Informationen zur EU-Datenschutzgrundverordnung für Vereine

In jedem Verein werden auf unterschiedlichste Art und Weise personenbezogene Daten verarbeitet. Dies sind beispielsweise Name und Anschrift der Mitglieder, deren Kontodaten, möglicherweise Gesundheitsdaten oder vieles Weitere. All dies verlangt von den Vereinen und Verantwortlichen bereits von sich aus einen verantwortungsvollen und sensiblen Umgang mit diesen Daten, zum Schutz der Mitglieder und des Vereins. Seit vielen Jahren bestehen hierzu gesetzliche Datenschutzregeln.

Am 25. Mai 2018 tritt nun eine europaweite Neuregelung, die EU-Datenschutzgrundverordnung (DSGVO), in Kraft, mit dem Ziel einer weitgehenden Vereinheitlichung der zurzeit noch in den Mitgliedsstatten der EU unterschiedlichen Gesetzgebungen zum Datenschutzrecht. Dementsprechend wird das Bundesdatenschutzgesetz (BDSG) zum 25.5.2018 in vielen Punkten angepasst. Für die Vereine gelten somit ab dem 25.5.2018 sowohl die Regularien der DSGVO, sowie des BDSG-neu.

Einhergehend mit dem Wirksamwerden werden auch die bei Verstößen möglichen Bußgelder deutlich erhöht, weshalb Vereinen dringend anzuraten ist, das Thema Datenschutz genauer zu betrachten und die Regeln zu befolgen. Im Folgenden möchten wir Ihnen einen Überblick über den Umfang, die Vorgaben und mögliche Umsetzungsmöglichkeiten geben, die die DSGVO für die Vereine mit sich bringt:

Hinweis: Die Vorgaben und Regularien der DSGVO sind in dem Text der Verordnung einfach verständlich und umfangreich beschrieben. Es lohnt sich somit bei der Arbeit mit diesem Thema immer der direkte Blick in die Verordnung. Beispielsweise unter: https://dsgvo-gesetz.de/

Anwendungsbereich der DSGVO:

Nach Art. 2 DSGVO kommen die Regeln der DSGVO und des BDSG-neu immer zur Anwendung bei der „ganz oder teilweisen automatisierten Verarbeitung personenbezogener Daten sowie bei nichtautomatisierter Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“ zur Anwendung.

Entscheidend sind hierbei folgende beiden Begriffe:

- **Personenbezogen Daten** sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person … beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, … identifiziert werden kann“. Die DSGVO findet demnach nur Anwendung, soweit es sich um Daten natürlicher Personen, sprich lebender Menschen, handelt. Daten über juristische Personen an sich fallen nicht in den Anwendungsbereich der DSGVO (Art. 4 Nr. 1 DSGVO).
- **Verarbeitung** beinhaltet jeden, „mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben,

das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“ (Art. 4 Nr. 2 DSGVO). Die DSGVO macht an dieser Stelle keinen Unterschied mehr zwischen automatisierter und nicht automatisierter Verarbeitung. Ebenfalls findet keine Unterscheidung mehr zwischen verschiedenen Datenverarbeitungen (Speichern, Bearbeiten, etc.) statt, was bedeutet, sobald Sie etwas mit den personenbezogenen Daten machen - egal was - gilt die DSGVO!

Sich hierüber im Klaren zu sein, ist auch bei der weiteren Vorgehensweise entscheidend, wenn man zunächst alle vorgenommenen Datenverarbeitungen im Verein zusammenträgt.

Hinweis: Weitere Begriffsbestimmungen finden Sie in Art. 4 DSGVO.

Gilt die DSGVO auch für Vereine?

Die DSGVO macht keinen Unterschied zwischen kleinen und großen Unternehmen und auch nicht zwischen wirtschaftlich arbeitenden Unternehmen und ideellen Vereinen. Auch spielt es weder eine Rolle, ob der Verein gemeinnützig ist oder nicht, noch ob der Verein in das Vereinsregister eingetragen („e.V.“) ist oder nicht.

Was sind die Grundsätze der neuen DSGVO?

