

Datenschutz im Verein mit dem "GLS Vereinsmeister"

Am 25. Mai 2018 trat die Europäische Datenschutzgrundverordnung (DSGVO) in Kraft. Auf der DSGVO basiert das neue Bundesdatenschutzgesetz (BDSG), das als Ergänzung und Konkretisierung gedacht ist. Gesetz und Verordnung regeln den Umgang mit personenbezogenen Daten und bilden die Rechtsgrundlage für eine ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten – auch im Verein. Dabei ist es unerheblich, ob ein Verein ins Vereinsregister eingetragen ist, ob er gemeinnützig anerkannt ist, oder ob es sich sogar um einen nicht rechtsfähigen Verein handelt.

Datenschutz und Datensicherheit

Bevor wir in die Details der Datenverarbeitung sowie der aus der DSGVO erwachsenden Rechte und Pflichten einsteigen, sollten die Begriffe Datenschutz und Datensicherheit einmal voneinander abgegrenzt werden – auch wenn die beiden Begriffe häufig synonym verwendet werden:

Beim Datenschutz geht es in erster Linie um den Schutz personenbezogener Daten vor dem Zugriff und dem Missbrauch durch unberechtigte Dritte. Hier geht es weniger um den Inhalt oder die Bedeutung von Daten, sondern eher um das Recht auf informationelle Selbstbestimmung. In Deutschland bezieht sich der Begriff des Datenschutzes ausschließlich auf die Daten von natürlichen Personen, nicht jedoch auf juristische Personen wie Firmen oder andere Körperschaften. Neben der DSGVO regeln auch andere Gesetze und Verordnungen den Umgang mit personenbezogenen Daten wie bspw. das Telemediengesetz oder landesspezifische Vorschriften. Einige Gesetze und Vorschriften „übersteuern“ auch die DSGVO und gelten vorrangig. Bspw. sind in Abgabenordnung (AO) und Handelsgesetzbuch (HGB) Aufbewahrungsfristen für Belege und Geschäftsdokumente geregelt, die von der DSGVO erstmal unberührt sind.

Der Begriff der Datensicherheit bezieht sich auf personenbezogene Daten aber auch auf beliebige andere Daten. Im Kontext der Datensicherheit werden in erster Linie technische und organisatorische Maßnahmen genannt, die dem Schutz beliebiger – aber eben auch personenbezogener – Daten dienen. Im Kern der Datensicherheit ist nicht nur der Zugriff und der Missbrauch durch unberechtigte Dritte, sondern auch der Verlust oder die ungeplante Veränderung der Daten thematisiert. Zusammengefasst geht es um Kontrollierbarkeit, Verfügbarkeit, Integrität und Vertraulichkeit aller Daten.

Personenbezogene Daten im Verein

Um im Verein den Regeln von DSGVO und BDSG gerecht zu werden, ist es nicht damit getan, eine beliebige Software einzusetzen, die vielleicht eine Art „DSGVO-Siegel“ trägt. In der DSGVO wird weder eine spezifische Software noch ein spezifischer Ablauf vorgeschrieben. Tatsächlich müssen die organisatorischen Abläufe des Vereins – von der erstmaligen Erhebung der Daten (bspw. Aufnahmeantrag) bis zur Löschung der Daten (bspw. durch Austritt eines Mitglieds) umfassend betrachtet und bewertet werden. In dem Zuge wird ein Verzeichnis erstellt, das die Abläufe der Datenverarbeitung festhält und detailliert beschreibt. Dabei sollte beachtet werden, dass sich personenbezogene Daten im Verein nicht nur auf Mitglieder beschränken. Auch Interessenten, Trainer, Mitarbeiter, Spender, Vorstände anderer Vereine, usw. können ebenso in die Kategorie fallen, sofern der Verein solche Daten verwaltet und verarbeitet. Der Einsatz einer geeigneten Software zur Vereinsverwaltung kann bei der Einhaltung der Vorschriften sehr gut unterstützen. In

der Regel wird bei einem Verein jedoch nicht nur eine Software eingesetzt, wo personenbezogene Daten abgelegt und verarbeitet werden. Auf dem Vereins-PC sind häufig gescannte Dokumente, Briefe, PDF-Dateien, E-Mails etc. gespeichert, welche ebenfalls Personenbezug haben.

