

Datenschutz im Verein

5 Jahre DSGVO – Zeit für ein Resümee

Überprüfung der getroffenen Maßnahmen

(DSGVO = Datenschutz-Grundverordnung)

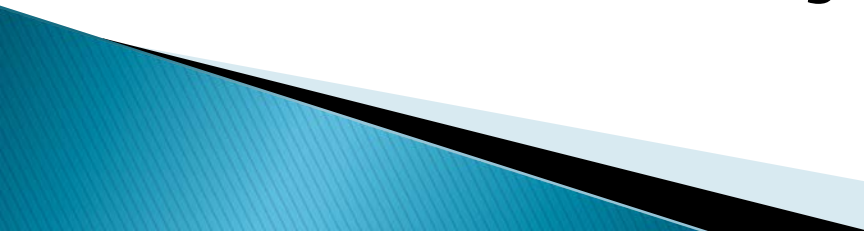
Kurze Vorstellung

- ▶ **Matthias Müller**
- ▶ **Information Security Officer bei Siemens seit 2005**
- ▶ **Seit über 30 Jahren ehrenamtlich in verschiedenen Organisationen tätig**
 - **Bayerische Sportjugend (bsj) Unterfranken,**
 - **DJK Sportverband Unterfranken**
 - **DJK Salz**
 - **Rhönklub Zweigverein Salz**

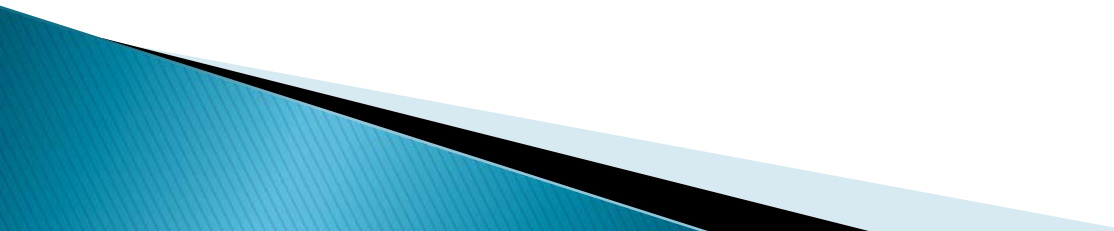
Wichtige Information!!!

- ▶ Ich bin kein Jurist
- ▶ Infoveranstaltung – keine Rechtsberatung
- ▶ Weitergabe von eigenen Erfahrungen bzw. eigenem Wissen
- ▶ Danke für Verwendung von Unterlagen:
 - Herrn Büchler, Deutscher Wanderverband
 - Herrn Kranig, ehem. Präsident Bayer. Landesamt für Datenschutzaufsicht (BayLDA)

5 Jahre DSGVO – Resümee

- ▶ Riesen Hype 2018 mit großer Verunsicherung
 - ▶ In den Vereinen nicht immer nachhaltig umgesetzt
 - ▶ Durch hohe Fluktuation von Ehrenamtlichen → regelmäßige Infos notwendig
 - ▶ Zeit nehmen zum Prüfen, denn Einhaltung von gesetzlichen Anforderungen
 - ▶ Bisher keine Strafen gegen Vereine bekannt, aber ...
- 

Agenda

- ▶ Ein paar Grundlagen müssen sein
 - ▶ 10 Punkte Plan zur Überprüfung der getroffenen Maßnahmen
 - ▶ Fragen?
- 

Grundlagen

»» Ein bisschen Theorie muss sein

Grundlagen

- ▶ Datenschutzgesetz sollen den Einzelnen davor schützen, dass er durch Umgang mit seinen personenbezogenen Daten in seinen Persönlichkeitsrechten beeinträchtigt wird
- ▶ Umsetzung von EU-Recht 2018 mit Neuordnung und teilweiser Verschärfung des alten Rechts (BDSG), das in der Vergangenheit viele sorglos „ignoriert“ haben
- ▶ Alle Vereine betroffen als „Verarbeiter“ von personenbez. Daten; Vereine gleichgestellt wie „Unternehmen“; „Verantwortlicher“ unabhängig von der Rechtsform
- ▶ Kein Unterschied zwischen Hauptberuf oder Ehrenamt
- ▶ Nicht Schutz von Daten („Datensicherheit“), sondern ausschließlich zum Schutz der Persönlichkeitsrechte

Rechtmäßigkeit

- Grundsätzlich keine Datenverarbeitung ohne Einwilligung oder andere Rechtsgrundlage

Rechtsgrundlagen, für die keine Einwilligung erforderlich ist:

