



Datenschutz in Vereinen

nach der neuen Europäischen Datenschutz-Grundverordnung







Agenda

- 1 Datenschutz was ist das?
- 2 Datenschutz was sagt die DS-GVO?
- 3 Umgang mit Bildern
- 4 Rolle und Aufgabe der Datenschutzaufsicht
- 5 Empfehlung zum Schluss





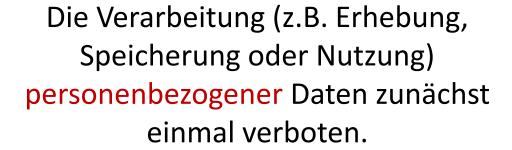
Warum sollte man die DS-GVO beachten?

Datenschutz ist Grundrechtsschutz



Verbot mit Erlaubnisvorbehalt

Hat Betroffener
Datenumgang
erlaubt?
Gibt es ein Gesetz
dafür?





Zulässig ist die Verarbeitung insbesondere nur, wenn eine Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.



. personenbezogene Daten

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





Welche personenbezogene Daten haben Vereine?

Vereinsmitglieder

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

Mitarbeiterdaten

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

Vereinsleben

- Webseite
- "Mannschafts"-bilder
- Vereinszeitung
- Mitgliederliste
- ... (und vieles mehr)

Betreute Menschen

- Gesundheitsdaten
- Krankenversicherung
- • •
- ... (und vieles mehr)





Artikel 4 Nr. 2 DS-GVO Begriffsbestimmungen

"Verarbeitung" [ist] jede mit oder ohne Hilfe automatisierter Verfahren ausgeführter 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;





Artikel 4 Nr. 2 DS-GVO Begriffsbestimmungen

"Verarbeitung" [ist] jede mit oder ohne Hilfe automatisierter

Verarbeitung ist... eigentlich alles







Verantwortlicher muss prüfen, ob er/sie Daten verarbeiten darf



Überlegung:

Habe ich für meine
Verarbeitung eine
Rechtsvorschrift,
die dies erlaubt oder
anordnet
oder hat der Betroffene
eingewilligt?





Agenda

- 1 Datenschutz was ist das?
- 2 Datenschutz was sagt die DS-GVO?
- 3 Umgang mit Bildern
- 4 Rolle und Aufgabe der Datenschutzaufsicht
- 5 Empfehlung zum Schluss



DS-GVO

Amtsblatt

L 119

der Europäischen Union



Artikel 99

Inkrafttreten und Anwends

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

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

Es ist eine Verordnung, die unmittelbar gilt.

(1) Text von Bedeutung für den EWR



ele Kechtzakten, deren 11tet in magerer Schrift gedruckt zind, handelt et zich um Kechtzakte der laufenden verwantung im Dereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

echtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakt





Für was und 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.





Für wen gilt DS-GVO?



Auch Verein ist "voll und ganz" von der neuen Datenschutz-Grundverordnung betroffen

... wie auch bisher schon vom Bundesdatenschutzgesetz!!





