25 JAHRE
Erfahrung - Kompetenz - Solidarität
SELBSTHILFE
Mecklenburg-Vorpommern e.V.

„Gemeinsames Haus“
Henrik-Ibsen-Straße 20

18106 Rostock

Tel: 03 81 - 7 69 03 40
03 81 - 7 69 12 35
Fax: 03 81 - 7 69 12 36

e-mail: rostock@lagsb-mv.de
homepage: www.lagsb-mv.de

Handreichung zur Einführung der

EU-Datenschutzgrundverordnung

(EU-DSGVO)

am 25.5.2018

für die Vereine der Selbsthilfe in Mecklenburg-Vorpommern

Herausgegeben von der SELBSTHILFE MV e.V. Stand: 07.05.2018

Verfasser: Christian Engelen

Vorwort:
Viele Vereine der Selbsthilfe fragen sich derzeit, welche Pflichten ihnen in Bezug auf den Datenschutz nach Inkrafttreten der neuen EU-DSGVO (DatenSchutzGrundVerOrdnung) und des neuen BDSG (BundesDatenSchutzGesetz) obliegen. Einige der hier bislang häufiger eingegangenen Fragen sollen daher nachfolgend in Form einer Frage und Antwortsammlung beantwortet werden. In der Anlage finden Sie zu den geforderten Unterlagen einige Beispiele und Vordrucke. **Sollten Sie in Ihren Gruppen und Vereinen Schulungsbedarf zu diesem Themengebiet sehen, teilen Sie uns dies bitte kurzfristig mit.**
Bitte beachten Sie die **Fragen 4, 6, 9, 11, 12 und 13!**

Grundlegend sollten Vorstände auf folgendes achten:

1. **Noch vor dem 25.05.2018 (Betrifft Internetauftritte und Drucksachen)**
    a. Fügen Sie eine DSGVO konforme **Datenschutzerklärung** zur Website an **prominenter** Stelle, z.B. als eigener neuer Menüpunkt im Hauptmenü oder direkt auf der Startseite hinzu. (Muster in der Anlage)
    b. Enthält Ihr Internetauftritt die Möglichkeit, persönliche Daten einzugeben (z.B. ein Kontaktformular, Newsletteranmeldung oder ähnliches): Reduzieren Sie die abgefragten Daten auf das Notwendigste und bauen Sie eine VOR dem Absenden der Daten zu bestätigende Abfrage ein, dass der Interessent die **Datenschutzerklärung** gelesen und akzeptiert hat.
    c. „Entrümpeln“ Sie generell die Internetauftritte und Drucksachen. Prüfen Sie, ob zu allen Fotos/Videos/Veröffentlichungen die notwendigen Einwilligungen der Abgebildeten/Genannten schriftlich vorliegen, andernfalls entfernen Sie die Medien vorsorglich oder holen zeitnah eine **Einwilligung** ein und legen diese zu Ihrer **Dokumentation** ab.
    d. Nutzen Sie Auswertungsdienste wie beispielsweise Google Analytics und/oder Sozial Media Plugins von Facebook, Twitter oder anderen? Stellen Sie sicher, dass diese entweder entfernt oder so in Ihren Webauftritt eingebaut sind, dass diese keine Daten ohne Zustimmung erheben und übertragen.
2. **Schnellstmöglich**
    a. Wenn die Internetseite/Website von einem Dritten bereitgestellt oder verwaltet wird (z.B. Strato, 1und1 oder ähnliche) sorgen Sie dafür, kurzfristig eine DSGVO konforme **Auftragsverarbeitungsvereinbarung** (Siehe Muster in der Anlage) mit diesem abzuschließen.
    b. Prüfen und dokumentieren Sie, wer Zugang zu und Zugriff auf die Daten des Vereins hat. Klären Sie intern, ob der Zugriff in dieser Form (noch) notwendig ist und ob diejenigen, die rechtmäßig Daten erhalten, auch nur die Daten bekommen, die Sie benötigen.
    c. Erstellen Sie kurzfristig die notwendigen Dokumentationen (**Verfahrensverzeichnis, Technisch/Organisatorische Maßnahmen**…) (Vorlagen zur Anpassung in der Anlage)
3. **Generell**
    a. Geben Sie die Daten nicht an Dritte weiter – es sei denn, Sie haben die schriftliche Einwilligung der betroffenen Person oder es basiert auf gesetzlichen Notwendigkeiten.
    b. Halten Sie die IT aktuell und orientieren Sie sich an den üblichen Sicherheitsstandards (regelmäßige Backups auf externe Medien, Firewall, Virenscanner, passwortgeschützter Zugang, evtl. Festplattenverschlüsselung).

