BUND DEUTSCHER AMATEURTHEATER E.V.
Bundesgeschäftsstelle • Lützowplatz 9 • 10785 Berlin
Fon 030 – 2639859 0 berlin@bdat.info
Fax 030 – 2639859-19 www.bdat.info

Praxistipps

So setzen Vereine die EU – Datenschutzverordnung um

Sie führen ehrenamtlich einen Verein? Sie haben nicht viel Zeit? Dennoch gilt auch für Ihren Verein: ab 25. Mai ist die EU – DSGVO anzuwenden. Um sich möglichst rechtssicher und dennoch mit leistbaren Arbeitsschritten in der Datenschutzwelt zu bewegen, hat der BDAT eine Handlungsempfehlung zusammengestellt.

1. Online - Website EU-DSGVO-gerecht anpassen

- **Datenschutzbestimmungen aktualisieren**

Ihre Website ist das „Fenster nach draußen“, durch das die Welt auch hineinschauen kann. Und findige Abmahnvereine oder „Nicht-Wohlgesinnte“ sehen ab dem 25. Mai, ob die neue Datenschutzverordnung angewendet wird. Bevor es zur Anzeige bei der zuständigen Datenschutzbehörde kommt: Erstellen Sie mit dem Administrator Ihrer Seite eine EU-DSGVO-gerechte Datenschutzerklärung für die Website. Jede Website verwendet andere Tools oder Erfassungsinstrumente, es gibt deshalb keine „allgemeine“ Datenschutzerkärung, die für alle richtig ist.

Einige Hinweise, die die neue Datenschutzerklärung – je nach Gestaltung - enthalten muss:

- Hinweis auf Analyse- und Statistikanwendungen (z. B. Piwik oder Google-Analytics) mit optionalem Opt-Out (Anklickmöglichkeit, dass der Besucher nicht erfasst werden möchte)
- Sie nutzen Social-Media-Plugins (Facebook, Instagram etc.)? Nicht ohne Hinweis in der Datenschutzerklärung!
- Hinweis auf den Umgang mit Kontaktdaten aufnehmen
- Interaktionsmöglichkeiten auf Websites in der Datenschutzerklärung Ihrer Website festhalten

Eine Mustervorlage gibt es hier (die entsprechend angepasst werden muss):

https://www.datenschutz.org/datenschutzerklaerung-muster.pdf

Zum Erstellen Ihrer angepassten Datenschutzerklärung können Sie kostenlose Generatoren im Internet zur Hilfe ziehen, in der Suchmaschine dafür „EU DSGVO Datenschutzerklärung Generator“ eingeben, zwei Beispiele:

https://datenschutz-generator.de/

https://www.activemind.de/datenschutz/datenschutzhinweis-generator/

- **SSL-Verschlüsselung**

Wichtig ist zudem, dass die Website Verschlüsselungsverfahren anwendet (SSL) und falls sie Formulare verwendet, müssen hier ausführliche Datenschutzhinweise eingebaut werden oder aber die Formulare von der Website entfernt werden.

- **Cookies**

Fast alle Webseiten verwenden Cookies. Diese sind dazu da, Nutzer wiederzuerkennen und ihnen das Surfen auf einer Website zu erleichtern, etwa dadurch, dass der Nutzer seine Zugangsdaten nicht bei jedem Besuch neu eingeben muss oder erkannt wird, was der Nutzer bereits gekauft hat. Sie sollten den Nutzer beim ersten Seitenaufruf über das Verwenden von Cookies und sein Widerspruchsrecht (Cookie Banner) informieren.

Weitere Hinweise hierzu: https://www.e-recht24.de/artikel/datenschutz/8451-hinweispflicht-fuer-cookies.html

- **Formulare**

Alle Formulare, z. B. Kontaktformular, Bestellformular, die online ausgefüllt werden, benötigen eine verpflichtende Checkbox, wo der Benutzer über den Datenschutz aufgeklärt wird und er diesen akzeptieren muss.

