BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

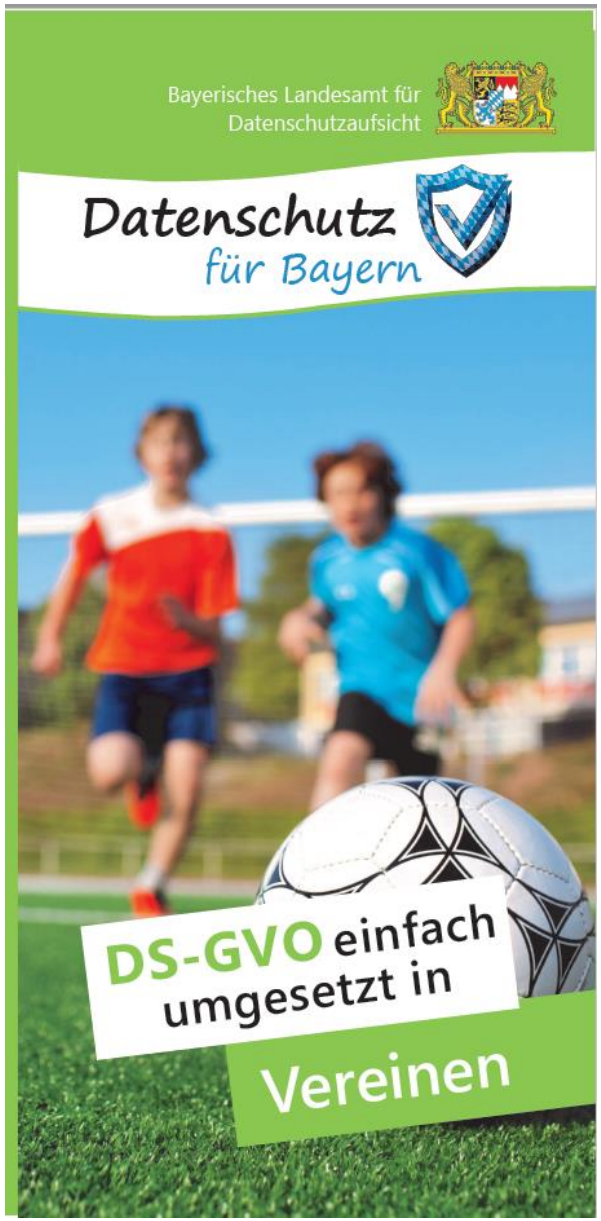
Datenschutz im Verein

- Anforderungen der DS-GVO -

Steinbach a. Wald, 25.10.2018

Alexander Filip,
Bayer. Landesamt für Datenschutzaufsicht

Unser neuer Flyer



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.

Hier kommt noch was

Hier steht schon was

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

Agenda

1. Datenschutz – was ist das?
2. DS-GVO – was bedeutet das?
3. DS-GVO und die Anforderungen für Vereine
4. Rolle und Aufgabe der Datenschutzaufsicht
5. Empfehlung zum Schluss

Agenda

1. **Datenschutz – was ist das?**
2. DS-GVO – was bedeutet das?
3. DS-GVO und die Anforderungen für Vereine
4. Rolle und Aufgabe der Datenschutzaufsicht
5. Empfehlung zum Schluss

Warum sollte man die DS-GVO beachten?

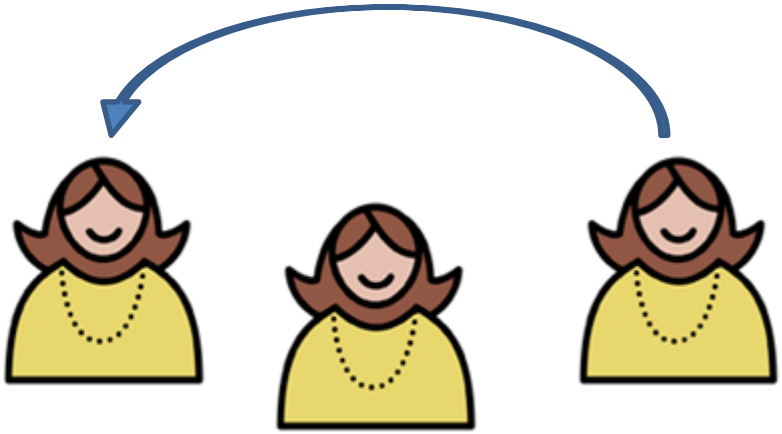
Datenschutz ist Grundrechtsschutz

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, ...)