Zweck und Erhebung von personenbezogenen Daten

DSGVO und BDSG erlauben die Erhebung und Verarbeitung personenbezogener Daten im Wesentlichen dann, wenn zwei Bedingungen zutreffen:

1. Es muss einen nachweisbaren Zweck für die Erhebung und Verarbeitung der Daten geben.
2. Die Person muss der Erhebung und Verarbeitung ihrer Daten ausdrücklich zustimmen.

Ein Zweck für die Datenverarbeitung ergibt sich aus der Mitgliedschaft und dem Geschäftsbetrieb im Verein. Um einen Beitrag zu erheben sind die Daten des Mitglieds erforderlich. Dabei ist es unerheblich, ob über den Beitrag eine Rechnung erstellt wird, der Beitrag bar entrichtet wird oder ob dieser per Lastschrift eingezogen wird. Je nach Art und Zweckes Vereins kann es erforderlich sein, über das Mitglied noch weitere Daten zu speichern. Dazu gehören neben Adresse und Bankverbindung auch das Eintrittsdatum, das Geschlecht (für die Bestandsmeldung an den Sportbund), ausgeübte Sportarten, sportliche Leistungen, Funktionen und u.U. Ehrungen. Vorsicht ist geboten, wenn es sich um besonders schützenswerte Daten handelt. Dazu könnten beispielhaft die politische Ausrichtung (->Parteien), die Religion oder bestimmte Krankheiten (->Selbsthilfevereine) gehören. Hier muss der Vorstand entscheiden, welche Daten erhoben werden und den Umgang damit im Verfahrensverzeichnis und ggf. in einer Datenschutzerklärung festhalten. An dieser Stelle kommt auch das Prinzip der „Datensparsamkeit“ zur Anwendung: es dürfen nur solche Daten erhoben und gespeichert werden, die der Zweck erfordert. „Datensammelei“ ist somit unzulässig. Im „GLS Vereinsmeister“ gibt es neben Namen und Mitgliedsnummern kaum weitere Pflichtfelder. Somit kann das Gebot der Datensparsamkeit problemlos eingehalten werden, indem nur die Daten erfasst werden, die für den Vereinszweck maßgeblich sind.

Die Zustimmung zur Erhebung der Daten muss verständlicherweise schon vor der Erhebung der Daten erfolgt sein. Idealerweise gibt es daher auf dem Aufnahmeantrag bereits einen Hinweis auf die Datenschutzerklärung des Vereins (ggf. die ganze Erklärung als Hand-Out an das Mitglied) und ein Unterschriftsfeld, wo das Mitglied der Speicherung und Verarbeitung seiner Daten explizit zustimmen kann. Vor Beginn der Mitgliedschaft erfolgt damit die Zustimmung schon bevor überhaupt Daten elektronisch verarbeitet werden.

Beispiel:

Hinweise zum Datenschutz

Ich willige ein, dass der Verein zum Zwecke der Mitgliederverwaltung und Beitragsabrechnung personenbezogene Daten wie Name, Anschrift, Geburtsdatum, Telefonnummer, Mailadresse und Bankverbindung erhebt und speichert. Weiterhin willige ich ein, dass der Verein an den Dachverband zum Zwecke der Bestandserhebung Name, Anschrift, Geburtsdatum und Eintrittsdatum weitergibt. Mir ist bekannt, dass dem Aufnahmeantrag ohne diese Einwilligung nicht stattgegeben werden kann.