- **Newsletter**

Wenn Sie einen Newsletter versenden, achten Sie darauf, dass die Anmeldungen über ein sogenanntes **„Double-opt-in"-Verfahren** gesendet wurden. Altbestände ggf. anschreiben, löschen und um Neuanmeldung bitten.

Das Anmeldeformular für Ihren Newsletter darf **nur ein Pflichtfeld** enthalten: die E-Mail-Adresse.

Rechtliche **Mindestvorgaben** in Newsletter E-Mails: Impressum, Abmeldelink, Link zur Datenschutzerklärung.

Haben Sie ein Newsletter-Anmeldeformular auf der Website, ist es ratsam unter den Button zur Newsletter-Anmeldung einen kurzen **Hinweistext** zu schreiben, der den Nutzer darüber aufklärt, was mit den Daten passiert und die Datenschutzerklärung verlinkt.

Haben Sie einen **Vertrag zur Auftragsdatenverarbeitung** mit Ihrem Dienstleister geschlossen?

Weitere Hinweise gibt es z. B. hier:

https://www.newsletter2go.de/whitepaper/eu-dsgvo/

- **Blogs**

Zusätzlich zu den unter „Website" genannten Aktualisierungen müssen **Kommentarfunktionen** einen Datenschutzhinweis berücksichtigen.

Weitere Infos zum Thema hat eine Bloggerin z. B. hier eingestellt:

https://chris-tas-blog.de/dsgvo-betrifft-auch-blogger-datenschutzverordnung/

2. Offline - Verzeichnis über Verarbeitungstätigkeiten anlegen

Die Datenschutzverordnung sieht vor, nur wirklich absolut notwendige Daten zu verarbeiten (Prinzip der Datenknappheit). Jeder Verein muss sich die Frage stellen: Was wird wo warum gespeichert u. verarbeitet, wer hat Zugriff darauf und überlegen, ob Speicherung und Zugriff wirklich in diesem Umfang notwendig ist. Aus diesen Überlegungen heraus wird das „Verzeichnis über die Verarbeitungstätigkeiten“ erstellt. Ein gut verständliches Muster stellt z.B. der Bayerische Datenschutzbeauftragte zur Verfügung:

https://www.lda.bayern.de/de/kleine-unternehmen.html

Auch hier gilt: der Vereins muss es nach den individuellen Gegebenheiten befüllen

3. Informationspflichten nachkommen

Durch den Beitritt eines Mitgliedes entsteht eine vertragsähnliche Beziehung, die den Verein berechtigt, Daten zu verarbeiten.
Nach §13 u. 14 EU DSGVO ist der Verein aber auf alle Fälle verpflichtet, auch die Vereinsmitglieder (bisherige und neue!) über erhobene Daten zu informieren. Dies geschieht in einer Datenschutzinformation/Datenschutzhinweis, die den Mitgliedern übergeben oder zugesendet wird.
Ein individuell noch anzupassendes Muster für Vereine hat der Landessportbund Nordrhein-Westfalen auf seiner Seite veröffentlicht:

http://www.vibss.de/vereinsmanagement/recht/datenschutz/

unter Musterschreiben – Informationspflichten nach Art. 13 u. 14 EU DSGVO

4. Daten sicher aufbewahren, Verpflichtungserklärungen einholen und prüfen: Datenschutzbeauftragter notwendig?

Was selbstverständlich klingt, muss überprüft werden: sind die Daten sicher vor dem Zugriff von außen? Welche technisch-organisatorischen Maßnahmen (kurz: TOM) ergreift der Verein, dass kein unberechtigter Zugriff erfolgt? Passwortschutz, geschützter Bereich auf einem PC, in verschlossenem Raum? Wie stellt der Verein sicher, dass nicht personenbezogene Daten auf einem Stick landen und dieser verloren geht? Diese Maßnahmen sollten auch im Verzeichnis Verarbeitungstätigkeiten (s. 2.) aufgeführt werden

Wichtig ist, die Personen im Verein, die berechtigten Zugriff auf Daten haben, eine Vertraulichkeitserklärung unterzeichnen zu lassen.