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 Daten haben Vereine und kleine Unternehmen?

- **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**)

- **Kundendaten**
  - Name, Adresse
  - Kaufverhalten
  - …
  - … (**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;

Verarbeitung ist… eigentlich alles

Agenda

1. Datenschutz – was ist das?
2. **DS-GVO – was bedeutet das?**
3. DS-GVO und die Anforderungen für Vereine
4. Rolle und Aufgabe der Datenschutzaufsicht
5. Empfehlung zum Schluss

DS-GVO

Amtsblatt L 119
der Europäischen Union

Artikel 99

Inkrafttreten und Anwend

(1) Diese Verordnung tritt am zwanzigsten Tag nach ihrer Verö[illegible]chung im Amtsblatt der Europäischen Union in Kraft.

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

(1) 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.

Es ist eine Verordnung, die unmittelbar gilt.

5,50 EUR

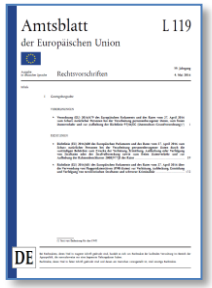
Ehmann / Kranig

Erste Hilfe zur Datenschutz-Grundverordnung

Zielgruppe:
Inhaber kleinerer Unternehmen; Vereinsvorsitzende; Datenschutzverantwortliche in kleineren Unternehmen und in Vereinen; datenschutzinteressierte Vereinsmitglieder.

Für was und für wen gilt die DS-GVO?

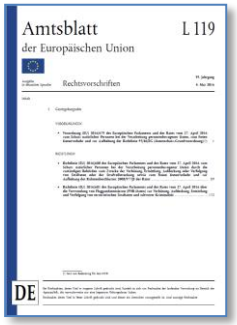
Für wen gilt DS-GVO?


Amtsblatt L 119
der Europäischen Union
Rechtsvorschriften
DE

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?


Amtsblatt L 119
der Europäischen Union
Rechtsvorschriften
DE

Auch Vereine und kleine Unternehmen sind „voll und ganz“ von der neuen Datenschutz-Grundverordnung betroffen

… wie auch bisher schon vom Bundesdatenschutzgesetz !!

… und was bedeutet das jetzt?

Agenda

1. Datenschutz – was ist das?
2. DS-GVO – was bedeutet das?
3. **DS-GVO und die Anforderungen für Vereine**
4. Rolle und Aufgabe der Datenschutzaufsicht
5. Empfehlung zum Schluss

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 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)

Bayerisches Landesamt für
Datenschutzaufsicht

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*

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.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.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, Virenscanner und Benutzerrechte. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen 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. 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.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf*
⇨ **BayLDA-Online-Service zur Meldung:** *www.lda.bayern.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-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 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.lda.bayern.de/media/dsk_kpnr_15_videoueberwachung.pdf*

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 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)

A Datenschutzbeauftragter (DSB)

Muss ein DSB vom Verein benannt werden?

☐ ja

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

Bestellung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter ist nach der DS-GVO zu benennen, 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 der DS-GVO zu benennen, wenn

Keine Pflicht zur Benennung eines Datenschutzbeauftragten nach DS-GVO

Bestellung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter ist nach BDSG zu 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 – absolute Ausnahme).

Bestellung eines Datenschutzbeauftragten

Zu den 10 Personen zählen nicht mit:

- Bereichsleiter im Sportverein (soweit dort nicht eigene Mitgliederverwaltung stattfindet),
- …

„ständig beschäftigt“

- d.h. überwiegender Anteil der Beschäftigung

Bestellung eines Datenschutzbeauftragten

Ein Datenschutzbeauftragter ist nach BDSG zu benennen, wenn

(in aller Regel) auch keine Pflicht zur Benennung eines Datenschutzbeauftragten nach BDSG

B Verzeichnis von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

☒ ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)

☐ nein

Verzeichnis der Verarbeitungstätigkeiten

Haben Sie einen Überblick darüber, welche personenbezogenen Daten bei Ihnen „verarbeitet“ werden ??