Datum, Unterschrift

Maßnahmen für Datenschutz und Datensicherheit

Um personenbezogene Daten auf dem Vereins-PC vor dem Zugriff durch unberechtigte Dritte zu schützen, muss zunächst einmal der PC selbst geschützt werden. Dabei ist es unerheblich, ob sich die schützenswerten Daten auf einem privaten PC zu Hause beim Vorstand befinden oder auf einem PC, der im Vereinsheim oder in der Geschäftsstelle steht. Unabhängig von der eingesetzten Software sollten folgende Maßnahmen unbedingt beachtet werden:

1. Der PC sollte durch ein starkes Kennwort geschützt werden. Das Kennwort darf nur dem berechtigten Personenkreis bekannt sein. Es ist empfehlenswert, in den vereinsinternen Datenschutzbestimmungen den Umgang mit Kennworten zu regeln. Der PC muss weiterhin so konfiguriert sein, dass keine automatische Anmeldung beim Hochfahren erfolgt, sondern grundsätzlich immer ein Login erfolgen muss. Wird der PC in Geschäftsstelle oder Vereinsheim von mehreren Anwendern genutzt, dann sollte jeder Anwender ein eigenes Benutzerkonto für den PC haben. Bei einem personellen Wechsel im Vorstand kann man so schnell eine Berechtigung sperren oder eine neue Berechtigung vergeben, ohne dass die anderen Anwender davon beeinflusst werden. Durch den Kennwortschutz des Betriebssystems ist bereits eine ganz wesentliche Grundlage für den Schutz der Daten erreicht. Ohne diesen Schutz könnten Daten auch von ansonsten kennwortgeschützten Anwendungen vom PC herunterkopiert werden und an einem anderen Ort ganz ungestört „geknackt“ oder entschlüsselt werden.
2. Bei Anwendungen, die – wie der „GLS Vereinsmeister“ - die Definition von Benutzern und Zugriffsrechten innerhalb der Software erlauben, sollte idealerweise ein Rollenkonzept erarbeitet und umgesetzt werden. Sobald im „Vereinsmeister“ Benutzer und Rechte definiert sind, ist der Zugriff auf beliebige Daten feingranular steuerbar. Die Rollen sollten dabei so definiert werden, dass nicht alle Anwender auf alle Daten zugreifen können, sondern jeder Anwender nur die für seinen Verantwortungsbereich notwendigen Daten sieht. Bspw. muss ein Anwender, der lediglich in der Finanzbuchhaltung arbeitet, keinen schreibenden Zugriff auf Mitgliederstammdaten haben. Für die Buchung von Beiträgen und offenen Posten ist ein lesender Zugriff auf Mitgliederdaten ausreichend. Im „Vereinsmeister“-Berechtigungsmodell lässt sich weiterhin auch steuern, welche Anwender Daten löschen oder drucken dürfen. Auf diesem Weg kann bspw. verhindert werden, dass Listen mit Mitgliederdaten gedruckt und mitgenommen werden. Im Handbuch finden Sie weitere Hinweise zum rollenbasierten Berechtigungsmodell im „Vereinsmeister“.



System/Einstellungen

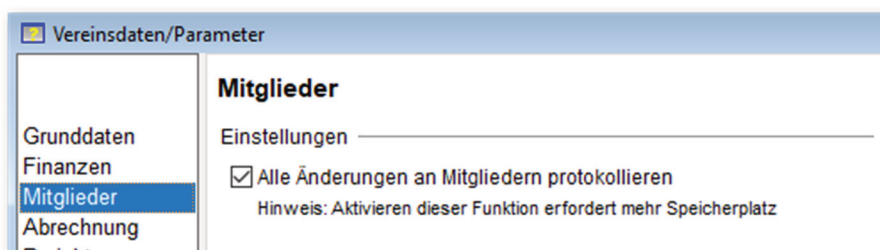
-  **Datenbankpflege**
Reorganisation, Datenexport und Datensicherung
-  **Benutzer**
Kennworte, Zugriffsrechte
-  **Rollen und Rechte**
Benutzerrollen und Berechtigungen