Nachfolgend sind die aus unserer Sicht wichtigsten Informationen so einfach wie möglich zusammengefasst.

1. **Betrifft uns eigentlich das Thema Datenschutz**?

   Datenschutz betrifft alle im Verein automatisiert verarbeiteten Daten, ob im Internet, am privaten Computer oder auch völlig analog in einem Karteikartensystem. Dies umfasst auch die Webseite, aber darüber hinaus auch jede andere Datenverarbeitung, angefangen von der Erstellung und Speicherung einer Mitgliederliste, über den Einzug der Mitgliedsbeiträge, bis hin zur Veröffentlichung von z.B. Anwesenheitslisten.

2. **Müssen wir die Satzung ändern?**

   Es ist zu empfehlen, in die Satzung als zentrale Grundlage der rechtlichen Beziehungen zwischen Verein und Mitglied auch einen Passus zum Datenschutz aufzunehmen. Hier sollte in knapper Form geregelt sein, welche Daten der Verein notwendigerweise erheben muss, dass diese nur im Rahmen des Vereinszweckes und nur für die Dauer der Mitgliedschaft genutzt werden, dass die Daten vor Zugriffen Dritter geschützt werden und auch, wenn sie einem Dachverband weitergegeben werden. Wir weisen darauf hin, dass eine solche Satzungsregelung keine Einwilligung in eine spezielle Datennutzung ersetzen kann oder gar eine Pauschaleinwilligung in die Nutzung der Daten darstellt.

3. **Darf jeder Zugriff auf die Daten haben?**

   Zugriff auf die Daten ist nur den Personen zu gewähren, die für die Zwecke der Mitgliedschaft im Verein zwingend Zugriff haben müssen oder in deren Zugriff der Betroffene ausdrücklich eingewilligt hat.

4. **Müssen wir einen Datenschutzbeauftragten bestellen?**

   Ein normaler Selbsthilfeverein mit üblichem Vereinsbetrieb wird in der Regel keinen Datenschutzbeauftragten bestellen müssen. Voraussetzung hierfür wäre, dass „in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind" (vgl. § 38 Abs. 1 BDSG in der ab 25. Mai 2018 gültigen Fassung) oder dass „eine Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten“ (Artikel 9, 10 DS-GVO) vorliegt. Bei der Zahl der Personen zählen zwar auch ehrenamtlich Aktive, aber trotzdem dürfte diese Grenze kaum ein Verein überschreiten. Eine freiwillige Benennung ist aber trotzdem möglich.
   Zum Einordnen, wann eine umfangreiche Verarbeitung von sensiblen Daten vorliegt, kann man sich an einem Beschluß der „Konferenz unabhängiger Datenschutzbehörden des Bundes und der Länder„ (kurz: DSK) vom 26.4.2018 orientieren. Darin steht unter Absatz 2:

   2. Bei Ärzten, Apothekern oder sonstigen Angehörigen eines Gesundheitsberufs, die zu mehreren in einer Berufsausübungsgemeinschaft (Praxisgemeinschaft) bzw. Gemeinschaftspraxis zusammengeschlossen sind oder die ihrerseits weitere Ärzte, Apotheker bzw. sonstige Angehörige eines Gesundheitsberufs beschäftigt haben, ist in der Regel nicht von einer umfangreichen Verarbeitung besonderer Kategorien von personenbezogenen Daten im Sinne von Art. 37 Abs. 1 lit. c DS-GVO auszugehen –

in diesen Fällen ist unter Berücksichtigung von Punkt 3 dann kein DSB zu benennen, ***wenn weniger als 10 Personen*** *mit der Verarbeitung personenbezogener Daten beschäftigt sind.*

Daraus folgt, daß selbst diese Institutionen, die erheblich mehr sensible Daten als ein Verein der Selbsthilfe erhalten und verarbeiten, keinen Datenschutzbeauftragten benötigen.