Verzeichnis der Verarbeitungstätigkeiten

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 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	• 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

Verzeichnis der Verarbeitungstätigkeiten

… verschaffen Sie sich einen Überblick, was in Ihrem Verein läuft und wer mit welchen Daten umgeht

C Datenschutz-Verpflichtung von Beschäftigten

Ist eine solche Verpflichtung durchzuführen?

☒ ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)

☐ nein

Datenschutz-Verpflichtung von Beschäftigten

DSK
DATENSCHUTZKONFERENZ

Kurzpapier Nr. 19

Unterrichtung und Verpflichtung von Beschäftigten auf Beachtung der datenschutzrechtlichen Anforderungen nach der DS-GVO

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Was regelt die Datenschutz-Grundverordnung (DS-GVO)?

Nach Art. 29 DS-GVO dürfen Beschäftigte eines Verantwortlichen (eines Unternehmens, eines Vereins, eines Verbands, eines Selbstständigen, einer Behörde usw.) oder eines Auftragsverarbeiters personenbezogene Daten ausschließlich auf Weisung des Verantwortlichen oder Auftragsverarbeiters verarbeiten, es sei denn, eine gesetzliche Regelung schreibt eine Verarbeitung dieser Daten vor.

Selbst wenn nach dem Wortlaut der DS-GVO nur die Beschäftigten eines Auftragsverarbeiters zu „verpflichten“ sind, trifft inhaltlich diese „verpflichtende Unterrichtung“ (im Folgenden: Verpflichtung) auch die Verantwortlichen und ihre Beschäftigten. Wie Verantwortliche diese gesetzliche Verpflichtung umsetzen (und ggfls. der Aufsichtsbehörde nachweisen), ist nicht verbindlich geregelt. Es wird empfohlen, dies in Form einer schriftlichen oder elektronischen Verpflichtungserklärung umzusetzen. Ein

Datenschutz-Verpflichtung von Beschäftigten

Anlage/Musterbeispiel für eine schriftliche Verpflichtung[1]:

Verpflichtung zur Vertraulichkeit und zur Einhaltung der datenschutzrechtlichen Anforderungen nach der Datenschutz-Grundverordnung (DS-GVO)

Frau/Herr

verpflichtet sich, personenbezogene Daten nicht unbefugt zu verarbeiten. Personenbezogene Daten dürfen daher nur verarbeitet werden, wenn eine Einwilligung vorliegt oder eine gesetzliche Regelung die Verarbeitung erlaubt oder vorschreibt. Die Grundsätze der DS-GVO für die Verarbeitung personenbezogener Daten sind zu wahren; sie sind in Art. 5 Abs. 1 DS-GVO festgelegt und beinhalten im Wesentlichen folgende Verpflichtungen[2]:

Personenbezogene Daten müssen

a) auf rechtmäßige und faire Weise, und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz");

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden („Zweckbindung");

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung");

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit");

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist („Speicherbegrenzung");

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit").

Personenbezogene Daten dürfen daher nur nach Weisung des Verantwortlichen verarbeitet werden. Neben Einzelweisungen der Vorgesetzten gelten als Weisung: Prozessbeschreibungen, Ablaufpläne, Betriebsvereinbarungen, allgemeine Dienstanweisungen sowie betriebliche Dokumentationen und Handbücher[3].

Verstöße gegen diese Verpflichtung können mit Geldbuße und/oder Freiheitsstrafe geahndet werden. Ein Verstoß kann zugleich eine Verletzung von arbeitsvertraglichen Pflichten oder spezieller Geheimhaltungspflichten darstellen. Auch (zivilrechtliche) Schadenersatzansprüche können sich aus schuldhaften Verstößen gegen diese Verpflichtung ergeben. Ihre sich aus dem Arbeits- bzw. Dienstvertrag oder gesonderten Vereinbarungen erge-

[1] Soweit die Verschwiegenheit von Beschäftigten im öffentlichen Bereich gesetzlich oder tariflich ausdrücklich geregelt ist, muss eine solche Verpflichtung nicht erfolgen.
[2] Der Inhalt der Verpflichtung ist im Einzelfall anzupassen. So können bestimmte Aufgaben und Tätigkeiten zusätzliche Unterrichtungen erfordern, etwa zum Beschäftigten- oder Sozialdatenschutz, zum Telekommunikationsgeheimnis usw.
[3] Die Aufzählung ist im Einzelfall anzupassen. So können weitere Unterlagen Weisungscharakter haben oder aufgezählte Typen für einzelne Verantwortliche nicht von Bedeutung sein.

bende Vertraulichkeitsverpflichtung wird durch diese Erklärung nicht berührt.

