Kreisausschuss

Stabsstelle Dezernatsbüro der Landrätin

LANDKREIS MARBURG BIEDENKOPF

Erste Infos zum „Datenschutz für Vereine“

Stand Mai 2018

Ab dem 25. Mai 2018 gelten EU-weit die Vorschriften und Maßgaben nach der neuen Datenschutz-Grundverordnung (DSGVO). Mit dieser soll in allen EU-Mitgliedsländern das Datenschutzrecht harmonisiert werden. Nicht nur Unternehmen und Behörden, auch Vereine müssen die gesetzlichen Vorgaben zum Datenschutz einhalten.

Auf den folgenden Seiten finden Sie einige Grundlagen-Informationen zu den Themen:

- Was ist Datenschutz und welche Daten sind davon betroffen?
- Welche allgemeinen Grundregeln zum Datenschutz müssen beachtet werden?
- Was bedeutet die DSGVO für Vereine?

Allgemeines zum Datenschutz

Was ist Datenschutz?

Mit Datenschutz ist der „Schutz von Personen vor dem Umgang mit ihren personen-bezogenen Daten“ gemeint, zum Beispiel vor:

- unberechtigter Speicherung
- fremder (unberechtigter) Kenntnisnahme und Verwendung
- unsauberem Umgang mit Daten (Computer, Internet)

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Einzelangaben, die sich auf eine bestimmte bzw. eine bestimmbare natürliche Person beziehen, zum Beispiel:

- Name und Vorname
- Privatanschrift
- E-Mail-Adresse
- Telefonnummer
- Ausweisnummer
- Standortdaten (z. B. die Standortfunktion bei Mobiltelefonen)
- IP-Adresse
- Kontonummer, Bankverbindung
- Arbeitgeber, Beruf
- Etc.

Letztlich sind personenbezogene Daten alle Daten, die die betroffene Person, deren Verhalten oder ihre Lebensumstände beschreiben.

Sind alle personenbezogenen Daten gleich?

Manche personenbezogenen Daten sind besonders schützenswert (Art. 9 DSGVO) und dürfen nur unter ganz bestimmten Voraussetzungen verarbeitet werden. Dazu zählen Angaben über:

- die rassische und ethnische Herkunft
- politische Meinungen
- religiöse oder weltanschauliche Überzeugungen
- die Gewerkschaftszugehörigkeit
- genetische und biometrische Daten,
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung.

Sollen solche Daten verarbeitet werden, ist grundsätzliche eine besondere Einwilligung nach Art. 7 DSGVO erforderlich. Aber auch „normale“ personenbezogene Daten können zu besonders schützenswerten personenbezogenen Daten werden, je nach dem, in welchem Zusammenhang sie verwendet werden.

Beispiel: Die Anschrift einer Person ist zwar prinzipiell wenig bedenklich. Allerdings kann die Anschrift eines Patienten in einer psychiatrischen Klinik einen Hinweis auf dessen Gesundheitszustand geben.

Welchen Zweck haben der Datenschutz und die Datenschutz-Grundverordnung (DSGVO), das Bundesdatenschutzgesetz (BDSG) und das Hessische Datenschutzgesetz (HDSG)?

Diese Verordnungen und Gesetze schützen die Grundrechte und Grundfreiheiten natürlicher Personen, insbesondere das Recht auf den Schutz personenbezogener Daten. Sie schützen

also die Bürgerinnen und Bürger vor der Beeinträchtigung ihrer Persönlichkeitsrechte, wenn deren personenbezogene Daten verarbeitet werden.

Das wesentliche Ziel des Datenschutzes ist es, den sogenannten „gläsernen Menschen“ zu verhindern. Jeder Mensch soll grundsätzlich selbst entscheiden können, welche seiner persönlichen Daten er wem, wann und wie zugänglich machen will. So bleibt es zum Beispiel jedem Menschen selbst überlassen, ob er Informationen über sich im Internet veröffentlicht oder nicht. Werden gegen seinen Willen solche Veröffentlichungen gemacht, kann er dagegen vorgehen, da sein Recht auf informationelle Selbstbestimmung verletzt wurde.

Wann dürfen Daten erhoben, verarbeitet und genutzt werden?

Grundsätzlich gilt: Personenbezogene Daten dürfen **gar nicht** erhoben, verarbeitet und genutzt werden!

Ausnahmen:

- Gesetzliche Regelungen (z.B. Bundesmeldegesetz)
- Spezielle (bereichsspezifische) Regelungen (z.B. Tarifvertrag)
- Durch Bundesdatenschutzgesetz erlaubt
- Betroffene Person willigt ein (z.B. vertragliche Regelung)

Ist auch Datenverarbeitung in Papierform betroffen?