- Verarbeitung von Daten, die zur Vertragserfüllung notwendig sind (Art. 6 Abs. 1 lit. b. DSGVO)
- „zur Wahrung berechtigter Interessen des Verantwortlichen“ (Art. 6 Abs. 1 lit. f. DSGVO)

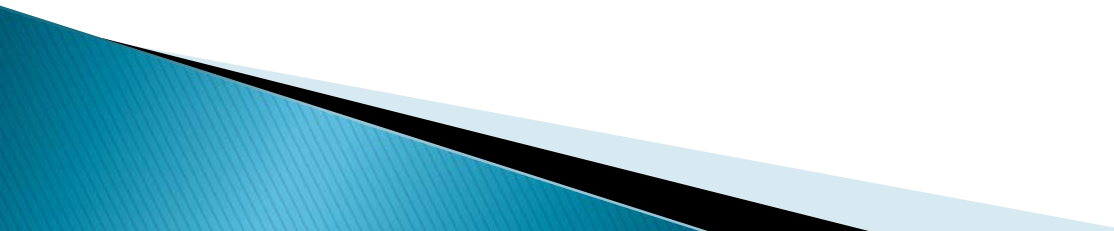


Zum Beispiel:

Mitglied im BLSV

Mitglied im Deutschen Wanderverein

Grundsätze

- Treu und Glauben: Geschützt werden müssen alle Daten über die persönlichen oder sachlichen Verhältnisse, die einer bestimmten Person (Betroffener) zugeordnet werden können
 - Transparenz: Rechenschaftspflicht gegenüber der zuständigen Aufsichtsbehörde und dem Betroffenen
 - Zweckbindung: nur für vorher konkret festgelegte Zwecke
 - Datensparsamkeit: nur notwendige und begründete Daten
 - Speicherbegrenzung, Integrität, Vertraulichkeit: Daten müssen sachlich richtig sein, aktualisiert werden, sicher gespeichert werden und auch wieder gelöscht werden
- 

IT-Sicherheit

- ▶ Technische Maßnahmen (derzeit gültige Standards) zur Verbesserung des Datenschutzes
- ▶ IT-Sicherheit durch aktuelle Hard- und Software
- ▶ Pseudonymisierung und Verschlüsselung
- ▶ Regelmäßige Backups
- ▶ Sichere Kommunikation speziell mit elektronischen Medien



Empfehlung: 10 Punkte Plan

»» Haben wir alles umgesetzt?

Übersicht

10 Punkte-Plan zur Umsetzung der DSGVO

1. Handlungsbedarf überprüfen
2. Internet-Auftritt – alles umgesetzt?
3. Aktuelles Verfahrens-Verzeichnisses
4. Beitrittserklärung aktuell?
5. Überprüfen der Satzung/eigene Datenschutzordnung
6. Verpflichtung auf das Datengeheimnis
7. Info über Datenschutz-Verantwortlichen/Beauftragten
8. Verträge zur Auftrags-Datenverarbeitung
9. Organisation der Auskunftspflicht
10. Meldung eines Vorfalles – wenn es denn mal passiert

1. Maßnahme

Handlungsbedarf überprüfen

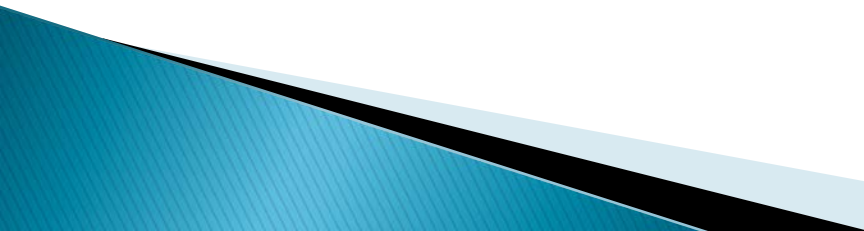
Inventur der Datenverarbeitung

- ▶ Welche Daten werden im Verein erfasst?
- ▶ Wer hat Zugriff auf die Daten?
- ▶ Zu welchem Zweck werden die Daten erhoben?
 - Mitgliederverwaltung, Beitragswesen
 - Meldung an Verbände
 - Versenden von Informationen an Mitglieder
 - Passwesen/Spielerlisten
 - Whatsapp-Gruppen zur Erreichbarkeit
 - Datenerfassung für spez. Vereinsveranstaltungen (Vereinsausflug, Zeltlager, ...)

