisches Landesamt für  
Datenschutzaufsicht



BayLDA   Aktuelles ▾   Online-Services ▾   Themen ▾   Veröffentlichungen ▾   Unsere Behörde ▾

Suche... 

 > Veröffentlichungen > Infoblätter & Flyer

## Informationsmaterialien

### Einleitende Worte

Das BayLDA hält auf dieser Seite verschiedene Informationsmaterialien zum Download bereit.


Die hier verfügbaren Informationsmaterialien können für eigene Zwecke, z. B. interne Schulungen, frei verwendet werden. Sollten Sie eine Vervielfältigung oder eine andere Verwendung anstreben, können Sie sich direkt mit dem BayLDA in Verbindung setzen.

Fragen und Antworten

**Flyer**


Weitere Datenschutzthemen

DS-GVO einfach umgesetzt in...




**Vereinen**

Der Fokus dieses Flyers liegt



**Unternehmen**

Der Fokus dieses Flyers liegt



**Arztpraxen**

Der Fokus dieses Flyers liegt



# Hilfreiche Dokumente

## Top 10 der wichtigsten Punkte

- ✓ Mitglieder über die Verarbeitung informieren
- ✓ Verzeichnis der Verarbeitungstätigkeiten
- ✓ Über Veröffentlichung von Fotos informieren
- ✓ Beschäftigte und Mitglieder sensibilisieren
- ✓ Webseite sicher halten
- ✓ Auftragsverarbeitungsverträge erforderlich?
- ✓ Einwilligungstexte überprüfen
- ✓ Regelmäßige Sicherung der Mitgliederdaten
- ✓ Datenpannen einfach online melden
- ✓ Ggf. Datenschutzbeauftragte/n benennen

Erläuterungen hierzu finden Sie auf

[www.lida.bayern.de/top10](http://www.lida.bayern.de/top10)

## Datenschutz

### Zentrale Datenschutzthemen



## Vereinen

7/50

Quelle: [https://www.lida.bayern.de/media/DS-GVO\\_in\\_Vereinen.pdf](https://www.lida.bayern.de/media/DS-GVO_in_Vereinen.pdf)



# Hilfreiche Dokumente

## Zielgruppe dieses Flyers



Der Fokus dieses Flyers liegt auf  
kleinen Vereinen.

Die genannten Datenschutzanforderungen  
betreffen kleine Vereine aus allen Bereichen,  
z. B. Traditions-, Sport-, Hobby-,  
Musik- und Kulturvereine.



## INFORMATIONSPFLICHTEN

Jeder Verein hat seinen Mitgliedern schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Zumindest muss er darauf hinweisen, wo die Informationen leicht zugänglich bereit gehalten werden. Es empfiehlt sich daher, diese Informationen bereits im **Aufnahmeantrag** zu erteilen.

„Bestandsmitglieder“, die schon vor dem 25.05.2018 eingetreten sind, muss der Verein **nicht** („rückwirkend“) nach den Vorschriften der DS-GVO informieren.

## SICHERHEIT DER VERARBEITUNG



Um Mitgliederdaten zu schützen, müssen Vereine **Standardsicherheitsmaßnahmen** anwenden.

Der Einsatz aktueller Betriebssysteme, Passwortschutz und Backups sind dabei das A und O.

Damit Unbefugte nicht an die schutzwürdigen Daten herankommen, sind Datenbanken mit personenbezogenen Daten entsprechend abzusichern.



## VERZEICHNIS DER VERARBEITUNGSTÄTIGKEITEN

Vereine gehen im Alltag mit vielen personenbezogenen Daten um, insbesondere mit Daten zu ihren Mitgliedern. Deshalb besteht auch für Vereine die **gesetzliche Verpflichtung**, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Aus diesem soll ersichtlich werden, welche Daten (Kategorien) zu welchem Zweck verarbeitet werden.

Wie so etwas aussehen kann, zeigt das BayLDA auf seiner Webseite in einem **Muster-Verzeichnis** für Vereine.

## EINWILLIGUNGEN



Für die Verwendung von Daten des Mitglieds zu Zwecken der **Mitgliederverwaltung** ist keine Einwilligung nötig. Gleiches gilt in der Regel für die Übermittlung von Daten an einen **Dachverband**, wenn die Übermittlung zur Erfüllung des Vereinszwecks erforderlich ist, z. B. zur Teilnahme von Mitgliedern an Wettkämpfen, die unter der Regie des Dachverbandes organisiert werden.

Eine Einwilligung ist nur für darüber hinausgehende Verarbeitungen nötig, z. B. (in aller Regel) wenn **Kontaktdaten** aller Mitglieder an alle Mitglieder verteilt werden sollen oder zur Veröffentlichung von Porträtfotos auf der Homepage.

## DATENSCHUTZVERLETZUNGEN

Kommt es im Verein zu Sicherheitsvorfällen im Umgang mit personenbezogenen Daten, so besteht eine **gesetzliche Meldepflicht** beim BayLDA als Aufsichtsbehörde.

Beispiele solcher Datenschutzverletzungen:

- Diebstahl oder Verlust eines Notebooks
- Hacking-Angriff auf die Mitgliederdatenbank
- Verschlüsselungstrojaner per E-Mail

Die Mitglieder sind übrigens nur dann zu informieren, wenn ein hohes Datenschutzrisiko besteht (was die Ausnahme ist).

## RECHTE DER VEREINSMITGLIEDER



Mit der DS-GVO werden den Personen, deren Daten verarbeitet werden (also z. B. den Vereinsmitgliedern), eine Reihe von Rechten eingeräumt. Die Mitglieder können vom Verein jederzeit **Auskunft** über die Verarbeitung ihrer Daten verlangen.

Sobald keine gesetzliche Grundlage mehr für die Speicherung der Daten besteht, sind sie zu **löschen** – Daten zur Mitgliederverwaltung grundsätzlich nach Austritt des Mitglieds (es sei denn, sie werden z. B. noch für steuerliche Zwecke oder eine Chronik benötigt).

## KOMMUNIKATION MIT MITGLIEDERN

Kommunikation mit Mitgliedern per E-Mail oder per Kontaktformular über die eigene Homepage ist meist problemlos möglich, wenn die erforderliche **Transportverschlüsselung** (STARTTLS/https) eingerichtet ist.

Sollen sensible Informationen ausgetauscht werden, ist die Möglichkeit für eine Inhaltsverschlüsselung als Maßnahme zum Schutz vor unbefugter Kenntnisnahme zu schaffen.

## DATENSCHUTZBEAUFTRAGTE/R (DSB)



Für viele Vereine besteht **keine Pflicht**, eine(n) DSB zu benennen. Ein(e) DSB ist insbesondere zu benennen, wenn in der Regel **mindestens zehn Personen ständig** mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.