Wesentliche Anforderungen der DS-GVO

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



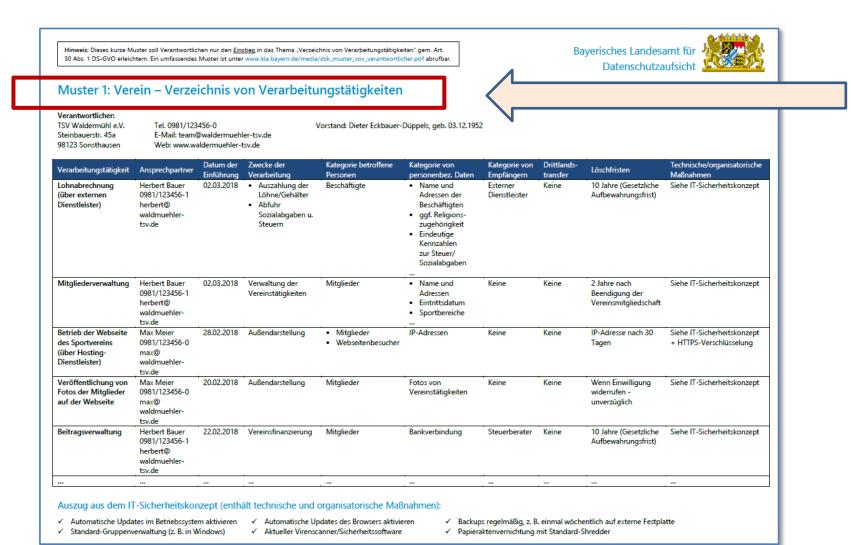


Verzeichnis der Verarbeitungstätigkeiten

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



Verzeichnis der Verarbeitungstätigkeiten







Wesentliche Anforderungen der DS-GVO

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





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



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

Satzung

- Vertrag
- Rechtliche Verpflichtung

(Mitteilung von Arbeitgeber an Sozialversicherung oder Finanzamt, Krankenkasse)

lebenswichtige Interessen

(Übermittlung der Blutwerte eines bewusstlosen Unfallopfers)

öffentliches Interesse

(Meldewesen, Sozialhilfe, Meldepflicht von Infektionskrankheiten)

berechtigte Interessen

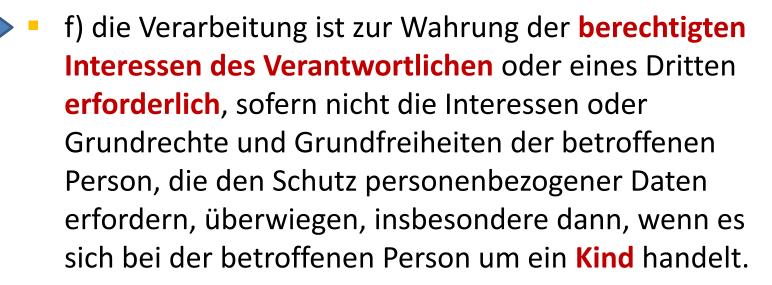






Rechtmäßigkeit bedeutet u.a.:

- (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
 - a) − e)







Rechtmäßigkeit (Art. 6 ff. DSGVO) bedeutet:

Wichtig:

Ausreichend ist eine Rechtsgrundlage.

Wenn Daten auf Grund von Vereinssatzung verarbeitet werden dürfen (Mitgliederverwaltung) oder Betreuungsvertrag (Hospiz) braucht es keine Einwilligung mehr!!





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



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





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.



Informationspflichten für Verein konkret:

- Bestandsmitglieder können "weiterlaufen"
- Mitgliedsanträge sollten angepasst werden
- Zwecke der Datenverarbeitung müssen festgelegt sein
- das berechtigte Interesse, sofern die Datenerhebung aufgrund eines berechtigten Interesses erfolgt, muss mitgeteilt werden
- ggf. die Empfänger(kategorien) mitteilen
- bei Übermittlung in Drittländer: die Arten verwendeter "Garantien" (z.B. Standarddatenschutzklauseln) benennen
- geplante Speicherdauer festlegen (evtl. sichern Chronik)
- die Betroffenenrechte (Auskunft, Löschung,...) benennen
- Beschwerderecht bei der Datenschutzaufsichtsbehörde





Informationspflichten für Verein konkret:

Umsetzungsmöglichkeiten: Aufnahmeantrag, Datenschutzordnung, Satzung, Info Mitgliederversammlung (Protokoll)



- Informationspflichten: Datenschutzerklärung:
- ... es muss beschrieben sein, was auf Webseite passiert
- BayLDA erarbeitet z.Zt. Orientierungshilfe für Webseiten und Datenschutzerklärungen



Informationspflichten für das Impressum:

Angaben gemäß § 5 TMG:

Verein e.V. Hauptstr. 1 12345 Musterstadt

Vertreten durch:

vertreten durch den 1. Vorstand Klaus Mustermann

Kontakt:

Telefon: 030/1234567-0 Telefax: 030/1234567-99 E-Mail: Vostand@verein.de

Registereintrag:

Registernummer: 12345 Registergericht: Musterstadt

Telemediengesetz (TMG) § 5 Allgemeine Informationspflichten

(1) Diensteanbieter haben für geschäftsmäßige, in der Regel gegen Entgelt angebotene Telemedien folgende Informationen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar zu halten

••••





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





- Sicherheit der Verarbeitung (Art. 32)
- Sind unter Berücksichtigung des Stands der Technik ... geeignete technische und organisatorische Maßnahmen getroffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; ...
 - Virenschutz
 - Firewall
 - Zugangskontrolle (Passwort, offene Ordner, nicht "Familien-PC)
 - Email
 - • • •
 - Umgang mit Gesundheitsdaten erfordert besondere Beachtung





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





Auftrags(daten)verarbeitung, Art 28

- Ist die Verarbeitung personenbezogener Daten "outgesourct"? (Webseite, Beitragseinzug, Werbeaktionen)
- Wenn Ja, gibt es dafür ausreichende Verträge zur Auftragsdatenverarbeitung ?
 (Muster siehe: <u>www.lda.bayern.de</u>)





Wesentliche Anforderungen der DS-GVO

- Verzeichnis der Verarbeitungstätigkeiten
- Anforderungen an die Datenverarbeitung
- Sicherstellung Betroffenenrechte
- 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

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





Wesentliche Anforderungen der DS-GVO

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



Bestellung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter <u>ist nach der DS-GVO zu</u> <u>benennen</u>, wenn

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder ...
 - Art. 9: ... religiöse oder weltanschauliche Überzeugungen oder ... Gesundheitsdaten
 - Kerntätigkeit
 - umfangreich





Bestellung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter ist nach BDSGzu benennen, wenn

- 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 – <u>absolute Ausnahme</u>).





Wesentliche Anforderungen der DS-GVO

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





Umgang mit Datenschutzverletzungen

Beispiele für Meldepflicht

Hacking

Verlust

Diebstahl

Fehlversand

Softwarefehler

Schadcode

Fehlentsorgung













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

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





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 sagt die DS-GVO?
- 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 Rechtsgrundlage (z.B. Einwilligung) der abgebildeten Person.





Handlungsempfehlungen: Umgang mit Bildern

Rechtmäßigkeit bedeutet u.a.:

- (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:
 - a) Die betroffene Person hat ihre Einwilligung gegeben
 - b) − e)
 - 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.





Handlungsempfehlungen: Umgang mit Bildern

- Verarbeitung von Bildern im Rahmen von Interessenabwägung ist möglich, aber nicht
 - bei Kindern,
 - von Bildern aus der Intimsphäre,
 - bei Arbeitnehmern (Rspr. BAG),
 - diskriminierenden Bildern (Party, Nacktphoto) und/oder
 - Bildern, die auf bes. Kategorien personenbezogener Daten hinweisen.





Handlungsempfehlungen: Umgang mit Bildern

- Dem Schutz der betroffene Personen ist hinreichend Rechnung zu tragen insbes. durch transparente Information und Widerspruchsmöglichkeit, z.B. durch
 - Hinweis, dass Fotos angefertigt werden,
 - für welchen Zweck Fotos gemacht werden,
 - ob, und wenn ja, wo Fotos veröffentlicht werden sollen und
 - an wen sich betroffene Person bei Datenschutzfragen wenden kann (Widerspruch, Löschung u.a.)





Handlungsempfehlungen: Einwilligung einholen



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.





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





... wer kümmert sich darum, dass Datenschutz eingehalten wird und wer kontrolliert?