Dokumentieren aller Aktivitäten

z.B. Datenschutzordner für alle Aktivitäten anlegen

Beispiel eines Inhaltsverzeichnis

1. Datenschutzverantwortlicher (im Regelfall Vereinsvors.)
 2. Verfahrensverzeichnis – in jedem Fall!!!
 3. Datenschutzordnung / Satzung
 4. Muster Beitrittserklärung
 5. Wie erfolgen Mitgliederinformationen
 6. Mitarbeiterinformationen (Verpflichtungserklärungen)
 7. Verträge zur Auftrags-Datenverarbeitung (wenn erforderlich)
 8. Vordruck für Auskunftsformular
- 

Löschfristen festlegen

...

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.

2. Maßnahme

Internet-Auftritt – alles umgesetzt?

Homepage prüfen

- ▶ Datenschutzerklärung auf der HP einstellen
- ▶ Punkt Datenschutz immer zugänglich
- ▶ Ggfs. Hinweis auf verwendete Cookies, bzw. Analyse-SW (z.B. Google-Analytics) – auch von Provider!
- ▶ Ggfs. Hinweis auf Übertragung von personenbezogenen Daten nur verschlüsselt (Verwendung von HTTPS)
- ▶ Impressum DSGVO-konform
- ▶ Gilt auch für Facebook oder andere soziale Medien!!!
- ▶ Muster-Datenschutzerklärung → z.B. Verband / Internet
Die Datenschutzerklärung muss individuell angepasst werden!

Beispiel BLSV

 Sicher | https://www.blsv.de/fileadmin/user_upload/pdf/Datenschutz/Datenschutzerklaerung_Website_DSGVO_BLSV_20180321.pdf

IMPRESSUM

Anbieter: Bayerischer Landes-Sportverband e.V.

Georg-Brauchle-Ring 93, 80992 München

Tel: 089 / 15 702-0,

Fax: 089 / 15 702-444

E-Mail: info@blsv.de

Sitz:

Amtsgericht München VR 4210

Umsatzsteueridentifikationsnummer:

DE 129 51 39 05

Präsident:

Jörg Ammon

Vertretungsberechtigter Vorstand (§ 26 BGB):

Jörg Ammon, Peter Rzytki, Klaus Drauschke, Bernd Kränzle, Harald Stempfer

Verantwortlich im Präsidium:

Jörg Ammon


Präsident

Verantwortlich i.S. des Presserechts:

Thomas Kern

Geschäftsführer, Pressechef

thomas.kern@blsv.de

 Sicher | <https://www.blsv.de/blsv>

- Hinweis auf Cookies ?
- Hinweis auf Analyse-SW ?

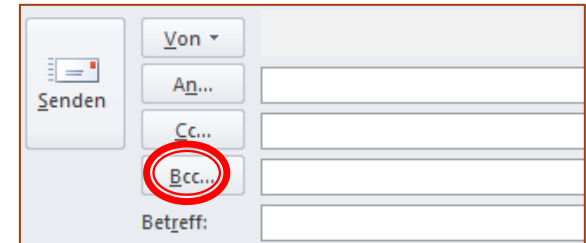
Hier ein Beispiel



Wir benutzen Cookies zur Erleichterung des Umgangs mit unserer Website und für Statistiken Google und Piwik Scripts. [zeige Details](#)

E-Mail/Newsletter überarbeiten

- ▶ Mails mit mehreren Empfängern nicht in An/CC sondern in BCC
- ▶ Anhänge mit sensiblen Daten verschlüsseln
- ▶ Mails mit sensiblen Daten (z.B. Bewerbungen) nach Frist löschen
- ▶ Kein unaufgeforderter Newsletter-Versand ohne Einwilligung
- ▶ Löschmöglichkeit anbieten
- ▶ Impressum ist im Newsletter Pflicht



3. Maßnahme

Aktualisieren des Verfahrens-
Verzeichnisses

Verfahrens-Verzeichnis

- ▶ Verschiedene Formen möglich, auch tabellarisch
- ▶ Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
- ▶ Konzept für Löschung der Daten
- ▶ Bei Kontrollen/Beschwerden ist es wichtig, hier etwas vorweisen zu können