Trainerinnen und Trainer sind nicht schon deshalb mitzuzählen, weil sie z. B. eine Liste ihrer Gruppen- oder Mannschaftsmitglieder haben.





# Politische Unterstützung

Veröffentlichung gemäß Ministerratsbeschluss  
vom 5. Juni 2018

## **Datenschutz-Grundverordnung (DSGVO): Der Bayerische Weg zu einer bürgernahen und mittelstandsfreundlichen Anwendung**

Der Ministerrat beschließt nachfolgenden Bayerischen Weg zu einer bürgernahen und mittelstandsfreundlichen Anwendung des Datenschutzrechts, die die Ziele der Datenschutz-Grundverordnung sachgerecht und mit Augenmaß verfolgt und damit auch ihre Akzeptanz in der Bevölkerung fördert:

- Kein Amateursportverein, keine Musikkapelle oder sonstige vor allem durch ehrenamtliches Engagement getragene Vereine müssen einen Datenschutzbeauftragten bestellen.
- Bei einem Erstverstoß im Dickicht der Datenschutzregeln drohen keine Bußgelder; Hinweise und Beratung haben Vorrang vor Sanktionen.



9/50

Quelle: <https://www.verkuendung-bayern.de/files/allmbl/2018/09/allmbl-2018-09.pdf>



# Politische Unterstützung

- Wir werden eine Praxis von Abmahnanwälten, die glauben bei Unternehmen formelle Datenschutzverstöße rechtsmissbräuchlich abmahnen und abkassieren zu können, nicht hinnehmen.
- Wir werden mit den Betroffenen weitere Bestimmungen im Datenschutzrecht identifizieren, bei deren Anwendung im Besonderen darauf hinzuwirken ist, dass die Ziele der Datenschutz-Grundverordnung sachgerecht und mit Augenmaß verfolgt werden.
- Hierzu werden wir weitere Gespräche mit Vereinen und Mittelständlern anbieten.



10/50

Quelle: <https://www.verkuendung-bayern.de/files/allmbl/2018/09/allmbl-2018-09.pdf>



## Grundlagen

***Daten sind das Öl des  
21. Jahrhunderts, und  
Datenanalyse der  
Verbrennungsmotor***

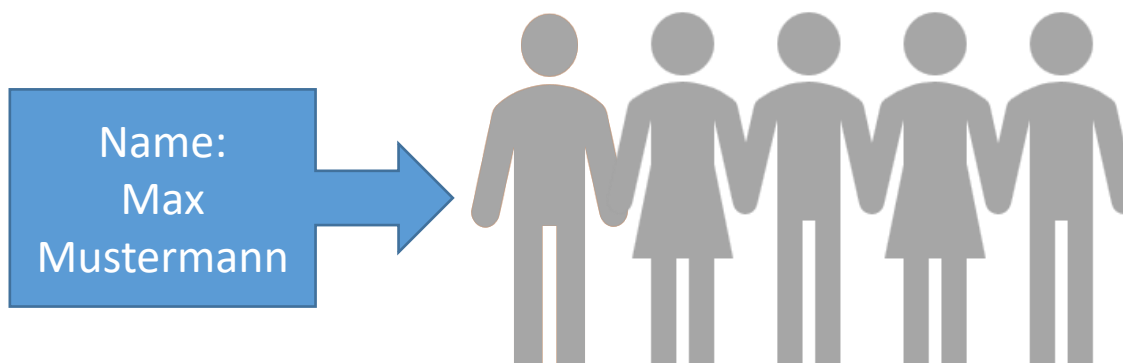


11/50



# Grundlagen

- ❖ **Worum geht es?** personenbezogene Daten (pbD)
- ❖ **Was ist das?** Was ist das? Alle Angaben, die sich auf eine identifizierte oder aber auch nur identifizierbare Person beziehen.
- ❖ **IDENTIFIZIERT** ist eine Person, wenn sich ihre Identität direkt aus dem Datum selbst ergibt.

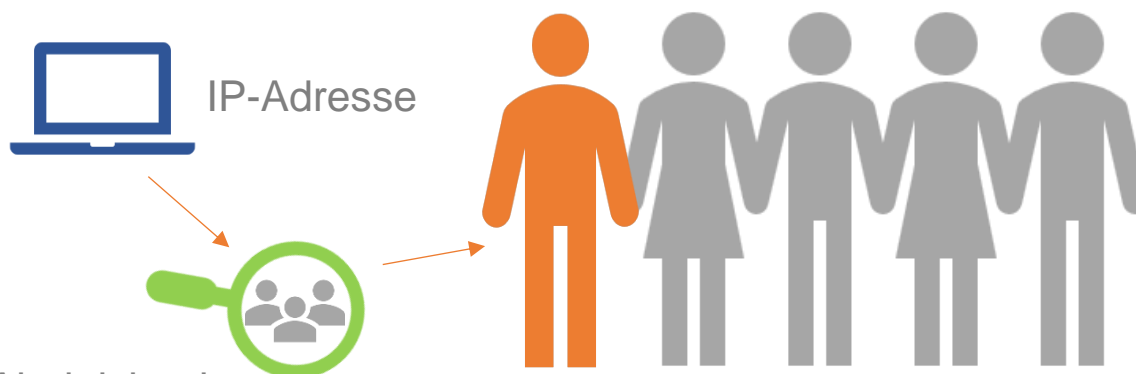






# Grundlagen

- ❖ **Worum geht es?** personenbezogene Daten (pbD)
- ❖ **Was ist das?** Alle Angaben, die sich auf eine identifizierte oder aber auch nur identifizierbare Person beziehen.
- ❖ **IDENTIFIZIERBAR** wird eine Person, wenn ihre Identität durch die Kombination des Datums mit einer anderen Information feststellbar wird.



13/50

Abgleich mit  
Providerdaten



# Grundlagen

- ❖ **Beispiele?** Name, Vorname, Geburtsdatum, Familienstand, Zahl der Kinder, Beruf, Eigentums- oder Besitzverhältnisse, Mitgliedschaft in Organisationen, Datum des Vereinsbeitritts, sportliche Leistungen, Platzierungen bei einem Wettbewerb, E-Mail-Adressen, Anschriften, Kfz-Kennzeichen, Flurnummern, Bankverbindungen, Sozialversicherungsnummern, Kundennummern, Fotos, IP-Adressen, Online-Kennungen, auch Eigenschaften wie „ledig“ oder „im Urlaub“,...



14/50



# Grundlagen

- ❖ **Was sind besondere Kategorien pbD?** rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder sexuellen Orientierung einer natürlichen Person **(besonderer Schutzbedarf!!!)**





# Grundlagen

- ❖ **Um wessen pbD geht es?** Mitarbeiter(innen), Mitglieder, Übungsleiter(innen), also alle (lebenden) natürlichen Personen



16/50





## Volkszählungsurteil des BVerfG (1983)

Jeder Mensch  
soll grundsätzlich **selbst** über die  
Preisgabe und Verwendung  
seiner persönlichen Daten  
bestimmen.