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

Art. 4 Nr. 7: Begriffsbestimmungen

"Verantwortlicher" die natürliche oder juristische Person¹), 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;

¹⁾ e.V. ist juristische Person





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

Art. 4 Nr. 7: Begriffsbestimmungen

"Verantwortlicher"

ist der e.V.

vertreten durch den im Vereinsregister eingetragenen Vorstand



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

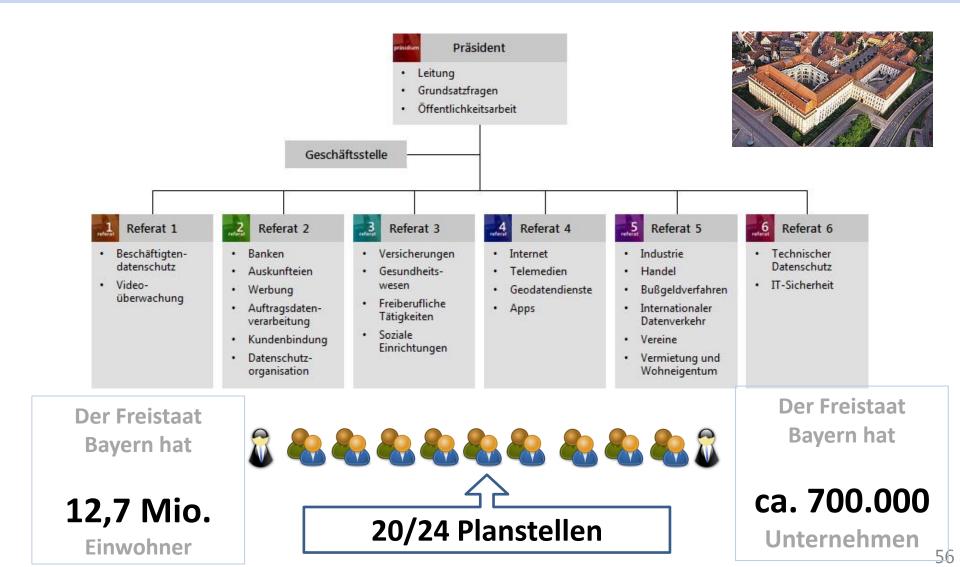


Sitz unserer Behörde ist **Ansbach**.

Wir nutzen die Räumlichkeiten der Ansbacher Residenz zusammen mit der Regierung von Mittelfranken.



Bayerisches Landesamt für Datenschutzaufsicht









Beschwerden

BayLDA





www.lda.bayern.de



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.

EU-Datenschutz-Grundverordnung

Ansbach, 29.05.2018

DSK veröffentlicht weiteres Kurzpapier

Die Datenschutzkonferenz(DSK) hat das Kurzpapier "Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO" veröffentlicht.



EU-Datenschutz-Grundverordnung

Ansbach, 30.04.2018

DSK veröffentlicht neues Kurzpapier

Die Datenschutzkonferenz(DSK) hat das Kurzpapier "Risiko für die Rechte und Freiheiten natürlicher Personen" veröffentlicht.



Hinweis: Meldung von Datenschutzbeauftragten

Ansbach, 18.05.2018

Meldeportal zur DSB-Mitteilung kurz vor Veröffentlichung

Verantwortliche müssen ab 25.05.2018 der Aufsichtsbehörde den eigenen Datenschutzbeauftragten (DSB) mitteilen. Das BayLDA bereitet hierfür einen Online-Service vor und bittet darum, von schriftlichen Meldungen abzusehen.



Pressemitteilungen

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.



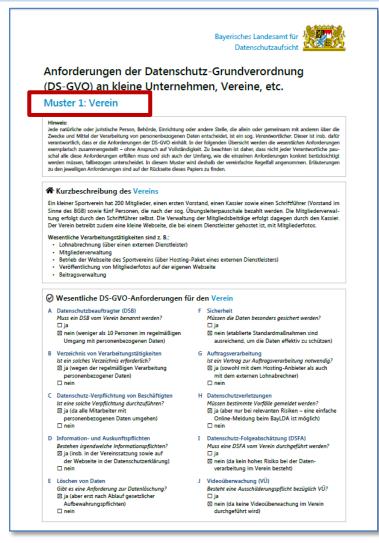


Unsere Handreichungen



... geht doch!!







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



Unsere Handreichungen



... geht doch!!