5. Welche Regeln gelten für die Mitgliederverwaltung?

Die hauptsächliche Datenerhebung und -nutzung in einem Verein der Selbsthilfe findet sicher meist zum Zweck der Erstellung einer aktuellen Mitgliederliste statt. Hier wird auch der Großteil an personenbezogenen Daten erhoben werden (wie Name, Anschrift, Geburtsdatum, Bankverbindung), so dass auf eine datenschutzkonforme Erhebung und Verwendung besonders Augenmerk zu richten ist.
Die hier bestehenden Regeln galten nahezu durchweg auch schon im alten Datenschutzrecht. Es gelten die Regeln der „Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz", der „Zweckbindung", der „Datenminimierung", der „Richtigkeit", der ,,Speicherbegrenzung" und der „Integrität und Vertraulichkeit", vgl. Art. 5 der EU-**DSGVO.**
Grundsätzlich ist zu unterscheiden zwischen Daten, die für die Mitgliedschaft im Verein zwingend notwendig sind und sonstigen Daten. Für die Verarbeitung letzterer Daten bedarf es grundsätzlich immer einer gesonderten und jederzeit widerruflichen Einwilligung des Betroffenen, erstere können auch ohne gesonderte Einwilligung im gesetzlichen Rahmen erhoben und genutzt werden, Art. 6 (1) S. 1 der EU-DSGVO.
Daten, die auf Grundlage einer Einwilligung erhoben wurden, dürfen nur soweit und solange genutzt werden, wie die Einwilligung reicht. Bei allen personenbezogenen Daten gilt ansonsten, dass sie nur in dem Umfang erhoben und genutzt werden dürfen, wie es zwingend erforderlich ist.
Dies betrifft auch die Entscheidung, wer Zugriff auf welche Daten haben darf, auch vorstandsintern. Nicht jeder einfache Beisitzer darf bspw. Zugriff auf die Kontodaten jedes Mitglieds haben, ein Aushängen der vollständigen Mitgliederliste in Vereinsräumen oder gar eine Veröffentlichung im Internet sind ohne gesonderte Einwilligung der Betroffenen völlig verboten. Dies betrifft ebenso die Sicherstellung der Datensicherheit, bspw. durch eine sichere Aufbewahrung, aktuelle Sicherheitssoftware, Backups etc.

1. Was gilt bei der Ersterhebung von Daten bspw. auf einem Mitgliedsantrag?

Bei der Neuerfassung ist zwischen notwendigen und sonstigen Daten zu unterscheiden. Soweit nur erstere erhoben werden, sollte eine kurze Datenschutzerklärung beigefügt werden, in der darauf hingewiesen wird, dass die Datenerhebung und Datennutzung auf Grundlage des Art. 6 (1) S. 1 b) der EU-DSGVO und nur für vereinsinterne Zwecke erfolgt und eine weitergehende Nutzung oder Weitergabe der Daten ohne vorherige Einwilligung nicht erfolgen wird. Soweit weitergehende Daten erhoben werden sollen, muss die Einwilligungserklärung den Anforderungen der Art. 7 f. der EUDSGVO entsprechen (Siehe Anlage).

b. Was gilt, wenn sich Daten ändern?

Die EU-DSGVO verpflichtet auch, die Daten aktuell zu halten. Mitglieder sind also darauf

hinzuweisen, ihre Daten bei Änderungen jeweils zu aktualisieren, die Vorstände müssen dies dann datentechnisch umsetzen.

6. Müssen wir jetzt bis zum 25.05.2018 von allen Mitgliedern neue Mitgliedsanträge oder Einwilligungen einholen?

Soweit die im Verein der Selbsthilfe verarbeiteten Daten nur im Umfang der für die Vereinsmitgliedschaft notwendigen Daten erfasst wurden, braucht man keine neuen Dokumente. Lediglich dann, wenn auch sonstige Daten erhoben wurden, ist die hierfür bestehende Einwilligungserklärung auf Konformität mit den neuen gesetzlichen Regeln zu prüfen und ggf. zu erneuern.
Es bietet sich aber an, an alle bestehenden Mitglieder auch die Datenschutzerklärung zu versenden, die zukünftig für Neumitglieder mit dem Mitgliedsantrag ausgegeben wird.