| Verfahrensmeldung gemäß Art. 30 DSGVO | |
|--|---|
| Deutscher Naturschutzring e.V. (DNR) | Tafel 1 |
| <p>► Mit diesem Dokument meldet die verantwortliche Stelle Verfahren, mit denen personenbezogene Daten verarbeitet werden, zur Aufnahme in das Verzeichnis von Verarbeitungstätigkeiten.</p> <p>► Diese neue Version entspricht den Vorgaben der DSGVO und dient zugleich als Grundlage zur datenschutzrechtlichen Prüfung und Bewertung der Verfahren im Rahmen der Datenschutz-Folgenabschätzung gem. Art. 30 DSGVO durch den Datenschutzbeauftragten.</p> <p>► Die Felder in dem Abschnitt A sind von der jeweiligen Fachabteilung auszufüllen.</p> <p>► Die Felder in dem Abschnitt B werden vom Datenschutzbeauftragten bearbeitet.</p> <p>► Bitte beachten: Auf einzelnen IT-Anwendungen können auch mehrere Verfahren zum Einsatz kommen. Für jedes Verfahren ist jeweils eine Meldung vorgesehen. Abzustellen ist auf das Verfahren und nicht auf die IT-Anwendung.</p> <p>► Die beizufügenden Anlagen sind zu nummerieren und aufzulisten.</p> <p>► Die meldenden Stellen sind zusammen mit dem beteiligten Fachbereich für die Vollständigkeit der Meldungen und deren Richtigkeit verantwortlich.</p> <p>► Ändern sich die Angaben zum Verfahren (z.B. Zweckbestimmung, Datenkategorie, berechtigte Empfänger, Zugriffsberechtigungen, Änderungen Dienstleister oder Standorte, etc.), ist eine aktualisierte Meldung an den Datenschutzbeauftragten zu senden.</p> | |
| Status der Verfahrensmeldung <input checked="" type="checkbox"/> Vorläufig Datum der Meldung 06.11.2017 <input type="checkbox"/> Final Datum der Meldung | |
| A. Angaben zum Verfahren | |
| 1. Basisinformationen zum Verfahren | |
| 1.1 Name und Anschrift der verantwortlichen Stelle | Deutscher Naturschutzring e.V. (DNR) Merkenstraße 19-20, 10117 Berlin |
| 1.2 Name des Verfahrens | Kurzfassung: Lohnabrechnung Langfassung: |
| 1.3 Version / Stand des Verfahrens | 1 |
| 1.4 Name der Fachabteilung | StBf Verwaltung/Buchhaltung |
| 1.5 Angaben zum Melder (Haupt-Ansprechpartner zum Verfahren) | XXXXXX |
| 1.6 Verantwortliche Führungskraft | XXXXXX |
| 1.7 Datenschutz-Ansprechpartner/-koordinator für den Datenschutzbeauftragten | Anja Nowak (Büroleitung) Tel.: 0304676 1776 - 914 E-Mail: anja.nowak@dnr.de |
| <small>DNA GmbH, Version 2.0, 10/2017, nur zur internen Verwendung</small> | |

- ▶ Muster Verzeichnis

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.km.bayern.de/media/04_muster_vom_verantwortlichen.pdf abrufbar.

Bayerisches Landesamt für
Datenschutzaufsicht 

Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher: TSV Waldermühl e.V., Steinbauerstr. 43a, 98123 Sonsthausen
Tel. 0981/123456-0, E-Mail: team@waldermuehler-tsv.de, Web: www.waldermuehler-tsv.de
Vorstand: Dieter Eckbauer-Düppel, geb. 03.12.1952

| Verarbeitungstätigkeit | Anspruchspartner | Datum der Einführung | Zwecke der Verarbeitung | Kategorie betroffene Personen | Kategorie von personenbez. Daten | Kategorie von Empfängern | Drittlands-transfer | Löschfrist | Technische/organisatorische Maßnahmen |
|--|--|----------------------|--|-------------------------------|--|--------------------------|---------------------|---|---------------------------------------|
| Lohnabrechnung (über externen Dienstleister) | Herbert Bauer 0981/123456-1 herbert@waldmuehler-tsv.de | 02.03.2018 | <ul style="list-style-type: none"> Aufzahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern | Beschäftigte | <ul style="list-style-type: none"> Name und Adresse der Beschäftigten ggf. Religionszugehörigkeit Einzelne Kennzahlen zur Steuer/ Sozialabgaben | Externer Dienstleister | Keine | 10 Jahre (Gesetzliche Aufbewahrungspflicht) | Siehe IT-Sicherheitskonzept |
| Mitgliederverwaltung | Herbert Bauer 0981/123456-1 herbert@waldmuehler-tsv.de | 02.03.2018 | Verwaltung der Vereinstätigkeiten | Mitglieder | <ul style="list-style-type: none"> Name und Adresse Eintrittsdatum Sportbereiche | Keine | Keine | 2 Jahre nach Beendigung der Vereinsmitgliedschaft | Siehe IT-Sicherheitskonzept |