17/50



# Grundlagen

- ❖ **Was schützt der Datenschutz?** Umgang mit pbD (Ausfluss des Schutzes der Würde des Menschen und der freien Entfaltung der Persönlichkeit – Grundrecht in GG und EU)
- ❖ **Warum ist das wichtig?** Immer mehr Daten werden verarbeitet, zusammengefasst und ausgewertet – Gefahr des Missbrauchs; deshalb: klare gesetzliche Vorgaben erforderlich, um jeden Einzelnen vor der Einschränkung seiner Persönlichkeits- und Freiheitsrechte gegen unrechtmäßige Datenverarbeitung zu schützen



# Grundlagen

- ❖ **Ist das neu?** Nein, erstes BDSG bereits im Jahr 1977, Neufassung aus dem Jahr 1990, Novellierung im Jahr 2009 zur Umsetzung der EG-Datenschutzrichtlinie aus dem Jahr 1995, BDSG neu im Jahr 2017 als Begleitgesetz zur Datenschutzgrundverordnung (DS-GVO)



19/50



# Grundlagen

## Rechtsexperte: Datenschutz-Grundverordnung als "größte Katastrophe des 21. Jahrhunderts"

27.04.2016 11:25 Uhr - Stefan Krempel

vorlesen



Thomas Hoeren (Bild: heise online / Stefan Krempel)

Der Münsteraner Informationsrechtler Thomas Hoeren hat die neue europäische Datenschutzverordnung zu "einem der schlechtesten Gesetze des 21. Jahrhunderts" gekürt. Das überbordende Werk sei "hirnlos".

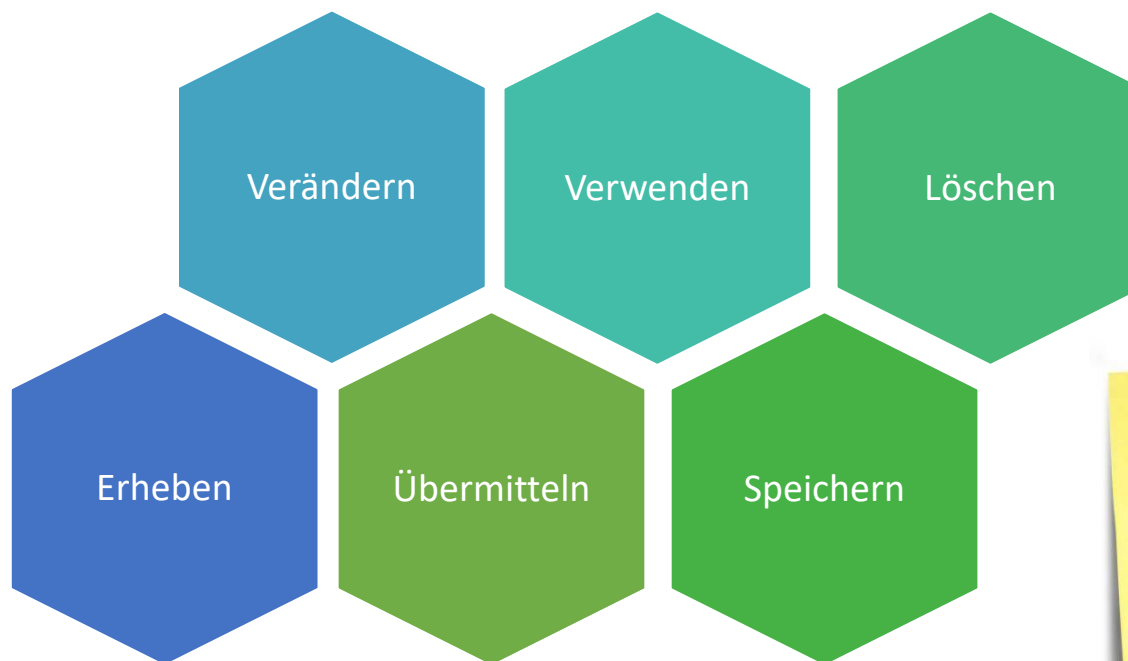
Quelle: <https://www.heise.de/newsticker/meldung/Rechtsexperte-Datenschutz-Grundverordnung-als-groesste-Katastrophe-des-21-Jahrhunderts-3190299.html>





# Datenverarbeitung

❖ **Verarbeitung** personenbezogener Daten Art. 4 Nr. 2 DSGVO, z.B.





# Datenverarbeitung

❖ So stellen wir uns einen Verein vor:

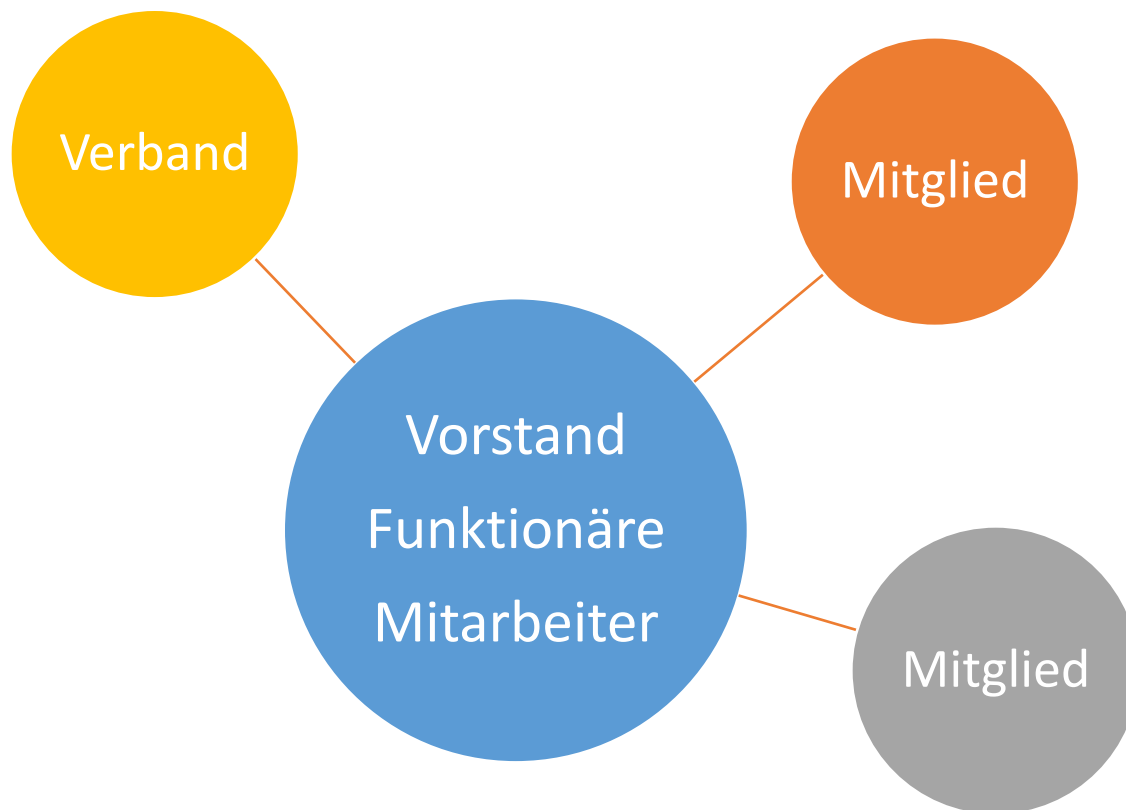


22/50



# Datenverarbeitung

❖ Verein im datenschutzrechtlichen Sinn:



23/50



# Finger weg!

❖ Das Datenschutzrecht **verbietet** grundsätzlich den Umgang mit personenbezogenen Daten, erlaubt diese aber unter bestimmten Voraussetzungen (Verbot mit Erlaubnisvorbehalt). DATENUMGANG ist **nur zulässig**, wenn er ...

- **durch das Datenschutzrecht selbst ...**

Beispiel: Zur Durchführung eines Vertrages



- **oder durch eine besondere Rechtsvorschrift ...**

Beispiel: Steuern, Abgaben



- **oder durch die Einwilligung des Betroffenen ...**

Beispiel: Einverständniserklärung zur Datennutzung



.. erlaubt **und** dem Betroffenen **transparent** gemacht wird.





# Rechtsgrundlage Art. 6 DS- GVO

Die Verarbeitung ist **nur rechtmäßig**, wenn **mindestens** eine der nachstehenden Bedingungen erfüllt ist:

- a) Die betroffene Person hat ihre **Einwilligung** zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b) die Verarbeitung ist für die **Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die **auf Anfrage der betroffenen Person** erfolgen;
- c) die Verarbeitung ist zur Erfüllung einer **rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt;





## Rechtsgrundlage Art. 6 DS- GVO

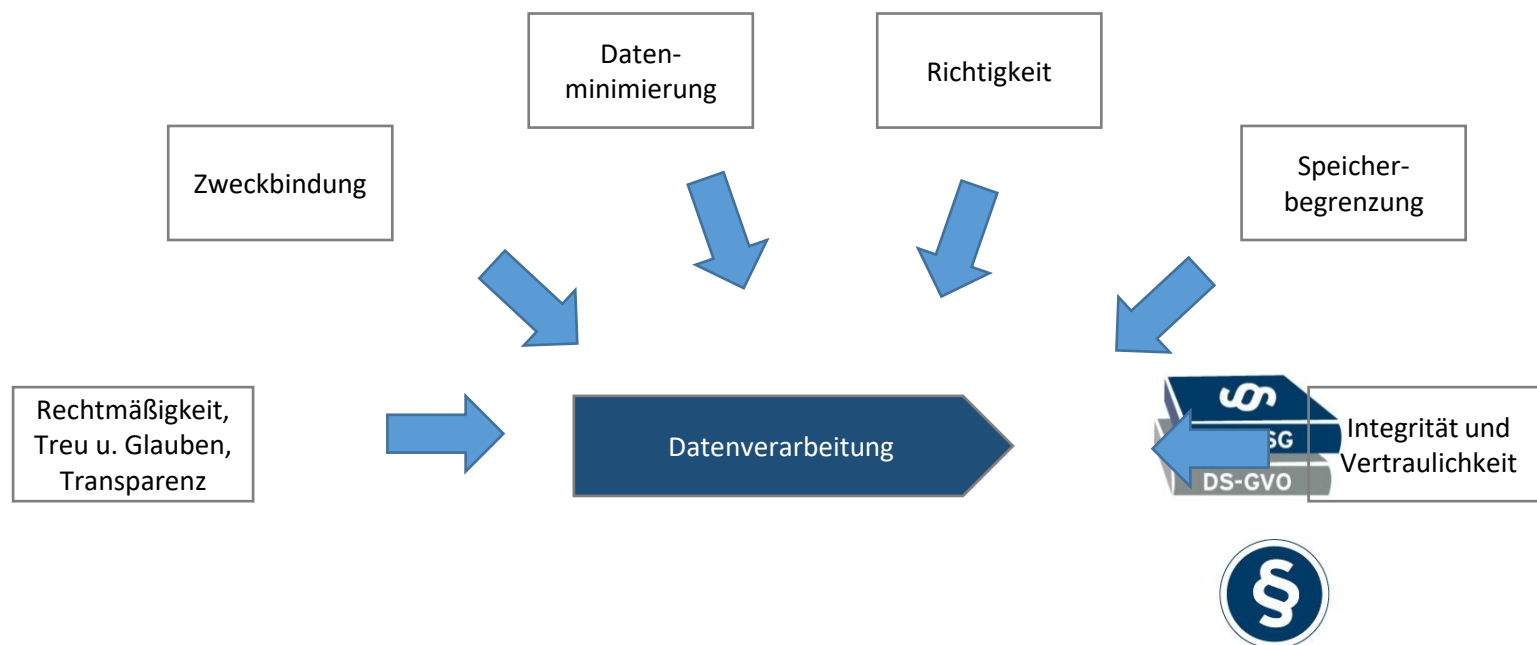
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.



Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.



# Verarbeitungsgrundsätze Art. 5 DS- GVO



**Art. 5 Abs. 2 DS-GVO: Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung (jederzeit) nachweisen können („Rechenschaftspflicht“, Accountability)**





# Anforderungen der Aufsichtsbehörde

Bayerisches Landesamt für  
Datenschutzaufsicht



Bayerisches Landesamt für  
Datenschutzaufsicht



## Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.

### Muster 1: Verein

#### Hinweis:

Jede 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, ist ein sog. Verantwortlicher. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält. In der folgenden Übersicht werden die wesentlichen Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

#### Kurzbeschreibung des Vereins

Ein kleiner Sportverein hat 200 Mitglieder, einen ersten Vorstand, einen Kassier sowie einen Schriftführer (Vorstand im Sinne des BGB) sowie fünf Personen, die nach der sog. Übungsleiterpauschale bezahlt werden. Die Mitgliederverwaltung erfolgt durch den Schriftführer selbst. Die Verwaltung der Mitgliedsbeiträge erfolgt dagegen durch den Kassier. Der Verein betreibt zudem eine kleine Webseite, die bei einem Dienstleister gehostet ist, mit Mitgliederfotos.

#### Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung (über einen externen Dienstleister)
- Mitgliederverwaltung
- Betrieb der Webseite des Sportvereins (über Hosting-Paket eines externen Dienstleisters)
- Veröffentlichung von Mitgliederfotos auf der eigenen Webseite
- Beitragsverwaltung

### 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 Informations- und Auskunftspflichten

Gibt es eine Anforderung zur Datenlöschung?

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

#### E Lösen 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)

## 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, wen 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.bayern.de/media/dsk\\_kpnr\\_12\\_datenschutzbeauftragter.pdf](http://www.lida.bayern.de/media/dsk_kpnr_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.bayern.de/media/muster\\_1\\_veerein\\_verzeichnis.pdf](http://www.lida.bayern.de/media/muster_1_veerein_verzeichnis.pdf)

DSK-Kurzpapier Nr. 1: [www.lida.bayern.de/media/dsk\\_kpnr\\_1\\_verzeichnis\\_verarbeitungstaetigkeiten.pdf](http://www.lida.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf)

DSK-Muster-Verzeichnis allgemein: [www.lida.bayern.de/media/dsk\\_muster\\_vor\\_verantwortlicher.pdf](http://www.lida.bayern.de/media/dsk_muster_vor_verantwortlicher.pdf)

### C Datenschutz-Verpflichtung von 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.bayern.de/media/info\\_verpflichtung\\_beschaeftigte\\_ds-gvo.pdf](http://www.lida.bayern.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.bayern.de/media/dsk\\_kpnr\\_6\\_auskunftsrecht.pdf](http://www.lida.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf)

DSK-Kurzpapier Nr. 10: [www.lida.bayern.de/media/dsk\\_kpnr\\_10\\_informationspflichten.pdf](http://www.lida.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf)

### E Lösen 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.bayern.de/media/dsk\\_kpnr\\_11\\_vergessenwerden.pdf](http://www.lida.bayern.de/media/dsk_kpnr_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.bayern.de/media/baylda\\_ds-gvo\\_1\\_security.pdf](http://www.lida.bayern.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.bayern.de/media/dsk\\_kpnr\\_13\\_auftragsverarbeitung.pdf](http://www.lida.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf)

BayLDA-Formulierungshilfe zum Vertrag: [www.lida.bayern.de/media/muster\\_10\\_v.pdf](http://www.lida.bayern.de/media/muster_10_v.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.bayern.de/media/baylda\\_ds-gvo\\_8\\_dat\\_breach\\_notification.pdf](http://www.lida.bayern.de/media/baylda_ds-gvo_8_dat_breach_notification.pdf)

BayLDA-Online-Service zur Meldung: [www.lida.bayern.de/de/datengpanne.html](http://www.lida.bayern.de/de/datengpanne.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 solches hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

DSK-Kurzpapier Nr. 5: [www.lida.bayern.de/media/dsk\\_kpnr\\_5\\_dsfa.pdf](http://www.lida.bayern.de/media/dsk_kpnr_5_dsfa.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.bayern.de/media/dsk\\_kpnr\\_15\\_videoueberwachung.pdf](http://www.lida.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf)

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



# Anforderungen der Aufsichtsbehörde

## A Datenschutzbeauftragter (DSB)

*Muss ein DSB vom Verein benannt werden?*

☐ ja

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

## 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.



# Anforderungen der Aufsichtsbehörde

## B Verzeichnis von Verarbeitungstätigkeiten

*Ist ein solches Verzeichnis erforderlich?*

- ☒ ja (wegen der regelmäßigen Verarbeitung  
personenbezogener Daten)  
☐ nein

## 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.bayern.de/media/muster\\_1\\_verein\\_verzeichnis.pdf](http://www.lida.bayern.de/media/muster_1_verein_verzeichnis.pdf)

DSK-Kurzpapier Nr. 1:

[www.lida.bayern.de/media/dsk\\_kpnr\\_1\\_verzeichnis\\_verarbeitungstaetigkeiten.pdf](http://www.lida.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf)

DSK-Muster-Verzeichnis allgemein:

[www.lida.bayern.de/media/dsk\\_muster\\_vov\\_verantwortlicher.pdf](http://www.lida.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf)



# Anforderungen der Aufsichtsbehörde

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.lda.bayern.de/media/dsk\\_muster\\_vov\\_verantwortlicher.pdf](http://www.lda.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](mailto:team@waldermuehler-tsv.de)  
Web: [www.waldermuehler-tsv.de](http://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 <a href="mailto:herbert@waldermuehler-tsv.de">herbert@waldermuehler-tsv.de</a>	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 <a href="mailto:herbert@waldermuehler-tsv.de">herbert@waldermuehler-tsv.de</a>	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 <a href="mailto:max@waldermuehler-tsv.de">max@waldermuehler-tsv.de</a>	28.02.2018	Außerdemarstellung	<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 <a href="mailto:max@waldermuehler-tsv.de">max@waldermuehler-tsv.de</a>	20.02.2018	Außerdemarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 <a href="mailto:herbert@waldermuehler-tsv.de">herbert@waldermuehler-tsv.de</a>	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
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virens Scanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder



# Anforderungen der Aufsichtsbehörde

## C Datenschutz-Verpflichtung von Beschäftigten

*Ist eine solche Verpflichtung durchzuführen?*

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

## C Datenschutz-Verpflichtung von 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.la-bayern.de/media/info\\_verpflichtung\\_beschaeftigte\\_dsgvo.pdf](http://www.la-bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf)





# Anforderungen der Aufsichtsbehörde

## D Information- und Auskunftspflichten

*Bestehen irgendwelche Informationspflichten?*

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

## 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.bayern.de/media/dsk\\_kpnr\\_6\\_auskunftsrecht.pdf](http://www.lida.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf)

DSK-Kurzpapier Nr. 10:

[www.lida.bayern.de/media/dsk\\_kpnr\\_10\\_informationspflichten.pdf](http://www.lida.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf)

**AKTUELL:**

<https://www.datenschutzzentrum.de/uploads/praxisreihe/Praxisreihe-4-Informationspflichten.pdf>

<https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/05/Praxisratgeber-f%C3%BCr-Vereine.pdf>



# Anforderungen der Aufsichtsbehörde

## E Löschen von Daten

*Gibt es eine Anforderung zur Datenlöschung?*

- ☒ ja (aber erst nach Ablauf gesetzlicher  
Aufbewahrungspflichten)  
☐ nein

## 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.bayern.de/media/dsk\\_kpnr\\_11\\_vergessenwerden.pdf](http://www.lida.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf)





# Anforderungen der Aufsichtsbehörde

## F Sicherheit

*Müssen die Daten besonders gesichert werden?*

☐ ja

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

## 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.bayern.de/media/baylda\\_ds-gvo\\_1\\_security.pdf](http://www.lida.bayern.de/media/baylda_ds-gvo_1_security.pdf)