Programmberechtigungen		Ändern	Löschen	Drucken
<input checked="" type="checkbox"/>	Stammdatenpflege			
<input checked="" type="checkbox"/>	Mitglieder	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Sparten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Gruppen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Banken	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	Kontakte	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Inventar	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	Belegtexte	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Konten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Wertelisten und Tabellen	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Vereinsdaten	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

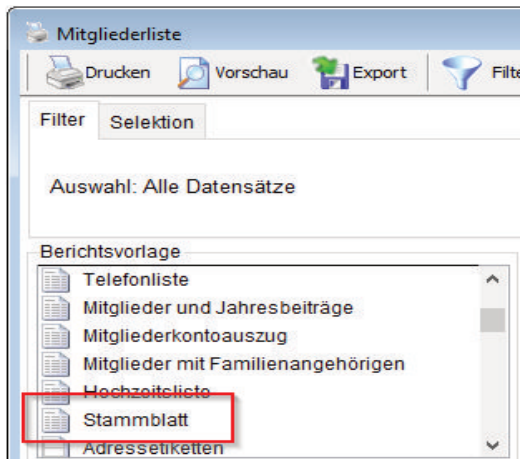
3. Andere Schutzziele im Kontext der Datensicherheit sind der Schutz vor Verlust und Veränderung. Zum Erreichen beider Ziele ist eine regelmäßige Datensicherung verpflichtend. Eine Datensicherung darf dabei nicht auf die gleiche Festplatte wie die Originaldaten erfolgen, sondern muss auf einem externen Datenträger liegen, der idealerweise auch an einem anderen Ort aufbewahrt wird. Dabei ist zu bedenken, dass ein Dritter den Zugang zum Vereinscomputer vielleicht gar nicht erlangen muss, wenn er in den Besitz einer Datensicherung kommt. Die Sicherungsmedien sollten daher gut verschlossen aufbewahrt und ebenfalls vor dem Zugriff Dritter geschützt werden. Wurden Daten ungeplant verändert oder verfälscht, dann kann das Einspielen der Sicherung dies rückgängig machen oder die Analyse der Sicherung kann Auskunft über Art und Umfang der Veränderungen geben. Im „GLS Vereinsmeister“ kann eine Datensicherung ganz leicht über den Menüpunkt „System->Datenbankpflege“ erstellt werden. Die Sicherung anderer auf dem PC befindlicher Daten (Dokumente, Briefe usw.) obliegt der Verantwortung und dem Ermessen des Anwenders.



4. Im Laufe einer Mitgliedschaft dürfen und sollen sich die Mitgliederdaten in der Regel häufiger ändern. Das Mitglied kann jederzeit seinen Status, seinen Beitrag, seine Spartenmitgliedschaft oder seine Anschrift verändern. Aus diesem Grund ist es nicht möglich, Mitgliederdaten dauerhaft vor Veränderungen zu schützen (bspw. indem keinem Anwender Änderungsrechte an Mitgliederdaten erteilt werden). Die DSGVO regelt auch, dass Veränderungen an personenbezogenen Daten protokolliert und nachgewiesen werden müssen. Im „GLS Vereinsmeister“ kann daher in den Vereinsdaten die Protokollierung von Änderungen aktiviert werden. Ist das Änderungsprotokoll eingeschaltet, dann wird jede Veränderung an den Mitgliedern im Logbuch festgehalten. Dabei wird nicht nur die Erfassung, Änderung und Löschung im Allgemeinen protokolliert, sondern ganz detailliert aufgezeichnet, welches Feld oder welche Eigenschaft verändert wurde, wann diese Änderung vorgenommen wurde und welcher Anwender die Änderung vorgenommen hat. Das Änderungsprotokoll kann weiterhin ausgewertet und ausgedruckt werden.