Muster-Verzeichnis

Hinweis: Dieses kurze Muster soll Verantwortlichen nur den Einstieg in das Thema „Verzeichnis von Verarbeitungstätigkeiten“ gem. Art. 30 Abs. 1 DS-GVO erleichtern. Ein umfassendes Muster ist unter www.lida.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf 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@waldermuehler-tsv.de | 02.03.2018 | <ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern | Beschäftigte | <ul style="list-style-type: none"> Name und Adressen der Beschäftigten ggf. Religionszugehörigkeit Eindeutige Kennzahlen zur Steuer/ Sozialabgaben | Externer Dienstleister | Keine | 10 Jahre (Gesetzliche Aufbewahrungsfrist) | Siehe IT-Sicherheitskonzept |
| Mitgliederverwaltung | Herbert Bauer 0981/123456-1 herbert@waldermuehler-tsv.de | 02.03.2018 | Verwaltung der Vereinstätigkeiten | Mitglieder | <ul style="list-style-type: none"> 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@waldermuehler-tsv.de | 28.02.2018 | Außendarstellung | <ul style="list-style-type: none"> 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@waldermuehler-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@waldermuehler-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 Virens Scanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

4. Maßnahme

Beitrittserklärung aktuell?

Infos auf der Beitrittserklärung

- ▶ Bestandsmitglieder vor 2018 können „weiterlaufen“
- ▶ Erstellen einer Datenschutzerklärung für die Beitrittserklärung
 - Welche Daten werden zu welchem Zweck erfasst?
 - Individuell anpassen und veröffentlichen
z.B. in Vereinszeitschrift informieren, Info Mitglieder-
versammlung (Protokoll)
- ▶ Foto- und Filmerlaubnis gleich mitregeln

Muster- Datenschutzbestimmungen

Ich willige ein, dass der oben genannte Verein als verantwortliche Stelle, die in der Beitrittserklärung erhobenen personenbezogenen Daten wie Name, Vorname, Geburtsdatum, Adresse, E-Mail-Adresse, Telefonnummer, Funktion im Verein und Bankverbindung (.....) ausschließlich zum Zwecke der Mitgliederverwaltung, des Beitragseinzuges und der Übermittlung von Vereinsinformationen durch den Verein, evtl. weitere Zwecke) und für alle in der Satzung genannten Zwecke verarbeitet und genutzt werden. Eine Übermittlung von Daten an übergeordnete Institutionen und (evtl. Stelle nennen) findet nur im Rahmen der in der Satzung festgelegte Zwecke statt. Diese Datenübermittlungen sind notwendig zum Zwecke des Vereins.

Eine Datenübermittlung an Dritte außerhalb der (evtl. Stellen nennen) findet nicht statt. Eine Datennutzung für Werbezwecke findet ebenfalls nicht statt. Bei Beendigung der Mitgliedschaft werden die personenbezogenen Daten gelöscht, soweit sie nicht entsprechend der gesetzlichen Vorgaben aufbewahrt werden müssen. Jedes Mitglied hat im Rahmen der Vorgaben der Datenschutzgrundverordnung (DSGVO) und des Bundesdatenschutzgesetzes n.F. (DSAnpUG EU) das Recht auf Auskunft über die personenbezogenen Daten, die zu seiner Person bei der verantwortlichen Stelle gespeichert sind. Außerdem hat das Mitglied, im Falle von fehlerhaften Daten, ein Korrekturrecht.

Beschwerdestelle ist das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) Promenade 27
91522 Ansbach

Ort, Datum Unterschrift des Mitglieds/ gesetzlichen Vertreters

Einverständniserklärung zur Veröffentlichung von Fotos und Filmaufnahmen

Ich willige ein, dass im Rahmen von Veranstaltungen und Sportbetrieb (weitere Zwecke?) angefertigte Foto- und Filmaufnahmen für Veröffentlichungen, Berichte, in Printmedien, Neuen Medien und auf der Internetseite des Vereines und seinen übergeordneten Verbänden unentgeltlich verwendet werden dürfen.

Eine Verwendung der Aufnahmen für andere als die beschriebenen Zwecke oder ein Inverkehrbringen durch Überlassung der Aufnahme an Dritte außer der Dachorganisation (evtl. Ergänzungen) des Vereins ist unzulässig.

Diese Einwilligung ist freiwillig. Durch eine nicht erteilte Einwilligung entstehen mir als Mitglied keine Nachteile. Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden.