Personenbezogene Daten sollen **unabhängig von der verwendeten Technik** geschützt werden. Die DSGVO umfasst also sowohl den Schutz der personenbezogenen Daten, die in elektronischer Form vorliegen als auch der personenbezogen Daten in Papierform.

Werden personenbezogene Daten unter Einsatz von Datenverarbeitungsanlagen erhoben, verarbeitet oder genutzt, dann spricht man von einer automatisierten Verarbeitung. Auf diese Weise lassen sich Daten einerseits besonders einfach und effektiv verarbeiten, andererseits sind damit auch Risiken verbunden. So können Daten etwa unzulässigerweise verknüpft oder ausgewertet werden. Dies ist zwar bei einer Auswertung mit Papier und Bleistift nicht so einfach möglich, trotzdem ist auch die Datenverarbeitung ohne Einsatz von elektronischen Medien **grundsätzlich** von der DSGVO betroffen. **Es ist zum Beispiel zu gewährleisten, dass Schriftstücke nicht von Unbefugten eingesehen werden können.**

Welche allgemeinen Grundregeln des Datenschutzes gelten?

- **Rechtsgrundlage**
  Immer wenn personenbezogene Daten „angefasst“ werden, muss es dafür ein Gesetz oder eine Einwilligung der betroffenen Person geben.
- **Datenerhebung direkt bei den Betroffenen**
  Wann immer möglich, sollten Daten direkt bei den Betroffenen erhoben werden. Ist dies nicht möglich, sind diese zumindest darüber zu informieren (informationelle Selbstbestimmung).

- **Auskunftsrechte**
  Die betroffenen Personen müssen jederzeit Kenntnis haben, dass Daten über sie gespeichert sind (Transparenzgebot). Sie dürfen auch Auskunft verlangen.
- **Zweckbestimmung**
  Erhobene Daten dürfen ausschließlich für den Zweck verwendet werden, zu dem sie ursprünglich erhoben wurden.
- **Datensparsamkeit**
  Es dürfen nur so viele Daten wie unbedingt nötig erhoben, verarbeitet und genutzt werden.
- **Berichtigung**
  Personenbezogene Daten, die falsch sind, müssen berichtigt werden.
- **Schutz durch technische und organisatorische Maßnahmen (TOMs)**
  Daten müssen durch geeignete technische und organisatorische Maßnahmen vor Missbrauch geschützt werden (z.B. durch abschließbare Schränke etc.).
- **Löschung**
  Wenn die Daten veraltet sind bzw. die Löschfrist abgelaufen ist, sind sie zu löschen.

Wie lange dürfen personenbezogene Daten gespeichert werden?

Öffentliche und nichtöffentliche Stellen dürfen in eng gestecktem Rahmen personenbezogene Daten erheben, verarbeiten und nutzen, solange der Datenschutz gewahrt bleibt. Doch: Die gespeicherten personenbezogenen **Daten können auch veralten, unzulässig erhoben worden oder der Zweck ihrer Verwendung erfüllt** sein. Zudem gelten für die Speicherung mitunter auch **Verjährungsfristen**. Tritt die Verjährung der Datennutzung ein, müssen die Daten gesperrt oder gelöscht werden. In diesen Fällen können Betroffene mit einem Antrag ihr Recht auf Berichtigung, Löschung oder Sperrung der Daten gegenüber öffentlichen und nichtöffentlichen Stellen in Anspruch nehmen.

In folgenden Fällen sind Daten von den Verantwortlichen in den öffentlichen und nichtöffentlichen Stellen zu berichtigen, zu löschen oder zu sperren:

- **Berichtigung**
  Die Daten sind dann zu korrigieren, wenn diese offensichtlich falsch bzw. veraltet sind.
- **Löschung**
  Daten müssen gelöscht werden, wenn:
  - die Erhebung nicht zulässig war (fehlende Zustimmung der betroffenen Person, fehlende Zweckbindung, fehlende rechtliche Grundlage usw.)
  - ein Recht auf Löschung der Daten besteht (im Zweifel können auch Berichtigungen oder Sperrungen erfolgen).
  - der Zweck der Speicherung erfüllt, also die Zweckgebundenheit aufgelöst ist
  - die Speicherfrist für die Daten abgelaufen ist.