7. Müssen die Mitglieder einer Nutzung ihrer Daten zur Kontaktaufnahme zustimmen?

Auch hier gilt: soweit es für die Mitgliedschaft im Verein notwendig ist, ist die Zustimmung nicht erforderlich. So kann selbstverständlich auch ohne Einwilligung die Einladung zur Mitgliederversammlung per Post an die Mitglieder geschickt werden. Falls der 2. Vorsitzende aber bspw. auf die Idee käme, die Daten zu nutzen, um Werbung für seine Kfz-Werkstatt zu machen, wäre dies selbstverständlich ohne explizite Einwilligung nicht erlaubt.

8. Ist jede Datenverarbeitung einwilligungspflichtig?

Nein, es gibt in Art. 6 (1) der EU-DSGVO weitere gesetzliche Fälle, wo eine Datenverarbeitung auch ohne Einwilligung erlaubt ist. So sind Selbsthilfe-Vereine berechtigt, zumindest die Daten zu verarbeiten, die für die Mitgliedschaft zwingend erforderlich sind oder soweit die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist. Regelungen dazu sollten Sie in Ihrer Satzung oder Beitragsordnung aufnehmen.

9. Ist die Veröffentlichung von Daten, insbesondere auf der Homepage, erlaubt?

Bei Veröffentlichungen im Internet macht der Gesetzgeber klare Vorgaben: Jede Veröffentlichung von personenbezogenen Daten im Internet durch einen Verein der Selbsthilfe ist grundsätzlich **unzulässig** – es sei denn, der Betroffene hat sich ausdrücklich damit einverstanden erklärt.
Dennoch gibt es einige Ausnahmen zu dieser Regelung. So ist die Veröffentlichung von allgemein zugänglichen Daten erlaubt, wenn es keine besonderen schutzwürdigen Interessen des Betroffenen gibt. Das heißt konkret: Eine offizielle Veranstaltung wie eine Demonstration oder eine offizielle Diskussion ist ein öffentliches Ereignis, über das z.B. auch die Lokalpresse berichtet. Daher dürfen Sie in diesem Fall personenbezogene Informationen zu Teilnehmern veröffentlichen. Diese Daten müssen aber nach angemessener Zeit gelöscht werden. Noch ein Tip beim Verwenden von Videos und Fotos. Diese dürfen ohne ausdrückliche Erlaubnis des Betroffenen (Abgebildeten) nur in Anlehnung an das KUG §23 veröffentlicht werden, da ansonsten ein Eingriff in das Persönlichkeitsrecht vorliegt.

Man kann sich daran orientieren, was §23 KUG (Urheberrechtsgesetz) bisher dazu ausführt:

(1) Ohne die nach § 22 erforderliche Einwilligung dürfen verbreitet und zur Schau gestellt werden:

1. ***Bildnisse aus dem Bereiche der Zeitgeschichte;***
2. ***Bilder, auf denen die Personen nur als Beiwerk neben einer Landschaft oder sonstigen Örtlichkeit erscheinen;***
3. ***Bilder von Versammlungen, Aufzügen und ähnlichen Vorgängen, an denen die dargestellten Personen teilgenommen haben;***
4. *Bildnisse, die nicht auf Bestellung angefertigt sind, sofern die Verbreitung oder Schaustellung einem höheren Interesse der Kunst dient.*

(2) Die Befugnis erstreckt sich jedoch nicht auf eine Verbreitung und Schaustellung, durch die ein berechtigtes Interesse des Abgebildeten oder, falls dieser verstorben ist, seiner Angehörigen verletzt wird.

10. Dürfen wir einmal erhobene Daten für immer nutzen?

Nein, selbstverständlich nicht. Die Verarbeitung der Daten ist auch zeitlich nur solange zulässig, wie sie notwendig ist. Wie lange dies ist, ist nicht pauschal zu beantworten und auch laufend zu prüfen. Manche Daten können auch während der Mitgliedschaft nur für eine begrenzte Zeit genutzt werden, manche sind mit Beendigung der Mitgliedschaft zu löschen. Für manche Daten besteht allerdings auch das Recht, diese für längere Zeit aufzubewahren, insbesondere soweit diese noch rechtlich relevant sein könnten.