5. Im DSGVO ist geregelt, dass eine Person jederzeit Auskunft über die über sie gespeicherten Daten verlangen darf. Im „GLS Vereinsmeister“ gibt es mehrere Möglichkeiten, einem solchen Auskunftsverlangen nachzukommen. Die einfachste Möglichkeit ist der Ausdruck eines Mitgliederstammblates, das alle Stammdaten eines Mitglieds enthält. In der „Pro“- und „Network“-Edition kann das Layout und der Inhalt des Stammblatts im grafischen Designer auch nach Belieben verändert werden. Das vorgenannte Änderungsprotokoll kann die Auskunft ergänzen und vervollständigen.



6. Weiterhin hat eine Person das Recht, die Löschung der über sie gespeicherten personenbezogenen Daten zu verlangen. Im Verein wird dies erst nach dem Austritt des Mitglieds vorkommen, da die Speicherung der Daten eines Mitglieds für den Geschäftsbetrieb des Vereins unabdingbar ist. Weiterhin erlischt mit dem Austritt des Mitglieds in aller Regel auch der Zweck, der die Speicherung der Daten legitimiert hat. Die DSGVO schreibt in dem Fall die unverzügliche Löschung der gespeicherten personenbezogenen Daten vor.



Im „GLS Vereinsmeister“ gibt es die Möglichkeit, Mitgliederdaten auch nach dem Austritt des Mitglieds zu archivieren. Auch wenn ein solches Archiv im Zusammenhang mit der Löschpflicht widersprüchlich erscheint, kann es – je nach Art des Vereins – durchaus einen legitimen Zweck für die Archivierung geben. Hierzu gehören bspw. Anschreiben oder Gratulationen zu besonderen Gelegenheiten (runde Geburtstage, Hochzeitstage, Ehrungen zu sportlichen Leistungen). Um hier nicht in eine rechtliche Grauzone zu geraten, sollte die weitere Speicherung der Mitgliedsdaten beim Austritt mit dem Mitglied geklärt werden und dafür ggf. eine gesonderte Zustimmung des Mitglieds eingeholt werden.

Auftragsverarbeitung und Datenweitergabe an Dritte

In manchen Fällen ist eine kontrollierte Weitergabe von Daten an Dritte notwendig. Dazu kann eine Meldung an einen Sportbund gehören, sofern hier personenbezogene Daten überhaupt notwendig sind. Bei den meisten Bestandsmeldungen werden lediglich statistische Zahlen abgefragt. In anderen Fällen sollen Namen, sportliche Leistungen oder Fotos auf einer Webseite des Vereins veröffentlicht werden. Hierzu ist dann häufig eine gesonderte Genehmigung einzuholen. Manchmal drucken und Versenden auch Dienstleister die Vereinszeitschriften oder Ausweise und manchmal wird über Dachverbände eine Versicherung o.ä. abgeschlossen.

Sobald Dritte mit der Verarbeitung von Daten des Vereins betraut sind, spricht man von „Verarbeitung im Auftrag“ oder auch „Auftragsverarbeitung“. Gibt es im Verein eine solche Weitergabe von personenbezogenen Daten an Dritte, dann sollte unbedingt mit diesen eine „Vertrag zur Auftragsverarbeitung“ (AV) geschlossen werden. Dieser AV regelt dann die Rechte und Pflichten im Umgang mit den anvertrauten Daten. Im Internet gibt es Muster für solche AVs zum Download.

Gleiches gilt auch, wenn der Verein Clouddienste verwendet oder selbst betreibt, bei denen personenbezogene Daten verarbeitet werden. Im „GLS Vereinsmeister“ kann dies im Zuge der Funktionen zur Kollaboration verschiedener Anwender oder im verteilten Mehrplatzbetrieb vorkommen:

- Synchronisation der lokal gespeicherten Daten zwischen Anwendern über Clouddienste
- Mehrplatzbetrieb mit einem über das Internet erreichbaren Datenbank- oder Anwendungsserver



Im Falle der Nutzung eines Clouddienstes zur Datensynchronisation (bspw. MS „Azure“) gibt es von den großen Anbietern (bspw. Microsoft) bereits herunterladbare Musterverträge.