Art. 5 der DSGVO beschreibt die Grundsätze der Verarbeitung personenbezogener Daten, die auch von Vereinen bei jedem Umgang mit persönlichen Daten zu beachten sind:

- **Rechtmäßigkeit der Verarbeitung:**
  Personenbezogene Daten dürfen nur verarbeitet werden, wenn die konkrete Verarbeitung von einer der in Art. 6 Abs. 1 DSGVO aufgeführten Rechtsgrundlagen gedeckt ist (siehe nächste Überschrift). Dementsprechend muss der Verein für jede einzelne Verarbeitung von Daten dies entsprechend prüfen.
- **Zweckbindung der Datenverarbeitung**
  Jede Datenverarbeitung darf nur zu einem vorab festgelegten Zwecke erfolgen.
- **Datenminimierung**
  Die Verarbeitung von Daten muss auf „auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“ (Art. 5 Abs. 1c DSGVO). Dies bedeutet auch, dass Sie nur die Daten erheben dürfen, die Sie für den entsprechenden Zweck benötigen. „Gerade mal noch ein paar weitere persönliche Daten für einen jetzt noch unbekannten Fall der Fälle abfragen“ sollten Sie vermeiden.
- **Richtigkeit der Daten**
  Nach den Vorgaben der DSGVO sind Sie nun auch explizit dafür verantwortlich, für die Richtigkeit der von Ihnen verarbeiteten personenbezogenen Daten zu sorgen. Hierzu gehört auch, dass Sie die Daten stets aktuell halten, sprich schnellstmöglich zu korrigieren oder zu löschen. Betreiben Sie also regelmäßige Datenpflege im Verein.
- **Speicherbegrenzung**
  Personenbezogene Daten dürfen nur „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.“ (Art. 5 Abs. 1e DSGVO). Das bedeutet, sobald der Zweck der Datenverarbeitung bzw. -speicherung nicht mehr vorhanden ist (z.B. Mitglied ist aus dem Verein ausgetreten) und auch die weiteren gesetzlichen Aufbewahrungsfristen verstrichen sind, haben Sie die Daten zu löschen oder durch Änderung den Personenbezug zu löschen.

- **Datenintegrität und Vertraulichkeit**
  Bei der Verarbeitung personenbezogener Daten müssen Sie sicherstellen, dass „eine angemessene Sicherheit der personenbezogenen Daten gewährleistet ist, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen“ (Art. 5 Abs. 1f DSGVO). Dies bedeutet, dass Sie sich in der Praxis konkret Gedanken machen müssen, über Ihre IT-Struktur, Zugriffsrechte (z.B. auf den PC des Vorsitzenden oder in der Geschäftsstelle, auf E-Mail-Konten, etc.) sowie insbesondere über eine regelmäßige Datensicherung.

Wann darf der Verein personenbezogene Daten verarbeiten?

Damit Sie personenbezogene Daten in Ihrem Verein verarbeiten dürfen, muss mindestens eine der in Art. 6 Abs. 1 DSGVO aufgeführten, die konkrete Verarbeitung erlaubenden Bedingungen erfüllt sein. Diese müssen Sie jeweils einzeln nach den zu verarbeitenden Daten (z.B. Name oder Adresse oder Geburtsdatum, etc.) und der beabsichtigten Verarbeitung beleuchten. Die im Verein in der Regel in Frage kommenden Rechtsgrundlagen sind:

- **Gesetzliche Rechtmäßigkeit aufgrund der Erfüllung eines Vertrages (nach Art. 6 Abs. 1 lit. b)**

  Personenbezogene Daten, die zur Erfüllung eines Vertragsverhältnisses erforderlich sind, dürfen ohne Einwilligung des Betroffenen verarbeitet werden. Hierunter fallen beim Verein insb. alle Daten, die für die Abwicklung der „Mitgliedschaft“ des Mitglieds in dem Verein erforderlich sind. Zum Beispiel der Name und die Adresse, zur Verwaltung der Mitgliedschaft oder das Geburtsdatum für die Altersklasseneinteilung in bestimmten Sportarten. Hierbei müssen Sie jedoch auch von dem Grundsatz der Datenminimierung ausgehen und können nicht alle für den Verein nützlichen personenbezogenen Daten grundsätzlich unter diesen Punkt fallen lassen. Erlaubt ist nur die Verarbeitung der für die Vertragserfüllung erforderlichen Daten. Kritisch wird es bereits bei weiteren Angaben wie dem Berufsstatus oder Ähnlichem.