11. Hat die EU-DSGVO Auswirkungen auf die Homepage?

Für die Nutzung der Daten auf der Homepage ergeben sich keine gesonderten Regeln gegenüber einer sonstigen Nutzung, alles ist unter dem Gebot der zwingenden Notwendigkeit für die Vereinsmitgliedschaft oder das Vorhandensein einer Einwilligung zu prüfen. Die Veröffentlichung von Daten ist bis auf wenige Ausnahmen ohne Einwilligung verboten, auch in internen Mitgliedsbereichen. Soweit auf der Homepage selbst Daten erhoben werden, bspw. in einem Kontaktformular, muss vorab konkret informiert werden, welche Daten zu welchem Zweck erhoben werden, wie sie genutzt werden und dass sie nach Zweckerreichung wieder gelöscht werden.
Wie bisher sollte auch eine Datenschutzerklärung auf die Homepage gestellt werden, die Auskunft gibt, ob und wenn ja, in welchem Umfang Daten auf der Homepage verarbeitet werden. Für die Erstellung dieser Erklärung gibt es im Internet zahlreiche hilfreiche Generatoren und im Anhang finden Sie ein Beispiel.

12. Müssen wir Abmahnungen befürchten?

Was ein ernstes Problem werden kann, sind Abmahnvereine/-anwälte. Diese suchen gezielt nach Webseiten und Drucksachen, die ab dem 25.5. nicht die erforderlichen Erklärungen und Nachweise enthalten. Das kann schon beim ersten Fall einige hundert Euro kosten. Darum die dringende Bitte:
Überarbeiten Sie Ihre Webseiten noch VOR dem **25.5.2018**. Fügen Sie einen neuen Haupt-Menüpunkt „Datenschutz“ hinzu und dort eine DSGVO konforme Datenschutzerklärung wie in Anlage X ein.

13. Wie sieht es mit Bußgeldern aus?

Es ist richtig, dass mit Einführung der DSGVO die Bußgelder und Strafrahmen erheblich erhöht bzw. verschärft werden. Oft wird davon gesprochen, daß beispielsweise Verstöße, die früher mit einem

Bußgeld in Höhe von 50 Euro abgetan waren, zukünftig 3300 Euro kosten sollen, also das 66 fache.

Dies ist NICHT so.

Laut Landesdatenschutzbeauftragten MV ändert sich die Arbeitsweise der Behörde nicht mit Einführung der DSGVO. Damit gilt:

- Bei einem Verstoß wird man **zuerst beraten** und bekommt auferlegt, binnen einer bestimmten Frist den Mißstand zu beheben.
- Sollte der Mißstand nach Ablauf der Frist noch bestehen, erfolgt eine behördliche Anordnung mit Fristsetzung, diesen Mißstand doch noch zu beheben.
- Wer dann immer noch nichts getan hat, den trifft dann der „Weckruf“ des Bußgelds.

Zu diesem Thema wurde uns mitgeteilt, dass die Behörden auf absehbare Zeit keine Veranlassung haben, in kleinen, ehrenamtlichen Strukturen wie der Selbsthilfe Kontrollen durchzuführen. Hier wird das Risiko für schwerwiegende Datenprobleme eher gering eingeschätzt.
Es kann aber vorkommen, dass sich jemand über einen Verein beschwert. Dann müssen die Aufsichtsgremien von Amts wegen tätig werden und hier zahlt sich die Erstellung der Dokumentation aus. Diese muß dann vorgelegt werden.

In jedem Fall ist es angeraten, für etwaige Anfragen der Datenschutzbehörden eine Dokumentation zu erstellen. Auch für kleine Gruppen ist dies eine einmalige Aufgabe, die dann jährlich selbst überprüft und fortgeschrieben werden muss. Um diese kommen wir nicht herum. Was genau jeder Verein/Gruppe in der Selbsthile erstellen muß, ergibt sich aus der DSGVO und dem neuen Bundesdatenschutzgesetz. Hier können wir beratend zur Seite stehen.