- **Sperrung**
  An die Stelle der Löschung tritt die Sperrung der Daten und der damit einhergehende Schutz vor weiterem Zugriff, wenn:

  - der Löschung gesetzlich geregelte Aufbewahrungsfristen entgegenstehen
  - anzunehmen ist, dass durch eine Löschung die schutzwürdigen Interessen des Betroffenen beeinträchtigt wären
  - die Löschung nicht oder nur unter unverhältnismäßigem Arbeitsaufwand erfolgen kann aufgrund der besonderen Speicherungsart

  Beim Sperren von personenbezogenen Daten werden diese zwar nicht aus der automatisierten Speicherung herausgenommen, sollen jedoch für sämtliche Personen unzugänglich aufbewahrt werden. Auch kein Mitarbeiter der öffentlichen oder nichtöffentlichen Stellen darf dann noch an die gesperrten Informationen herankommen. Schon allein die Tatsache der Sperrung darf auch nicht mehr übermittelt werden.

Grundsätzlich sind öffentliche und nichtöffentliche Stellen dazu verpflichtet, von sich aus **regelmäßig den Datenbestand zu prüfen** und auf Verjährungsfristen, Zweckerfüllung und datenschutzkonforme Verwendung der Daten zu achten. Durch das nach dem BDSG-neu und der DSGVO im Datenschutz gewährte Recht der Betroffenen auf Löschung der Daten (bzw. der Berichtigung oder Sperrung) soll diesen jedoch eine erhöhte **Kontrolle über den regelkonformen Umgang** mit ihren personenbezogenen Daten gewährt werden. Jede betroffene Person kann **Auskunft über die zur eigenen Person gespeicherten Daten verlangen**. Stellt sie Fehler in der Auskunft fest, kann sie die Berichtigung, Löschung oder Sperrung personenbezogener Daten beantragen.

Datenschutz im Verein
Worauf sollten Vereine beim Umgang mit personenbezogenen Daten achten?

Quelle:
https://www.dsb-ratgeber.de/artikel/Datenschutz-im-Verein-darauf-sollten-Sie-achten.html

Rechtlicher Rahmen

Das BDSG beziehungsweise die DSGVO regelt genau, was ein Verein bei der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beachten muss. Unter personenbezogenen Daten versteht der Gesetzgeber nicht nur Angaben zur Person (zum Beispiel Name, Adresse, Geburtsdatum), sondern auch weitere Informationen wie Wettkampfergebnisse, Mitgliedschaften in Organisationen oder persönliche Interessen. Verantwortlich für die Einhaltung der Datenschutzvorgaben ist der Vereinsvorstand. Er muss dafür sorgen, dass das Persönlichkeitsrecht der Mitglieder angemessen berücksichtigt wird. Außerdem müssen Betroffene, also z.B. die Vereinsmitglieder, umfassender über die Speicherung ihrer Daten informiert werden, etwa bei der Eingabe von Daten in ein Spendenformular. Immer dann, wenn Daten der Mitglieder erhoben werden, wie im Antrag auf Mitgliedschaft, müssen die in Art. 13 genannten Informationen mitgeteilt werden. So ist

insbesondere über Art, Umfang und Zweck der Datenerhebung aber auch über die Rechte der Betroffenen zu informieren.

Erheben personenbezogener Daten

Die meisten Vereine erhalten personenbezogene Daten durch den Mitgliedsantrag, Spendenformulare oder durch Anmeldeformulare zu Wettkämpfen oder einer Fortbildung. Welche Daten durch den Verein erhoben werden, hängt von den Vereinszielen ab. Diese sollten verständlich in der Vereinssatzung festgelegt sein. Möchte ein Verein zusätzlich weitere Informationen wie zum Beispiel persönliche Interessen erfahren, muss auf dem Aufnahmeantrag klar erkennbar sein, welche Angaben freiwillig sind und zu welchem Zweck diese Daten erhoben und genutzt werden. Am besten händigen Sie eine datenschutzrechtliche Belehrung aus, die darüber Auskunft gibt, welche Daten zu welchem Zweck erhoben, gespeichert und genutzt werden.

Verarbeiten und Nutzen der Daten durch den Verein

Mit Verarbeiten meint der Gesetzgeber das Speichern, Verändern, Übermitteln, Sperren und Löschen von personenbezogenen Daten. Unter die Nutzung fällt zum Beispiel die Datenweitergabe innerhalb des Vereins im Vorstand oder wenn der Verein die Daten extern verwalten lässt. Generell gilt, dass jeder Funktionsträger im Verein nur entsprechend seiner Aufgaben auf die erforderlichen Mitgliederdaten Zugriff haben darf.