Ort, Datum Unterschrift des Mitglieds/ gesetzlichen Vertreters

5. Maßnahme

Überprüfen der Satzung/
eigene Datenschutzordnung

Satzung / Datenschutzordnung

- ▶ Verantwortlicher für den Datenschutz
→ i.d.R. Vorsitzender
- ▶ Bestellung eines Datenschutz-Beauftragten (wenn notwendig)
- ▶ Details besser in einer eigenen Datenschutzordnung regeln, z.B.
 - Welche Daten werden erfasst?
 - Zugriff auf Daten
 - Löschfristen festlegen
 - Geplante Speicherdauer festlegen (evtl. sichern für Chronik)
 - Zwecke der Datenverarbeitung müssen festgelegt sein
 - Die Betroffenenrechte (Auskunft, Löschung, ...) benennen
 - Beschwerderecht bei der Datenschutzaufsichtsbehörde
- ▶ Muster-Datenschutzordnung (bei Verbänden / im Internet)

6. Maßnahme

Verpflichtung auf das
Datengeheimnis

Verpflichtung auf das Datengeheimnis

- ▶ Info aller Mitarbeiter (auch ehrenamtliche), die mit personenbezogenen Daten arbeiten
- ▶ Datenschutzverpflichtung der Mitarbeiter muss nachweisbar sein, aber nicht zwingend schriftlich
→ z.B. unterschriebene Teilnehmerliste

- ▶ Muster-Datenschutzverpflichtung

Muster Datenschutzverpflichtung

Anlage/Musterbeispiel für eine schriftliche Verpflichtung¹:

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 Verpflichtungen¹:

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 Handbücher².

Verstöße gegen diese Verpflichtung können mit Geldbußen und/oder Freiheitsstrafe beahndet werden. Ein Ver-

bindende 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**

Sicherheit der Datenverarbeitung

- ▶ Info aller Mitarbeiter, die mit personenbezogenen Daten arbeiten
- ▶ Hinweis auf technische und organisatorische Maßnahmen zum sicheren Umgang, z.B.
 - Virenschutz, Firewall, Passwortsafe
 - Zugangskontrolle (Passwort, keine offenen Ordner, nicht „Familien-PC“)
 - Löschpflichten von ausgeschiedenen Mitarbeitern
 - Backups, Zugangsdaten sicher hinterlegen
- ▶ **Umgang mit Gesundheitsdaten erfordert besondere Beachtung!**

7. Maßnahme

Datenschutzverantwortlicher
/ Beauftragter

Datenschutz–Beauftragter notwendig?

Ein Datenschutzbeauftragter ist nach BDSG zu benennen, wenn

- ▶ mindestens 10 Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind (§38 Abs. 1 Satz 1 BDSG–neu)
- ▶ Daten verarbeiten, die wegen eines hohen Risikos für die betroffenen Personen eine Datenschutz–Folgenabschätzung erfordern (§38 Abs. 1 Satz 2 BDSG–neu –absolute Ausnahme)

Die gute Nachricht!!!

Zu den 10 Personen **zählen nicht** mit:

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

„ständig beschäftigt“

- ▶ D.h. überwiegender Teil der Beschäftigung

Herr Kranig, BayLDA

8. Maßnahme

Auftragsverarbeitung

Vertrag zur Auftrags- Datenverarbeitung

- ▶ Für wen müssen Verträge abgeschlossen werden?
 - Internet-Provider
 - Externe Lohnabrechnung
 - Andere externe Partner, z.B. Versender Vereinszeitung
- ▶ Muster-Vertrag

GDD - Arbeitskreis „Datenschutz-Praxis“

Hinweise: Der nachstehende Mustertext soll eine Orientierungshilfe bieten. Er ist je nach den Umständen des konkreten Einzelfalls anzupassen. Bei komplexen Auftragsverhältnissen oder der Verarbeitung sensibler personenbezogener Daten im Auftrag werden weitere bzw. ergänzende Vertragsklauseln notwendig sein.

Die einzelnen schriftlichen Festlegungen nach § 11 Abs. 2 Nr. 1 bis Nr. 10 BDSG sollten vollständig in die Vereinbarung übernommen und wie eine Checkliste abgearbeitet werden. Die für das konkrete Dienstleistungsverhältnis zutreffenden Alternativen sollten angekreuzt werden. Leerfelder sind ggf. entsprechend des konkreten Auftrags auszufüllen.