Die Verpflichtung gilt auch nach Beendigung der Tätigkeit weiter.

Ich bestätige diese Verpflichtung. Ein Exemplar der Verpflichtung habe ich erhalten.

Ort, Datum	Unterschrift des Verpflichteten	Unterschrift des Verantwortlichen

Muster für Verpflichtung der Beschäftigten;

kann auch für Funktionäre verwendet werden

D Information- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

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

☐ nein

Informations- und Auskunftspflichten

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.

Informations- und Auskunftspflichten

- **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.

Informations- und Auskunftspflichten

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

u.a.

Informations- und Auskunftspflichten

- **Informationspflichten für Verein konkret:**

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

u.a.

Informations- und Auskunftspflichten

- **Informationspflichten: Datenschutzerklärung:**

- … es muss beschrieben sein, was auf **Webseite** passiert

- BayLDA erarbeitet z.Zt. Orientierungshilfe

Gut für die Orientierung, was geht

Informations- und Auskunftspflichten

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

.....

Informations- und Auskunftspflichten

- **Betroffenenrechte (Auszug)**
  - **Recht auf Auskunft**
  - Recht auf Berichtigung
  - Recht auf Löschung
  - Recht auf Widerruf einer Einwilligung

E Löschen von Daten

Gibt es eine Anforderung zur Datenlöschung?

☒ ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)

☐ nein

Löschen

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.

F Sicherheit

Müssen die Daten besonders gesichert werden?

☐ ja

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

Sicherheit der 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)
  - .
  - **Umgang mit Gesundheitsdaten erfordert besondere Beachtung**

G Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

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

☐ nein

Auftragsverarbeitung

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

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

Auftragsverarbeitung

- **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: www.lda.bayern.de)

H Datenschutzverletzungen

Müssen bestimmte Vorfälle gemeldet werden?

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

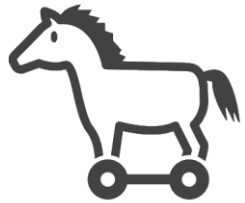
☐ nein

Datenschutzverletzungen

Datenschutzverletzungen (Art. 33)

Beispiele für Meldepflicht

- **Hacking**
- **Verlust**
- **Diebstahl**
- **Fehlversand**
- **Softwarefehler**
- **Schadcode**
- **Fehlentsorgung**
- **Vernichtung Verlust**
- **Sonstiges?**



72 Stunden

Datenschutzverletzungen

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

I Datenschutz-Folgeabschätzung (DSFA)

Muss eine DSFA vom Verein durchgeführt werden?

☐ ja

☒ nein (da kein hohes Risiko bei der Daten-verarbeitung im Verein besteht)

Datenschutz-Folgenabschätzung

Datenschutz-Folgenabschätzung und vorherige Konsultation

Artikel 35
Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko** für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche …

Datenschutz-Folgenabschätzung

… kaum vorstellbar, dass das für „normale Vereine“ (wie z.B. Sport- oder Kulturverein) relevant werden kann

J Videoüberwachung (VÜ)

Besteht eine Ausschilderungspflicht bezüglich VÜ?

☐ ja

☒ nein (da keine Videoüberwachung im Verein durchgeführt wird)

Videoüberwachung

- **Rechtmäßigkeit der Videoüberwachung (Art. 6):**

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

  - a) – 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.

… und was sonst noch zu beachten ist

… Mitgliederverwaltung

… Umgang mit Bildern

… Sanktionen

… und was sonst noch zu beachten ist

… Mitgliederverwaltung

… Umgang mit Bildern

… Sanktionen

Anforderungen für Mitgliederverwaltung

- **Häufige Frage:**
  Brauche ich eine Einwilligung, um die Daten meiner Mitglieder zu verwalten?