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 Mitgliedeverwaltung macht – "nicht ständig beschäftigt" ist dagegen bzyw, wer als Übungsteller nur mit den Namen seiner Mannschaft umgeht.

- → DSK-Kurzpapier Nr. 12: www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pd/
- 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.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- DSK-Kurzpapier Nr. 1: www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf
 DSK-Muster-Verzeichnis allgemein: www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf
- DSK-Muster-Verzeichnis angenient. www.tou.boyen.be/motorpusk_muster_vov_verantwortache.pd
- 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.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.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 beyw. Informationen auf der Homepage und der Satzung leicht zugänglich bereihalten. Die betroffenen Personen (z. B. Vereinsmitglieder) haben auch das Recht, Auskunft über der Verarbeitung ihrer Oten zu erhalten.

- → DSK-Kurzpapier Nr. 6: www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf
- DSK-Kurzpapier Nr. 10: www.lda.bayern.de/media/dsk_kpnr_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.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pd/
- F Sicherhe

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u.a. aktuelle Betriebsysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Vitenscanner und Benutzerrechte. Soweit private PCS genutzt werden, ist sicherzustlich, dass nur berechtigte Personen auf die Daten zugsreifen können.

- → BayLDA-Kurzpapier Nr. 1: www.lda.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.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf
- BayLDA-Formulierungshilfe zum Vertrag: www.lda.bayern.de/media/muster_adv.pdf
- H Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. 8. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Vereinsdaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenninis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

- BayLDA-Kurzpapier Nr. 8: www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf
- → BayLDA-Online-Service zur Meldung: www.lda.bayem.de/de/datenpanne.html
- I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein <u>hohes Risiko</u> 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.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf
- J Videoüberwachu

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.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf







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.lda.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.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf
- ⇒ DSK-Kurzpapier Nr. 1: www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf
- ⇒ DSK-Muster-Verzeichnis allgemein: www.lda.bayern.de/media/dsk_muster_vov_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.lda.bayern.de/media/info_verpflichtung_beschaeftigte_dsgvo.pdf





Bayerisches Landesamt für Datenschutzaufsicht



Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

TSV Waldermühl e.V. Tel. 0981/123456-0
Steinbauerstr. 45a E-Mail: team@waldermuehler-tsv.de
98123 Sonsthausen 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	Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern	Beschäftigte	Name und Adressen der Beschäftigten ggf. Religions- zugehörigkeit Eindeutige Kennzahlen zur Steuer/ Sozialabgaben	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	Name und Adressen Eintrittsdatum Sportbereiche	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	Mitglieder Webseitenbesucher	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
 ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
 ✓ Aktueller Virenscanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder





Agenda

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







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.lda.bayern.de



ITIL ISO 27001 **IT-GRUNDSCHUTZ** NOTFALLKONZEPT **TLS 1.2 SPIONAGE RSA** CLOUD FACEBOOK **BSI GRUNDSCHUTZ BCRYPT** METASPLOIT **BEDROHUNGSLAGE** XSS **EXPLOIT STARTTLS** IOS IPV4 DLP W3AF **SQL INJECTION** SCHWACHSTELLE **HACKER BYOD PRISM AES-256 ANDROID AWARENESS HACKTIVISMUS WAF TROJANER FORWARD SECRECY FIREWALL** APT **BOTNETZ IPSEC** DMZ **VPN PHISHING ZERO-DAY EXPLOIT NSA** IPV6 **IDS FIPS DATENSCHUTZ** ISIS12 **AUTHENTIFIZIERUNG OSCP BDSG IPS BACKDOOR HTTPS CSRF EV-ZERTIFIKAT DDOS MITM PGP SPOOFING BSI DIEBSTAHL CRIME ENISA CYBERSÖLDNER HYDRA BEAST TOMS MDM ROOTKIT APPS GOOGLE SPAM AKTENVERNICHTUNG** S/MIME WATERHOLE ATTACK PBKDF2 MD5 **JAVA QUANTENCOMPUTER** DARKNET **WINDOWS XP** NMAP **AUTORISIERUNG**