Muster: Auftrag gemäß § 11 BDSG

Vereinbarung

zwischen dem / der

.....
- nachstehend Auftraggeber genannt -

und dem / der

.....
- nachstehend Auftragnehmer genannt -

1. Gegenstand und Dauer des Auftrags

Gegenstand des Auftrags

- Der Gegenstand des Auftrags ergibt sich aus der Leistungsvereinbarung / SLA / vom, auf die hier verwiesen wird (im Folgenden Leistungsvereinbarung).

oder

- Gegenstand des Auftrags zum Datenumgang ist die Durchführung folgender Aufgaben durch den Auftragnehmer:

..... (Definition der Aufgaben)

Verträge für Auftragsverarbeitung

- ▶ Auftragsverarbeiter auf Musterverträge ansprechen, sind oftmals vorbereitet
- ▶ Banken sind keine Auftragsverarbeiter (unterliegen der Bankenaufsicht)
- ▶ Nicht nötig bei Rechtsanwälten, Steuerberatern oder Wirtschaftsprüfern (haben Prüfpflicht)
- ▶ Auftragnehmer außerhalb der EU möglichst vermeiden, weil Anforderungen viel höher

Vertrag mit Dachverband nötig?

? **Müssen mit dem BLSV und den zugehörigen Sportfachverbänden AV-Verträge abgeschlossen werden?**

Zwischen dem BLSV als Dachverband und seinen Mitgliedsvereinen sind keine Auftragsverarbeitungsverträge erforderlich. Dies ergibt sich insbesondere aus § 59 der BLSV-Satzung, da der BLSV die Daten zu eigenen Zwecken verarbeitet und nicht weisungsgebunden im Auftrag seiner Mitgliedsvereine ist.

Im Verhältnis zwischen den lokalen Sportvereinen und deren Verbände (als Vereinszusammenschlüsse), wie dem BLSV oder den Sportfachverbänden, liegen regelmäßig keine Sachverhalte einer Auftragsverarbeitung vor. Die Weitergabe von Mitgliederdaten dorthin stellt eine Datenübermittlung dar und die Verarbeitung bei den Verbänden erfolgt unabhängig sowie eigenverantwortlich. Rechtsgrundlagen für diese Datenübermittlungen an die Verbände sind meist in den Beitrittserklärungen der BLSV-Sportvereine enthaltene Einwilligungen oder Satzungsregelungen bei den Sportvereinen, die die Mitglieder mit dem Beitritt anerkennen.

Erforderliche Bedingung dafür ist, dass die Vereinsverantwortlichen im Rahmen ihrer Informationspflichten gemäß Art. 13 und 14 DSGVO die betroffenen Personen z.B. im Rahmen einer Datenschutzordnung/ Datenschutzerklärung beim Beitritt über die satzungsgemäße (verpflichtende) Weitergabe an den BLSV informieren (siehe Vorlage „Muster Datenschutzerklärung Verein „ im BLSV-Cockpit.

9. Maßnahme

Auskunftspflicht vorbereiten

Auskunftspflicht vorbereiten

- ▶ Welche Auskunft muss vom Verein mit welcher Qualität und in welcher Zeit zur Verfügung gestellt werden?
- ▶ Wie ist der Prozess im Verein geregelt?

Aus BLSV-Unterlagen

Betroffenenrechte sicherstellen

- ▶ Auf Auskunftersuchen nach Art. 15 DSGVO vorbereiten
- ▶ Müssen unverzüglich (spätestens innerhalb eines Monats) erfüllt werden
- ▶ Überprüfen, ob alle Daten korrigiert und gelöscht werden können
- ▶ Musterschreiben vorbereiten

Deutscher Wanderverband
Kassel, [Empfänger]

Deutscher Wanderverband
130 Jahre engagiert für Wanderwege
www.zeichen-setzen-pro-hiesem.de

Erteilung der Auskunft nach Art 15 DSGVO

Sehr geehrte/r [Auskunftsverberin],

1. Ihren Antrag auf Auskunft nach Art 15 DSGVO haben wir am [Datum] erhalten. Sie haben darin Ihre Identität ausreichend nachgewiesen.
2. (Bei einer Beantwortung innerhalb der gesetzlichen Frist) Innerhalb der gesetzlichen Frist von einem Monat kommen wir hiermit Ihrem Antrag nach. (Bei Fristverlängerung nach Art. 12 Abs. 3 DSGVO) Wie mit Schreiben vom [Datum] mitgeteilt, haben wir aufgrund [entsweder Komplexität des Antrages oder Anzahl Ihrer Anträge, nähere Begründung notwendig] die Möglichkeit zur Fristverlängerung auf drei Monate in Anspruch genommen.
3. (falls keine Daten verarbeitet werden) Es werden keine Daten zu Ihrer Person verarbeitet. (Dann weiter mit Textbaustein Nr. 9). (Wenn Daten verarbeitet werden) Wir verarbeiten folgende Daten zu Ihrer Person: [es folgt eine Liste mit den konkret verarbeiteten Daten]. Ausdrücke der relevanten Datenverarbeitungen finden Sie im Anhang.
4. Diese werden zu folgenden Zwecken verarbeitet: [Zwecke einschließlich Rechtsgrundlagen aufzählen]
5. (falls Daten weitergegeben werden) Die Daten werden an folgende Empfänger übermittelt: [Empfänger bzw Empfängerkategorien einschließlich ihrem Sitzland aufzählen]. (falls Daten in ein Drittland übermittelt werden) Die Übermittlung der Daten an jene Empfänger, die sich in einem Drittland befinden, basiert auf folgenden Garantien: [Garantien ergänzen]
6. Wir speichern Ihre Daten [Dauer oder zumindest Kriterien für Speicherdauer angeben].