14. Müssen wir den Datenschutzbehörden Auskunft geben?

Die Rolle der Datenschutzbehörden ist durch die neue EU-DSGVO deutlich gestärkt worden, hier bestehen umfangreiche Auskunfts- und Mitteilungspflichten. So muss den Datenschutzbehörden bspw. auf Anforderung das Verarbeitungsverzeichnis vorgelegt werden und soweit ein Datenschutzbeauftragter benannt ist, muss dieser den Datenschutzbehörden genannt werden. Zudem müssen die Datenschutzbehörden im Fall einer Verletzung des Schutzes personenbezogener Daten innerhalb von 72 Stunden selbständig durch den Vorstand informiert werden.

17. Betrifft die EU-DSGVO auch die Datensicherheit?

Eindeutig ja. Verarbeiter der Daten sind verpflichtet, die erhobenen Daten sicher aufzubewahren und vor Zugriffen Unbefugter und vor Verlust zu schützen. So müssen die technischen Geräte, die zur Datenverarbeitung genutzt werden (PC, Tablet, Smartphone, etc.), mit aktueller Software, einem aktuellen Virenscanner und einer Firewall ausgestattet und passwortgeschützt sein. Die Daten sind zudem verschlüsselt zu speichern und zu übertragen. Die Maßnahmen sollen dem aktuellen Stand der Technik entsprechen, es genügen aber dem Zweck angemessene Maßnahmen. So muss zwar nicht das Wohnhaus des Kassenwarts/Schatzmeisters mit Fingerabdruck-Scannern und Wachpersonal ausgestattet werden, nur weil dort die Kontodaten aufbewahrt werden, aber er sollte diese auch nicht einfach auf dem ungesicherten Rechner aufbewahren.

18. Welche Sozialen Medien können wir nutzen?

Soziale Medien wie Facebook, Twitter, Instagram, Whatsapp und die vielen anderen sind derzeit auch im Vereinsleben groß angesagt. Aufgrund der aktuellen rechtlichen Situation ist von der Nutzung dieser Medien für Vereine der Selbsthilfe generell abzuraten.

Alle diese Systeme haben den gravierenden Nachteil, daß die hauptsächliche Datenverarbeitung außerhalb der EU stattfindet und damit ein gleichwertiger Datenschutz nicht gewährleistet werden kann. Wie schon viele Skandale z.B. bei Facebook und Oxford Analytica gezeigt haben, kann trotz gegenteiliger Beteuerungen der Betreiber nicht davon ausgegangen werden, „dass die Daten dort schon sicher genug sind".

Insbesondere Gruppenchats auf Whatsapp sowie Foren und Chatrooms auf diversen Platformen sind eine Fundgrube für Datensammler. Leider wird von den Teilnehmern oft nicht beachtet, daß sie sich öffentlich äußern nach dem Motto „Ich habe ja nichts zu verbergen".

Auch die Nutzung von Facebook für den Vereinsauftritt kann nach dem Schachzug von Facebooks Chef Mark Zuckerberg, zuerst die europäischen Schutzvorschriften in höchsten Tönen zu loben und danach sämtliche relevanten Mitglieder-Daten aus der EU in andere Bereiche der Erde zu transferieren, nicht mehr vertreten werden.

19. Wie sieht es mit Cloud-Diensten aus, z.B. Office 365?

Alle diese Systeme haben den gravierenden Nachteil, daß die hauptsächliche Datenverarbeitung außerhalb der EU stattfindet und damit ein gleichwertiger Datenschutz nicht garantiert werden kann, selbst mit dem Versprechen einer sicheren Telekom-Cloud.

Wie schon Windows 10 mit seinem extremen Telemetriedatenübertragungen nach Übersee zeigt, ist nicht auszuschließen, daß auch sensible Daten von Microsoft Systemen verschwinden können.

Office365 liegt nun vollständig außerhalb Ihres Einflußbereiches in der Cloud, und damit möglichweise außerhalb der EU-DSGVO. Die genaue Einstufung, wie sicher die Nutzung ist, wird in den nächsten Monaten passieren und bis dahin raten wir dringend ab, Microsoft Office 16 oder Office 365 für die Vereinsarbeit zu nutzen.