# Anforderungen der Aufsichtsbehörde

## G Auftragsverarbeitung

*Ist ein Vertrag zur Auftragsverarbeitung notwendig?*

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

## 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.

**AKTUELL:**

[https://www.lida.bayern.de/media/FAQ\\_Abgrenzung\\_Auftragsverarbeitung.pdf](https://www.lida.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf)



# Anforderungen der Aufsichtsbehörde

## H Datenschutzverletzungen

*Müssen bestimmte Vorfälle gemeldet werden?*

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

## 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.bayern.de/media/baylda\\_ds-gvo\\_8\\_data\\_breach\\_notification.pdf](http://www.lida.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf)

BayLDA-Online-Service zur Meldung:

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

Online Meldung für Datenpannen:

<https://www.lida.bayern.de/de/datenpanne.html>



# Anforderungen der Aufsichtsbehörde

## I Datenschutz-Folgeabschätzung (DSFA)

*Muss eine DSFA vom Verein durchgeführt werden?*

☐ ja

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

## I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

DSK-Kurzpapier Nr. 5:

[www.lida.bayern.de/media/dsk\\_kpnr\\_5\\_dsfa.pdf](http://www.lida.bayern.de/media/dsk_kpnr_5_dsfa.pdf)



# Anforderungen der Aufsichtsbehörde

## J Videoüberwachung (VÜ)

*Besteht eine Ausschilderungspflicht bezüglich VÜ?*

☐ ja

☒ nein (da keine Videoüberwachung im Verein durchgeführt wird)

## 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.bayern.de/media/dsk\\_kpnr\\_15\\_videoueberwachung.pdf](http://www.lida.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf)



# Empfohlene Lektüre

- ❖ Webseiten (Tipps und Muster):
  - <https://www.lida.bayern.de>
  - <https://www.dsgvo-verstehen-bayern.de/vereine/>
- ❖ Dokumente und Muster:
  - [Praxisratgeber für Vereine](#)
  - [Datenschutz im Verein nach der DS-GVO](#)
  - [Fotos im Verein](#)
- ❖ Mustervorlagen und Arbeitshilfen:
  - [Württembergischer Landessportbund e.V.](#)
  - [Landessportbund Thüringen](#)
  - [Fragen und Antworten](#)
  - [Facebook Fanpage](#)



# In eigener Sache

Quelle:  
Weissenburger  
Tagblatt vom  
17.11.2018

Seite 6 / Nr. 266

## LOKALES

Interview mit Rechtsanwalt Thomas Engelhardt zur neuen Datenschutz-Grundverordnung

### „Insgesamt ist die DSGVO positiv“

Der zertifizierte Datenschutzbeauftragte kennt die Verunsicherung der Vereine und rät zur Gelassenheit

WEISSENBURG – Die neue Datenschutz-Grundverordnung (DSGVO) versichert viele kleine Vereine in der Region. Wie soll man fortan mit personenbezogenen Daten umgehen? Was darf man überhaupt noch auf die vereinseigene Internetseite stellen? Wie müssen die Mitgliedsanträge verändert werden, um rechtskonform zu sein, und vieles mehr. Fragen, auf die Thomas Engelhardt Antworten hat.

Herr Engelhardt, Sie sind zertifizierter Datenschutzbeauftragter und reisen derzeit durch die Lande, um die verunsicherten Vereine fit für die Anforderungen der neuen Datenschutz-Grundverordnung (DSGVO) zu machen. Was sind denn die größten Ängste der Vereine?

Thomas Engelhardt: Es existiert leider immer noch eine allgemeine Verunsicherung bei den Vereinsverantwortlichen. Das beginnt bei der Frage, was überhaupt personenbezogene Daten sind, über die doch recht juristisch geprägten und formellen Anforderungen der DSGVO bis hin zu Haftungsfragen in Anbetracht des doch beachtlichen neuen Bußgeldrahmens.

Sie kennen die Arbeit im Verein aus eigener Erfahrung, weil Sie selbst 13 Jahre lang Vorsitzender eines kleinen Sportvereins waren. Wurde Ihrer Ansicht nach bislang mit persönlichen Daten, die Sie in Ihren Seminaren auch als „das Öl des 21. Jahrhunderts“ bezeichnen, zu sorglos umgegangen?

Engelhardt: Im Großen und Ganzen geht man mit personenbezogenen Daten in den Vereinen durchaus verantwortungsbewusst um, gerade im Vergleich zu den globalen Playern, wie Facebook und Co. Allerdings stelle ich immer wieder fest, dass das Thema IT-Sicherheit nicht den erforderlichen Stellenwert genießt. Was macht man beispielsweise, wenn die Festplatte des Computers den Geist aufgibt? Gerade eine regelmäßige Sicherung ist in derartigen Fällen Gold wert und wird auch datenschutzrechtlich gefordert. Das Zitat, dass Daten das Öl des 21. Jahrhunderts sind, spiegelt das wirtschaftliche Potenzial von Daten wider.

Vor der Landtagswahl wurde bezüglich der DSGVO von der CSU der Eindruck erweckt, dass Bayern einen Sonderweg einschlagen könnte und man es im Freistaat mit der DSGVO nicht so genau nehmen müsse. Wie bewerten Sie diese Auffassung?

Engelhardt: Bei den für Vereine und Unternehmen geltenden Gesetzen handelt es sich um die Datenschutz-Grundverordnung (DSGVO) und das neue Bundesdatenschutzgesetz (BDSG). Das sind Gesetze der EU und des Bundes, keine Landesgesetze. Allein daran kann man schon erkennen,



Ist Experte für Datenschutz und berät Vereine; der Gunzenhauser Rechtsanwalt Thomas Engelhardt. Foto: Steiner

inwieweit die Bayerische Staatsregierung mit einem Ministerratsbeschluss Einfluss auf diese nehmen kann. Die DSGVO und das BDSG gelten auch innerhalb Bayerns uneingeschränkt. Ungeachtet dessen hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) mit Sitz in Ansbach als Aufsichtsbehörde für den Datenschutz bei bayerischen Unternehmen und Vereinen zwischenzeitlich auf seiner Webseite [lda.bayern.de](http://lda.bayern.de) hervorragende Muster zur Verfügung gestellt, an denen man sich als Vereinsverantwortlicher gut orientieren kann. Dies gilt auch für die Webseite des Bayerischen Staatsministerium des Innern unter [dsgvo-verstehen-bayern.de](http://dsgvo-verstehen-bayern.de).

Der Münsteraner Informationsrechtler Thomas Hoeren hat die neue europäische Datenschutz-Grundverordnung zu einem der schlechtesten Gesetze des 21. Jahrhunderts gekürt...