Wird vom Verein ein eigener Server bei einem Provider gemietet und betrieben, dann sollte Kontakt zu dem Provider aufgenommen werden, ob dort ebenfalls ein Mustervertrag erhältlich ist. In anderen Fällen muss ggf. ein AV gesondert und direkt geschlossen werden.

Datenschutzbeauftragter

Kommen im Verein regelmäßig mehr als 10 Personen (ständig) mit personenbezogenen Daten in Kontakt, dann ist vom Verein verpflichtend ein Datenschutzbeauftragter zu nennen. Diese Aufgabe kann eine Person im Verein übernehmen oder auch an einen externen Datenschutzbeauftragten delegiert werden. Diese Notwendigkeit kann auch schon bestehen, wenn weniger als 10 Personen an der Datenverarbeitung teilhaben und die verarbeiteten Daten risikobehaftet sind, so dass sie besonders schutzbedürftig sind (siehe oben zu „Zweck und Erhebung“). Auch wenn die Kerntätigkeit des Vereins in der Verarbeitung von Daten besteht, die eine Überwachung und Kontrolle von Personen ermöglicht (bspw. Videoüberwachung im Stadion), gibt es die Verpflichtung zur Nennung eines Datenschutzbeauftragten.

Datenschutzfolgeabschätzung

Wenn die Verarbeitung der Daten im Verein einem besonderen Risiko für die Rechte und Freiheit der betroffenen Personen unterliegt, kann eine Datenschutzfolgeabschätzung notwendig sein. Das kann bspw. bei Gesundheitsdaten, religiösen oder politischen Daten oder bspw. Daten über Straffälligkeiten der Fall sein. Verarbeitet der Verein solche Daten, dann muss die Folge von Verlust, unberechtigter Zugriff durch Dritte, Veröffentlichung, Manipulation usw. abgeschätzt und festgehalten werden. In dem Zusammenhang gibt es für Datenschutzvorfälle auch eine Meldepflicht an die zuständigen Behörden.

Fazit

Die Einhaltung der Vorschriften von DSGVO und BDSG ist weder eine Frage der richtigen Werkzeuge noch gibt es ein „Schema-F“, das jeder Verein ohne Aufwand umsetzen kann. Datenschutz ist weniger ein technisches Thema, sondern zunächst auf organisatorischer Ebene zu betrachten. Dazu gehört die Bewertung der Prozesse hinsichtlich ihrer datenschutzrechtlichen Relevanz – von der ersten Erhebung über alle Verarbeitungsschritte bis zur Löschung. Letztlich ist es eine Entscheidung des Vorstandes, wie der Verein mit den Anforderungen von Gesetz und Verordnung umgeht.

Der Einsatz einer Software mit unterstützenden Funktionen – wie dem „GLS Vereinsmeister“ – ist dabei ein wichtiger Baustein, um den Anforderungen an Datenschutz und Datensicherheit gerecht zu werden. Aber nur die ganzheitliche Betrachtung der Prozesse und der Art der Daten im eigenen Verein führt zu Rechtssicherheit in diesem schwierigen Thema. Jeder Verein ist anders, hat andere Prozesse und Verfahren und damit andere Anforderungen zu bewältigen.

Zum Schluss möchten wir noch auf den hervorragenden Praxisratgeber „Datenschutz im Verein nach der DSGVO“ des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg als Lektüreempfehlung hinweisen. Der Ratgeber kann im Internet auf der Datenschutzseite des Landes Baden-Württemberg heruntergeladen werden.

Bei spezifischen Fragen zum Datenschutz im Allgemeinen wenden Sie sich an den für Sie zuständigen Landesdatenschutzbeauftragten. Für Fragen zum „GLS Vereinsmeister“ wenden Sie sich selbstverständlich wie immer an unseren Support oder stellen Sie Ihre Frage im Supportforum.

Freundliche Grüße

Ihr Team von
GLS SOFTWARE & SYSTEME