- **Klare Antwort: NEIN**

Anforderungen für Mitgliederverwaltung

- **Rechtmäßigkeit (Art. 6 ff. DSGVO) bedeutet:**
  - Einwilligung
  - Vertrag
  - …
  - …
  - berechtigte Interessen

Satzung

Anforderungen für Mitgliederverwaltung

- **Rechtmäßigkeit bedeutet u.a.:**

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

  - a) – 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.

… und was sonst noch zu beachten ist

… Mitgliederverwaltung

… Umgang mit Bildern

… Sanktionen

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**.

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.

Umgang mit Bildern

- Verarbeitung von Bildern im Rahmen von **Interessen-abwägung** ist möglich; Schutzinteresse der betroffenen Personen überwiegt in jedem Fall bei

  - von Bildern aus der Intimsphäre,
  - diskriminierenden Bildern (Party, Nacktphoto) und/oder
  - Bildern, die auf bes. Kategorien personenbezogener Daten hinweisen.

Sonderfall:

- Bilder von Arbeitnehmern (Rspr. BAG),

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.)

BayLDA

Einwilligung
ist nicht immer
erforderlich

und

Widerspruch
klappt auch
nicht immer

Umgang mit Bildern

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.

Homepage BayLDA

FAQ zur DS-GVO

Bayerisches Landesamt für Datenschutzaufsicht

Frage	**Was muss ein Verein im Zusammenhang mit der Erstellung und Veröffentlichung von Bildern beachten?**
Stichworte	Bilder, Verein, Chronik
Norm	Art. 38 BayDSG; Art. 6 Abs. 1 Buchstabe a, b und f DS-GVO
Antwort	Das Aufnehmen, Speichern und Veröffentlichen von Bildern, auf denen natürliche Personen enthalten sind, wird in der Datenschutz-Grundverordnung unter dem einheitlichen Begriff „Verarbeiten" zusammengefasst. Für die Frage der Rechtmäßigkeit der Verarbeitung ist zu unterscheiden, ob der Verein die Bilder zu journalistischen, künstlerischen oder literarischen oder aber zu sonstigen Zwecken verarbeitet. **1. Erstellung und Veröffentlichung von Bildern zu journalistischen, künstlerischen oder literarischen Zwecken (Art. 38 BayDSG)** Gemäß Art. 38 BayDSG gelten bei der Verarbeitung personenbezogener Daten zu journalistischen, künstlerischen oder literarischen Zwecken - vereinfacht gesagt - nur die Vorschriften zum Datengeheimnis und zur Datensicherheit (Medienprivileg). Alle übrigen Vorschriften zum Datenschutz gelten nicht. Das bedeutet konkret, dass z.B. die Regelungen zur Rechtmäßigkeit der Verarbeitung oder zu Betroffenenrechten nicht zu berücksichtigen sind.

… und was sonst noch zu beachten ist

… Mitgliederverwaltung

… Umgang mit Bildern

… Sanktionen

… und wenn es daneben geht?

Sanktionen

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. DS-GVO – was bedeutet das?
3. DS-GVO und die Anforderungen für Vereine
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?

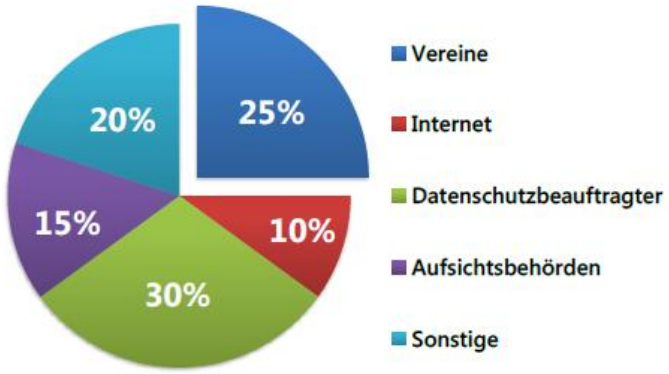
Sitz unserer Behörde ist
Ansbach.

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

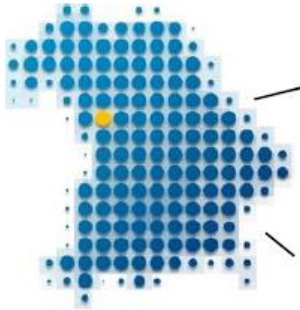
Was macht die Datenschutzaufsicht mit der DS-GVO ?