Engelhardt: Einige Dinge, die Prof. Dr. Hoeren moniert hat, haben sich zwischenzeitlich geklärt. Ungeachtet dessen wurde gerade bei den Informationspflichten in der DSGVO dem Datenschutz ein Bärendienst erwiesen, indem immer unausgefordert über die Datenverarbeitung umfassend informiert werden muss. Dies ist nach meiner Einschätzung eher kontraproduktiv und aufwendig. Ansonsten dürfen wir nicht vergessen, dass die DSGVO das bisher in Deutschland ohnehin schon geltende Datenschutzrecht weitestgehend übernommen hat. Dieses war allerdings auch in Deutschland kaum bekannt und noch weniger in der Praxis umgesetzt. Insgesamt bewerte ich daher die DSGVO als durchaus positiv. Unternehmen wie Face-

book und Google nehmen Datenschutz deutlich ernster im Hinblick auf das Bußgeldrisiko von bis zu vier Prozent des weltweiten Jahresumsatzes. Unbefriedigend ist für mich allerdings, dass bei vielen Fragen, zum Beispiel ob Vereine einen Datenschutzbeauftragten zu bestellen haben, also bei der Auslegung des neuen BDSG, schon die Datenschutzaufsichtsbehörden innerhalb Deutschlands unterschiedliche Auffassungen vertreten. Wie wollen wir da ein europaweit einheitliches Datenschutzniveau erreichen?

Wohin kann man sich denn wenden, wenn man als Vereinsvertreter Fragen zur neuen Datenschutz-Grundverordnung hat und verunsichert ist?

Engelhardt: Die von mir angesprochenen Internetseiten bieten Hilfestellung und Muster, wobei man ergänzend sagen muss, dass auch viele Verbände zwischenzeitlich viele Musterverträge für ihre spezifischen Bereiche zur Verfügung stellen. Auch eine telefonische Anfrage beim BayLDA ist dem Grunde nach möglich, wenn man Fragen zum Thema hat. Ansonsten empfiehlt es sich, Rechtsanwälte mit entsprechendem Fachwissen oder Berater zum Thema Datenschutz zu konsultieren.

Was sind denn die wichtigsten Punkte, um als Verein auf der sicheren Seite zu sein?

Engelhardt: Die Mitglieder über die Verarbeitung informieren, ein Verzeichnis der Verarbeitungstätigkeiten erstellen, über die Veröffentlichung von Fotos informieren, Beschäftigte und Mitglieder sensibilisieren, die Internetseite sicher halten, prüfen, ob Auftragsverarbeitungsverträge erforderlich sind, die Einwilligungstexte überprüfen, eine regelmäßige Sicherung der Mitgliederdaten, Datenpannen online melden und gegebenenfalls eine/n Datenschutzbeauftragte/n benennen. Wenn man sich an den Anforderungen des BayLDA orientiert, ist diese imposant wirkende Liste mit vertretbarem Aufwand zu erfüllen.

Wenn es zu einer Datenpanne im Verein kommt, besteht eine gesetzliche Meldepflicht beim Bayerischen Landesamt für Datenschutz in Ansbach. Wie werden Ihrer Ansicht nach denn Verstöße gegen die DSGVO geahndet?

Engelhardt: In der DSGVO steht explizit, dass die im Einzelfall verhängte Sanktion „wirksam, verhältnismäßig und abschreckend“ sein muss. Es hängt also immer entscheidend vom Einzelfall ab, also was geschehen ist und ob die Datenpanne beispielsweise vorsätzlich oder fahrlässig passiert ist. Bei einem geringen Erstverstoß wird man nach meiner Einschätzung nicht mit der Verhängung einer Geldbuße rechnen müssen.

Interview: MARKUS STEINER





# Bilder

https://www.lida.bayern.de/de/infoblaetter.html

BayLDA Aktuelles Online-Services Themen Veröffentlichung

> Veröffentlichungen > Infoblätter & Flyer

Informationsmaterialien

FLYER FRAGEN UND ANTWORTEN WEITERE DATENSCHUTZTHEMEN

- ⌚ Abgrenzung Auftragsverarbeitung
- ⌚ ADV Formerfordernis
- ⌚ Amtssprache
- ⌚ Auftragsverarbeitung Arzt
- ⌚ Bestellpflicht von DSB wegen ständiger Beschäftigung
- ⌚ DSB im medizinischen Bereich
- ⌚ Hosting keine Auftragsverarbeitung
- ⌚ Informationspflicht im Verein
- ⌚ Informationspflichten Sprache
- ⌚ Informationspflichten Telefon
- ⌚ Löschen von Patientendaten
- ⌚ Steuerberater keine ADV
- ⌚ Rechtsgrundlage der Verarbeitung Arztpraxis
- ⌚ Aufruf Patienten mit Namen
- ⌚ Bilder und Verein
- ⌚ Versand von Patientenunterlagen in passwortgeschützter ZIP-Datei

## ⌚ Bilder und Verein

42/50





## **AI** In anderen EU-Ländern kassieren Behörden groß ab

Die schlechte Ausstattung auch ein Standortnachteil, heißt es aus Sachsen. "Wir sind nicht nur Aufsichtsbehörde, sondern auch Berater und Service-Dienstleister."

## Deutschland



Von Lars Wienand  
21.11.2018, 08:30 Uhr

Unter Landespolitikern haben Datenschützer neben Unverständnis auch Unwillen gespürt, für eine Aufgabe zu zahlen, die von der EU kommt. Andere EU-Länder haben zum Teil andere Finanzierungsmodelle gefunden. "Behörden finanzieren sich aus den Bußgeldern selbst und können hohe Bußgelder erzielen", erläutert Brink. "Deutsche Datenschutzbeauftragte haben von Bußgeldverfahren nur den Aufwand, weil das Geld in den Landeshaushalt fließt."

Allerdings führt das andere Modell auch zu Auswüchsen: In Portugal wurde ein Bußgeld von 400.000 Euro gegen ein Krankenhaus mit schlechtem Datenzugriffskonzept verhängt, was in Deutschland vielleicht zu einer Geldbuße von 20.000 Euro führen würde, so Brink. "Mittelfristig werden die unterschiedlichen Maßstäbe auch zum Thema auf EU-Ebene werden. Es ist auch eine Frage ungleichen Wettbewerbs, wenn ein Automobilkonzern in Frankreich eine massive Millionenstrafe zahlen muss und in Deutschland für den gleichen Verstoß mit einer besseren Ermahnung davon kommt."

utz

43/50

Quelle: [https://www.t-online.de/digital/id\\_84813238/dsgvo-chaos-deutschland-droht-eu-verfahren-wegen-datenschutz.html](https://www.t-online.de/digital/id_84813238/dsgvo-chaos-deutschland-droht-eu-verfahren-wegen-datenschutz.html)




# Aktuelles

KNUDELS-LEAK

## Datenschützer verhängen erstmalig Bußgeld nach DSGVO

Der Karlsruher Chatanbieter Knuddels muss nach einem [Datenleck mit fast zwei Millionen veröffentlichten Zugangsdaten](#) ein Bußgeld in Höhe von 20.000 Euro zahlen. Das teilte der baden-württembergische Datenschutzbeauftragte Stefan Brink am Donnerstag mit. Wegen der ungeschützten Speicherung von Passwörtern habe Knuddels gegen den [Artikel 32 der EU-Datenschutz-Grundverordnung \(DSGVO\)](#) [verstoßen](#). Es ist laut Brink das erste Bußgeld, das eine Datenschutzbehörde in Deutschland [nach der im Mai 2018 in Kraft getretenen DSGVO](#) verhängt hat.