- **Einwilligungserklärung (nach Art. 6 Abs. 1 lit. a)**

  Treffen die in Art. 6 Abs. 1 b) bis f) aufgeführten Rechtsgrundlagen nicht auf die jeweils von Ihnen beabsichtigte Datenverarbeitung zu, so müssen Sie sich grundsätzlich die Einwilligung der betroffenen Personen zur Verarbeitung der entsprechenden personenbezogenen Daten einholen.

  Neu mit Inkrafttreten der DSGVO ist nach Art. 7 Abs. 1 die Beweislastumkehr in Bezug auf die Einwilligung. Dabei hat zukünftig der Verein die Beweispflicht, dass der Betroffene eine wirksame Einwilligung erteilt hat. Deshalb wird dringend empfohlen, sich die Einwilligungen von den Betroffenen schriftlich erteilen zu lassen.

  Dabei gibt die DSGVO in Art. 4 Abs. 11 in Verbindung mit Art. 7 die genauen Voraussetzungen für eine rechtlich wirksame Einwilligungserklärung vor und enthält zusätzlich Vorschriften wie die Einwilligungserklärung ausgestaltet sein muss:

  - Die Einwilligung muss freiwillig abgegeben worden sein. Nach Erwägungsgrund 42 der DSGVO ist eine Einwilligung freiwillig, wenn die betreffende Person „eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.“
  - Die Einwilligung sollte „durch schriftliche Erklärung“ abgegeben worden sein, das heißt, dass Sie sich das entsprechende Formular von der betroffenen Person unterschreiben lassen. Dies dient auch Ihrer Nachweispflicht. Erfolgt diese Einwilligung durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um die Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist. D.h. die Einwilligungserklärung muss sich z.B. auf dem

Anmeldeformular klar von anderen Inhalten abheben und darf nicht versteckt oder „heruntergespielt“ werden.

- Die Einwilligung muss durch eine „unmissverständlich abgegebene Willensbekundung“ erfolgt sein, was bedeutet, dass die entsprechende Person selbst und aktiv eine entsprechende Handlung durchführen muss (Ankreuzen, Unterschreiben, etc.). Ein z.B. bereits angekreuztes Kästchen (Opt-Out) oder nur ein Hinweistext im Aufnahmeantrag auf eine mögliche Datennutzung ist nicht ausreichend.
- Die Einwilligung kann nur für einen näher bestimmten Fall bzw. Zweck gegeben werden. Eine „allgemeingültige“ Einwilligung als Freifahrtschein für jegliche Nutzung der Daten ist nicht zulässig.
- Sie müssen der betreffenden Person konkret aufführen, welche Daten für welchen Zweck verarbeitet werden.
  Tipp: Idealer Weise kombinieren Sie die Erklärung der Einwilligung mit den zuvor zu gebenden Informationen (siehe unsere Mustervorlage).
- Sie müssen angeben, ob bzw. in wie weit die Erfüllung des Vertragsverhältnisses, z.B. das Mitgliedsverhältnis, „von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.“
- Die Einwilligungserklärung muss einen Hinweis auf das Recht der betroffenen Person zu widerrufen enthalten. Dabei muss der Widerruf an sich „so einfach wie die Erteilung der Einwilligung sein“.

Art. 8 DSGVO stellt besondere Anforderungen an die Einwilligung bei Kindern.

Nach Art. 9 DSGVO ist die Verarbeitung von personenbezogenen Daten besonderer Kategorien (z.B. Gesundheitsdaten, Daten zur ethnischen Herkunft, etc.) grundsätzlich nur nach ausdrücklicher Einwilligung der betroffenen Personen erlaubt.

Wichtig: Oft kommt die Frage dabei auf, ob bereits eingeholte Einwilligungen nach dem 25.5.2018 weiterhin gelten. Dies ist der Fall, sofern die erteilten Einwilligungen bereits den neuen Vorgaben entsprechen. Ist dies nicht der Fall, wovon in den meisten Fällen auszugehen ist, müssen die Einwilligungen erneut nach den neuen Vorgaben eingeholt werden! Das bedeutet, dass Sie zwingend ihre bestehenden Einwilligungen prüfen müssen.