Ein solches Musterschreiben zu „Verpflichtung zur Wahrung der Vertraulichkeit und zur Beachtung der datenschutzrechtlichen Regelungen“ findet sich auf der Seite des Sportbundes NRW.

http://www.vibss.de/vereinsmanagement/recht/datenschutz/

Datenschutzbeauftragter (DSB): Nicht bei allen Vereinen wird das der Fall sein, aber, bei manchen eben schon. Durch die zusätzliche nationale „Aufsattelung“ des Bundesdatenschutzgesetzes (BDSG) gilt wie im bisherigen Gesetz auch ab 25. Mai weiterhin: falls mehr als 9 Personen regelmäßig Daten verarbeiten (d.h. auch darauf Zugriff haben!), besteht die gesetzliche Pflicht eine geeignete, fachkundige Person als Datenschutzbeauftragte*n intern zu berufen oder extern zu beauftragen . Das gilt nicht nur für Unternehmen, sondern auch für ehrenamtliche Vereine. „Regelmäßig“ muss dabei nicht täglich oder wöchentlich sein, sondern kann auch eine längere Intervalle bedeuten.

Weiterführende Hinweise in der Broschüre der Bundesdatenschutzbeauftragten (pdf):

https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO6.html

5. Einwilligung von Personen zur Datenspeicherung einholen

Ihr Verein hat einen Email- oder Postverteiler, um z.B. regelmäßig zu Vorstellungen einzuladen? Falls keine „vertragsähnliche Bindung“, also eine Mitgliedschaft im Verein vorliegt, gilt: auch hier müssen Sie dokumentieren können, dass Sie die Einwilligung der Personen besitzen, denen diese personenbezogenen Daten gehören. Lassen Sie sich die Einwilligung schriftlich bestätigen mit einem Formular, dem Sie ergänzend Datenschutzhinweise beilegen. Wie der BDAT selbst die Personen in seinen Verteilern informiert und versucht, Einwilligungen einzuholen, sehen Sie hier in zwei Entwurfsformularen:

Entwurf_Einwilligungserklärung.doc
BDAT_Datenschutzhinweise_Ausschreibungen.doc

6. Daten löschen - Löschkonzept

Schließlich gilt: Alle personenbezogenen Daten, für die keine vertragsähnliche Bindung wie Mitgliedschaft vorliegt, oder für die Sie von den betroffenen Personen keine Einwilligung vorliegenhaben, müssen Sie löschen. Sie haben kein Recht, sie zu verarbeiten, zu speichern.

Mittel- und langfristig muss der Verein ein Löschkonzept anlegen: wann werden Daten gelöscht - wenn Mitglieder ausgetreten sind? Datenschutzgrundsätze müssen außerdem in einer Datenschutzordnung des Vereins niedergelegt werden.

Hierzu informieren wir noch.

Hinweise:

Dokumentieren Sie Ihre Datenschutzaktivitäten. Sie sind verpflichtet nachzuweisen, dass Sie die Daten rechtmäßig verarbeiten.

Musterformulare können die Arbeit erleichtern. In jedem Fall müssen Vereine sie aber an ihre eigenen Gegebenheiten anpassen.

Bitte beachten Sie: Dies ist eine Handlungsempfehlung mit Stand vom 15.05.2018 und stellt keine Rechtsberatung dar. Der BDAT übernimmt keine juristische Gewähr für die Richtigkeit oder Vollständigkeit der Angaben und der Links.

Neue Umsetzungsauslegungen der EU DSGVO könnte es auch in der Zukunft geben. Bitte informieren Sie sich auch bei den Datenschutzbeauftragten Ihres Bundeslandes:

https://www.bfdi.bund.de/DE/Infothek/Anschriften_Links/anschriften_links-node.html

Auch unsere Mitgliedsverbände im BDAT informieren auf ihren Websites über die neuen Regelungen:

https://bdat.info/der-verband/mitglieder/mitgliedsverbaende/

Stand: 15. Mai 2018