Kassel, _____
Deutscher Wanderverband
Kleine Rosenstraße 1-3
34117 Kassel
Telefon 05 61 9 38 73-0
Telefax 05 61 9 38 73-10
info@wanderverband.de
www.wanderverband.de

Bankverbindung:
Volkbank Odenwald eG
Konto 1 805 484 012 508635 930
IBAN: DE00 5086 3533 0001 8056 81
BIC: GEMODE33WIC

Verband Deutscher Gebirgs- und Wandervereine e.V.
kurz: Deutscher Wanderverband

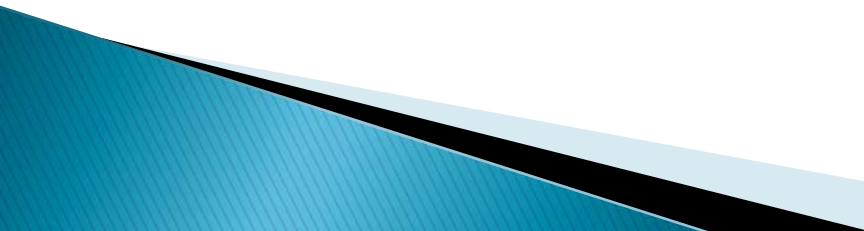
10. Maßnahme

Meldung eines Vorfalls

Erkennen eines Vorfalls

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

Meldung eines Vorfalls

- ▶ Beispiele: USB-Stick mit Mitglieder-daten verloren / unverschlüsseltes Laptop mit personenbezogenen Daten im Zug vergessen, Großer Mailverteiler in CC, Hacker-Angriff / Schadsoftware
 - ▶ Müssen der Aufsichtsbehörde und den Betroffenen gemeldet werden
 - ▶ Meldung eines Vorfalles innerhalb von 72 Stunden
 - ▶ Kontaktdaten griffbereit im Datenschutzordner
- 

Meldestelle

Aufsichtsbehörde für Bayern

Bayerisches Landesamt für Datenschutzaufsicht (BayLDA)

Promenade 27, 91522 Ansbach

E-Mail: poststelle@lda.bayern.de

Telefon: 0981 / 53-1300



Und zum Schluss ...

Es geht nicht um Angst zu schüren!

Bleiben Sie dem Ehrenamt treu!

Quellenangaben

»» Informationen zum Nachlesen

Flyer Datenschutzerfordernungen

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

Zentrale Datenschutzhemen



Unser Webangebot für Sie:



Mehr Informationen unter

www.lida.bayern.de

HERAUSGEBER

Bayerisches Landesamt für Datenschutzaufsicht
Promenade 27 (Schloss)
91522 Ansbach

Bayerisches Landesamt für
Datenschutzaufsicht



Datenschutz für Bayern



Bayerisches Landesamt für
Datenschutzaufsicht



Flyer Datenschutzerfordernngen

Zielgruppe dieses Flyers



Der Fokus dieses Flyers liegt auf **kleinen Vereinen**.

Die genannten Datenschutzerfordernngen 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 zwanzig 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.

Empfohlene Quellen

- ▶ Bayerisches Landesamt für Datenschutzaufsicht (Hrsg.):
Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine. (5,50 €)
- ▶ Der Beauftragte für den Datenschutz Baden-Württemberg: Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO). Informationen über die datenschutzrechtlichen Rahmenbedingungen beim Umgang mit personenbezogenen Daten in der Vereinsarbeit. (kostenlos)
- ▶ Datenschutzbeauftragten des Landes einfach bei Fragen anrufen



Verwendete Quellen

- ▶ Unterlagen deutscher Wanderverband
Folien Sven Büchler
- ▶ Unterlagen Bayer. Landesamt für Datenschutzaufsicht
Folien Thomas Kranig und www.lida.byern.de
- ▶ Unterlagen BLSV → Vereins-Cockpit
- ▶ Bayernsport