- **Gesetzliche Pflicht (nach Art. 6 Abs. 1 lit. c)**

  Eine weitere Rechtmäßigkeit zur Verarbeitung personenbezogener Daten ohne Einwilligung kann die Verarbeitung aufgrund der Erfüllung einer rechtlichen Verpflichtung sein. Dies trifft beispielsweise bei Aufbewahrungspflichten des Vereins im Rahmen des Steuerrechts (z.B. § 147 AO), oder Ähnlichem zu. Auch hier sollten Sie jedoch kritisch prüfen, welche Daten genau für die Erfüllung der gesetzlichen Pflichten benötigt bzw. „aufbewahrt“ werden müssen.

Wie muss ich meine Mitglieder informieren?

Eine wesentliche Neuerung im Datenschutz, die mit der DSGVO umgesetzt wird, sind die umfassenderen Informationspflichten für den Verein. Sie müssen als Verein den Personen, deren personenbezogenen Daten Sie erheben, bereits „zum Zeitpunkt der Erhebung dieser Daten“ eine Reihe an Informationen mitteilen. Welche Informationen das sind, finden Sie detailliert aufgeführt in Art. 13 EU-DSGVO.

Welche weiteren Rechte haben die Personen, deren Daten verarbeitet werden?

Die weiteren Rechte - neben dem Recht auf „Information“ - der betroffenen Personen, deren Daten Sie verarbeiten, sind in Art. 12 bis 23 DSGVO umfassend erläutert. Diese Rechte stellen sozusagen den Kern

der DSGVO dar, da durch den Datenschutz insbesondere die Rechte und Freiheiten natürlicher Personen geschützt werden sollen. Dabei sollen die betroffenen Personen wissen wer, welche ihrer Daten und zu welchem Zweck nutzt. Fragen Sie sich einmal selbst, wäre dies nicht auch Ihr Anspruch, wenn Sie Ihre personenbezogenen Daten, zum Beispiel Ihre Bankverbindung oder Daten über Ihren Gesundheitszustand preisgeben?

- **Das Recht auf „Auskunft“**

  Jede Person hat das Recht, Auskunft darüber zu verlangen, welche sie betreffenden personenbezogenen Daten vorhanden sind sowie in welchem Umfang und wofür sie verarbeitet bzw. genutzt werden. Hierzu gehören unter anderen Angaben zu den genauen Verarbeitungszwecken, wem die Daten offengelegt werden bzw. ob diese an Dritte übermittelt werden, die geplante Dauer der Speicherung, aber auch die entsprechenden Rechte auf Löschung, Berichtigung und Beschwerde bei der Aufsichtsbehörde (siehe Art. 15 Abs. 1 DSGVO). Sie müssen der die Auskunft verlangenden Person eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, kostenlos zur Verfügung stellen. Für alle weiteren Kopien, die die betroffene Person beantragt, können Sie ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Auskunftsantrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern die betroffene Person nichts anderes angibt (Art. 15 Abs. 3 DSGVO).

  Tipp: Es ist ratsam, dass Sie sich auch hier vorab eine Mustervorlage mit denen in Ihrem Verein in der Regel verarbeiteten Daten erstellen, um schnell auf Anfragen z.B. der Mitglieder reagieren zu können.

- **Das Recht auf „Berichtigung“**

  Dies sollte in der Praxis eines der unkompliziertesten Betroffenenrechte sein, und eines der selbstverständlichsten. Denn nach Art. 16 DSGVO sind Sie verpflichtet, auf Verlangen betroffener Personen unverzüglich unrichtige personenbezogene Daten zu korrigieren.

- **Das Recht auf „Löschung“ bzw. „Vergessenwerden“**

  Einhergehend mit dem Grundsatz der Datenminimierung hat jede Person das Recht auf Löschung ihrer persönlichen Daten sofern insbesondere der Zweck der Datenverarbeitung nicht mehr gegeben ist oder die Einwilligung zur Verarbeitung von ihr widerrufen wurde (siehe Art. 17 Abs. 1)

- **Das Recht auf „Einschränkung der Verarbeitung“**

  Unter bestimmten Voraussetzungen (siehe hierzu Art. 18 Abs. 1) haben betroffene Personen das Recht, eine Einschränkung der Verarbeitung der eigenen personenbezogenen Daten zu verlangen.