Veröffentlichungen im Internet und von Fotos

Bei Veröffentlichungen im Internet macht der Gesetzgeber klare Vorgaben: Jede Veröffentlichung von personenbezogenen Daten im Internet durch einen Verein ist grundsätzlich erstmal 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: Ein offizielles Fußballspiel ist ein öffentliches Ereignis, über das auch die Lokalpresse berichtet. Daher dürfen Sie beispielsweise personenbezogene Informationen zur Mannschaftsaufstellung veröffentlichen. Diese Daten müssen aber nach angemessener Zeit gelöscht werden. Ähnlich verhält es sich beim Verwenden von Videos und Fotos. Diese dürfen ohne ausdrückliche Erlaubnis des Betroffenen nicht veröffentlicht werden, da ansonsten ein Eingriff in das Persönlichkeitsrecht vorliegt.

Wann ist ein Datenschutzbeauftragter nötig?

Der Vorstand muss einen Datenschutzbeauftragten bestellen, wenn mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. Es ist aber in jedem Fall ein Datenschutzbeauftragter zu benennen, wenn Angaben beispielsweise zur Gesundheit oder politischen Meinung oder zur Bewertung der Person erfasst werden.

Genau wie bei Unternehmen wirkt ein Datenschutzbeauftragter im Verein auf die Einhaltung der Vorschriften hin.

Was müssen Vorstände beachten?

Zusammenfassend ergeben sich für den Vorstand folgende Grundregeln für den Umgang mit personenbezogenen Daten:

- Verwenden Sie personenbezogene Daten nur für vereinsinterne Zwecke gemäß der Vereinssatzung.
- Geben Sie die Daten nicht an Dritte weiter – es sei denn, Sie haben die schriftliche Einwilligung der betroffenen Person.
- Beschränken Sie den internen Zugriff auf personenbezogene Daten.
- Halten Sie die IT aktuell und orientieren Sie sich an den üblichen Sicherheitsstandards (Firewall, Virenscanner, passwortgeschützter Zugang, evtl. Festplattenverschlüsselung).

Checkliste: Welche Maßnahmen müssen Vereine ergreifen?

Vereine sollten sicherstellen, dass u.a. folgende Maßnahmen und Aufgaben erfüllt werden:

- **Bestandsaufnahme Datenverarbeitung**: Wer verarbeitet personenbezogene Daten in welchen Prozessen? Welche Informationen dürfen gespeichert werden?
- **Datenschutzbeauftragten benennen** (wenn mindestens zehn Personen im Verein ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind)
- **Internetseiten** im Hinblick auf die DSGVO prüfen und **Datenschutzerklärung veröffentlichen bzw. anpassen**
- **Verzeichnisses der Verarbeitungstätigkeiten** erstellen: Hierbei handelt es sich um eine Übersicht über die Verfahren, bei denen personenbezogene Daten verarbeitet werden. Es dient der Transparenz und dem Nachweis der Einhaltung der Datenschutzvorschriften nach innen und nach außen.
- **Vereinbarungen zur Auftragsdatenverarbeitung** mit externen Dritten abschließen (zum Beispiel mit dem Provider Ihrer Internetseite, sofern dieser Auftragsdaten verarbeitet)
- **Einwilligungserklärungen** gemäß den Vorgaben der DSGVO überarbeiten
- Datensicherheit gewährleisten durch geeignete **technische und organisatorische Maßnahmen** (TOMs)
- Sicherheitskonzept erstellen und dokumentieren, welche Maßnahmen umgesetzt werden (Nachweis, dass man sich an die DSGVO hält)
- **Rechte der Betroffenen sicherstellen** (Recht auf Information und Auskunft über erhobene Daten und deren Verwendung, auf Korrektur oder Löschung der Daten etc.)

Weiterführende Links:

http://www.spiegel.de/netzwelt/web/dsgvo-das-sollten-sie-zur-datenschutz-grundverordnung-der-eu-wissen-a-1205985.html (Artikel Spiegel Online)

https://datenschutz-generator.de/ (Datenschutz-Generator)

https://www.lda.bayern.de/de/kleine-unternehmen.html (Internetseite des Bayerischen Landesamts für Datenschutzaufsicht)

https://www.baden-wuerttemberg.datenschutz.de/datenschutz-im-verein/ (Internetseite des Landesbeauftragten für Datenschutz und Informationssicherheit in Baden Württemberg)

https://www.impulse.de/recht-steuern/rechtsratgeber/dsgvo-website/7304684.html (Checkliste für DSGVO-konforme Webseiten)

Kontakt

Landkreis Marburg-Biedenkopf
Stabsstelle Dezernatsbüro der Landrätin
Fachdienst Bürgerbeteiligung und Ehrenamtsförderung
Susanne Batz, Servicestelle für Vereine und ehrenamtlich Engagierte
Tel.: 06421 405-1789
E-Mail: ehrenamt@marburg-biedenkopf.de
Internet: www.ehrenamt.marburg-biedenkopf.de