44/50

Quelle: <https://www.golem.de/news/knuddels-leak-datenschuetzer-verhaengen-erstmalig-bussgeld-nach-dsgvo-1811-137857.html>



# Aktuelles





45/50





# Aktuelles

BayLDA  Bayerisches Landesamt für Datenschutzaufsicht 

Statistik BayLDA

BayLDA Statistik	2013	2014	2015	2016	2017	2018 (01.01-22.10)	2018 davon bis 25.Mai	2018 davon seit 25.Mai	Abweichung 2017(22.10) zu 2018	Trend
						Summe				
Beratungen Vereine, Unternehmen	1733	1821	1850	2003	2974	<b>7051</b>	3834	3217	<b>+ 4077<sup>1)</sup></b>	↑ ↑ ↑
Beratungen Privatpersonen	799	991	977	1065	1104	<b>853</b>	399	454	<b>-251</b>	⇒
Beschwerden	925	953	1103	1424	1707	<b>2708</b>	731	1977	<b>+ 1001</b>	↑ ↑
Bußgeld- verfahren	53	64	94	79	78	<b>104</b>	49	55	<b>+ 26</b>	⇒
„Datenpannen“	32	21	28	85	150	<b>1658</b>	92	1566	<b>+ 1508</b>	↑ ↑ ↑

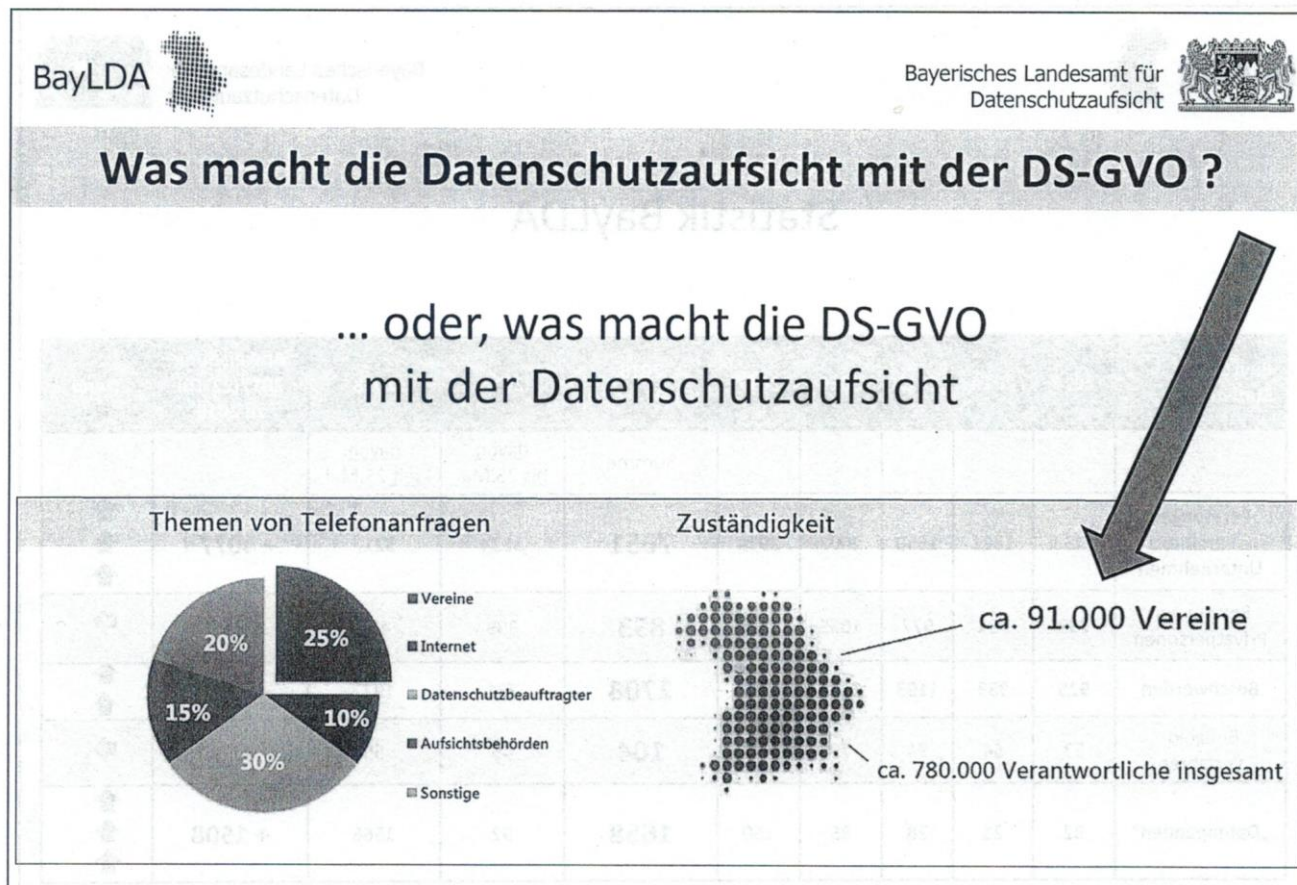
Stand: 22.10.2018

<sup>1)</sup> zzgl. Hotline

46/50



# Aktuelles



47/50





# Aktuelles

**... lassen Sie sich nicht  
verrückt machen ...**

**... bleiben Sie dem  
Ehrenamt treu, wir  
brauchen Sie!!**

48/50





# Ende

## Noch Fragen?

Datenschutz-T.E.  
Rechtsanwalt Thomas Engelhardt

Ochsenbuck 2  
91710 Gunzenhausen

Tel.: 09831 61 33 42  
Fax: 09831 61 31 13  
Mobil: 01525 59 60 86 9



E-Mail: [info@externer-datenschutzbeauftragter-bdsg.de](mailto:info@externer-datenschutzbeauftragter-bdsg.de)  
<https://externer-datenschutzbeauftragter-bdsg.de>



**Ende**

**Ende**



50/50