- **Das Recht auf „Datenübertragung“**

  Dieses Recht ist neu mit Inkrafttreten der DSGVO. Sollte eine Person, deren Daten Sie verarbeiten, an Sie herantreten und Verlangen seine Daten an Sie herauszugeben, um diese elektronisch an weitere Dritte zu übermitteln, sind Sie nach Art. 20 Abs. 1 dazu verpflichtet dem nachzukommen. Sie müssen daraufhin der betroffenen Person diese in „einem strukturieren, gängigen und maschinenlesbaren Format“ zur Verfügung stellen.

Was muss ich noch alles machen?

- **Verfahrensverzeichnisse**
  Neu für viele Vereine ist – und dies ist ein Punkt der (zunächst) einmaligen Arbeitsaufwand bedeutet – die Verpflichtung nach Art 30. Abs. 1 Satz 1 DSGVO „ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen“ zu führen. Zwar gilt dies nach Art. 30 Abs. 5 DSGVO nicht für Einrichtungen „die weniger als 250 Mitarbeiter beschäftigen“. Jedoch dürfte die darauffolgende

Ausnahme von der Befreiung „die Verarbeitung erfolgt nicht nur gelegentlich“, auf viele Vereine zutreffen.

Umsetzungstipp: Bei der Erstellung der Verfahrensverzeichnisse können sich Vereine an den bereits zur Information der betroffenen Person zusammengestellten Informationen orientieren und dies als Grundlage nutzen.

- **Dokumentationspflicht**
  Ein besonderes Augenmerk sollte zukünftig auch auf die Dokumentation jeder Maßnahme beim Umgang mit Daten bzw. in der Umsetzung der EU-DSGVO gelegt werden, da nach Art. 5 Abs. 2 EU-DSGVO der Verein in Zukunft, sollte es zu Datenschutzverstößen kommen, nachweisen können muss, dass er die datenschutzrechtlichen Regelungen eingehalten hat.

- **Verträge mit Auftragsverarbeitern**
  Sobald Ihr Verein eine natürlichen oder juristischen Person etc. beauftragt, die vom Verein erhobenen personenbezogenen Daten für Ihren Verein zu verarbeiten, muss der Verein sicherstellen, „dass geeignete technische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt“ (Art. 28 Abs. 1 DSGVO). Dies „erfolgt auf der Grundlage eines Vertrags“ (Art. 28 Abs. 3 DSGVO) mit dem Auftragsverarbeiter. Beispiele einer Auftragsverarbeitung sind: eine Mitgliederverwaltung im Internet, bei der die Daten auf den Servern des Anbieters liegen oder die gehostete Webseite, über die Daten erfasst bzw. versendet werden. Hierbei reicht es allein schon aus, wenn der Auftragsverarbeiter die Daten „nur“ speichert. Deshalb ist z.B. auch der Austausch personenbezogener Daten über die Cloud (z.B. dropbox) eine Auftragsverarbeitung durch den Anbieter der Cloud.

- **Maßnahmen zur IT-Sicherheit**
  Nach Art. 24 Abs. 1 und Art. 32 DSGVO müssen auch Vereine dafür Sorge tragen und überprüfen, ob die eigenen technischen und organisatorischen Maßnahmen der Datenverarbeitung geeignet sind, Datensicherheit zu gewährleisten. Bei allen Datenverarbeitungsvorgängen muss demnach überprüft werden, ob ausreichende Sicherheitsvorkehrungen getroffen worden sind (Datensicherung, Verschlüsselung, etc.). Außerdem muss der Verein sicherzustellen, dass ihm unterstellte natürliche Personen (egal ob haupt-, neben- oder ehrenamtlich für den Verein tätig), die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des nach § 26 BGB vertretungsberechtigten Vorstands des Vereins verarbeiten.