… oder, was macht die DS-GVO mit der Datenschutzaufsicht

Themen von Telefonanfragen



Zuständigkeit



ca. 91.000 Vereine

ca. 780.000 Verantwortliche insgesamt

Bayerisches Landesamt für Datenschutzaufsicht

Präsident
- Leitung
- Grundsatzfragen
- Öffentlichkeitsarbeit

Geschäftsstelle

1 Referat 1
- Beschäftigten-datenschutz
- Video-überwachung

2 Referat 2
- Banken
- Auskunfteien
- Werbung
- Auftragsdaten-verarbeitung
- Kundenbindung
- Datenschutz-organisation

3 Referat 3
- Versicherungen
- Gesundheits-wesen
- Freiberufliche Tätigkeiten
- Soziale Einrichtungen

4 Referat 4
- Internet
- Telemedien
- Geodatendienste
- Apps

5 Referat 5
- Industrie
- Handel
- Bußgeldverfahren
- Internationaler Datenverkehr
- Vereine
- Vermietung und Wohneigentum

6 Referat 6
- Technischer Datenschutz
- IT-Sicherheit

Der Freistaat Bayern hat

12,7 Mio.

Einwohner

24 Planstellen

Der Freistaat Bayern hat

ca. 700.000

Unternehmen

Was macht die Datenschutzaufsicht mit der DS-GVO ?

… oder, was macht die DS-GVO mit der Datenschutzaufsicht

BayLDA Statistik	2013	2014	2015	2016	2017	2018 (01.01-17.09)	2018	2018	Abweichung 2017 zu 2018	Trend
						Summe	davon bis 25.Mai	davon seit 25.Mai		
Beratungen Vereine, Unternehmen	1733	1821	1850	2003	2974	**6629**	3834	2795	**+ 3655** [1)]	
Beratungen Privatpersonen	799	991	977	1065	1104	**772**	399	373	**-332**	
Beschwerden	925	953	1103	1424	1707	**2229**	731	1498	**+ 522**	
Bußgeld-verfahren	53	64	94	79	78	**82**	49	33	**+ 4**	
„Datenpannen“	32	21	28	85	150	**1231**	92	1139	**+ 1081**	

Stand:18.09.2018

[1)] **zzgl. Hotline**

Beschwerden

www.lda.bayern.de

- Hotline für Vereine
- Häufig gefragt
- Beschwerde einreichen
- Datenpanne melden
- DSB melden

Facebook Custom Audience

VG Bayreuth entscheidet: Facebook-Verfahren „Custom Audience" ist ohne Nutzer-Einwilligung unzulässig.

Weitere Informationen

DSK-Webseite

Das BayLDA betreut zukünftig die erste gemeinsame Webseite der deutschen Datenschutzkonferenz (DSK).

Weitere Informationen

Datenschutzverletzung

Mitteilungen nach Artikel 33 DS-GVO können über den neuen Online-Service eingereicht werden.

Weitere Informationen


Bayerisches Landesamt für
Datenschutzaufsicht
Suche...
Hotline für Vereine
Häufig gefragt
Beschwerde einreichen
Datenpanne melden
DSB melden

Kleine Unternehmen und Vereine

Handreichungen zur DS-GVO-Umsetzung

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**

5,50 EUR

Ehmann / Kranig

Erste Hilfe zur Datenschutz-Grundverordnung

Zielgruppe:
Inhaber kleinerer Unternehmen; Vereinsvorsitzende; Datenschutzverantwortliche in kleineren Unternehmen und in Vereinen; datenschutzinteressierte Vereinsmitglieder.

… lassen Sie sich nicht verrückt machen …

… bleiben Sie dem Ehrenamt treu, wir brauchen Sie!!


… und für weitere Fragen …
Hotline des BayLDA
0981-531810
bis 30.10.2018

BayLDA

Bayerisches Landesamt für Datenschutzaufsicht

Vielen Dank für Ihre Aufmerksamkeit

Alexander Filip, Bayer. Landesamt für Datenschutzaufsicht

www.lda.bayern.de