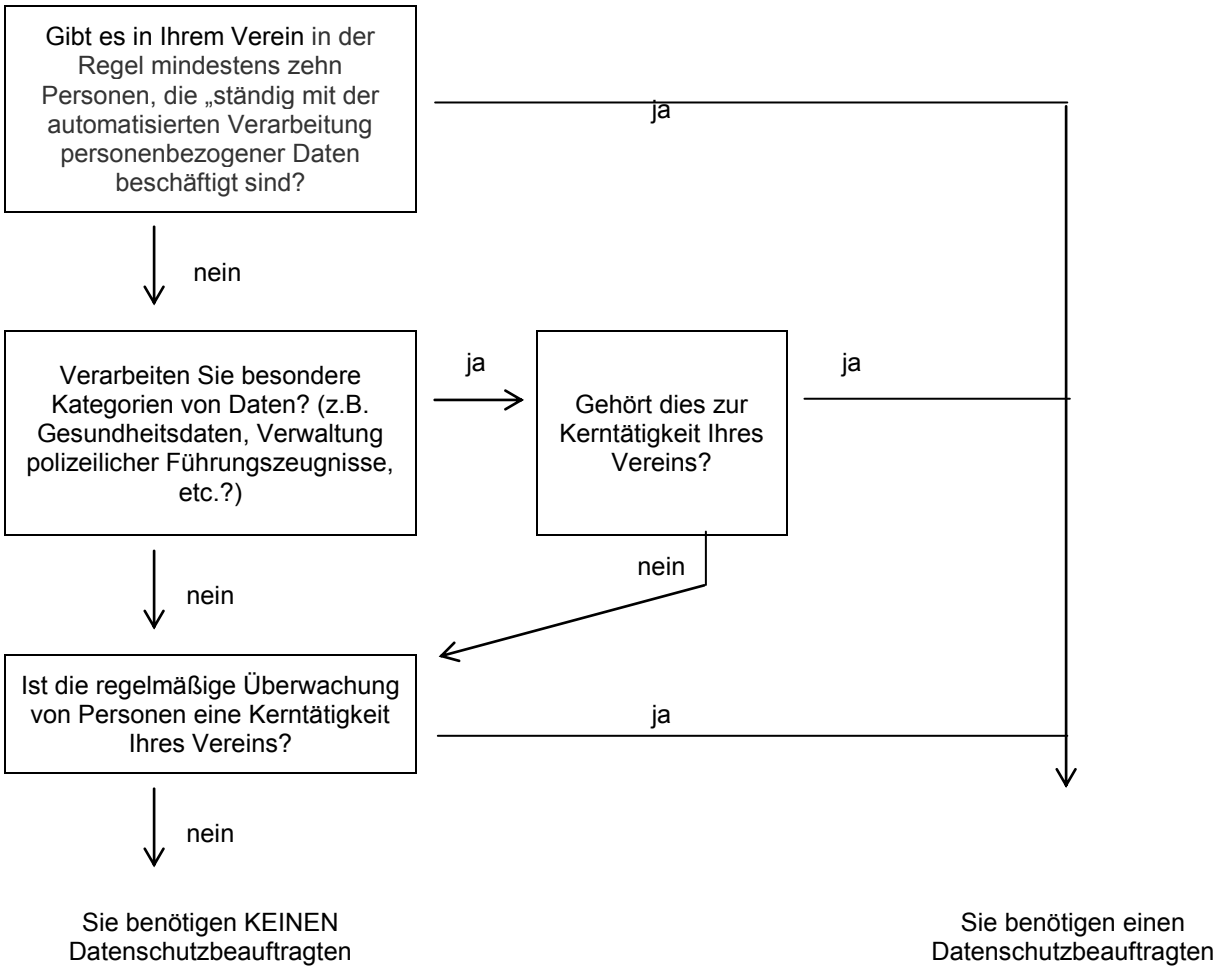
- **Datenschutz-Folgeabschätzung**
  Nach Art 35 Abs. 1 DSGVO muss der Verein prüfen, ob die Verarbeitung der Daten „insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge“ hat. Diese Prüfung muss für die jeweiligen einzelnen Datenverwendungen durchgeführt werden. Kommt man dabei zu dem Ergebnis, dass dies der Fall ist, so führt der Verantwortliche - mit dem Ziel das Risiko zu minieren - vor der Datenverarbeitung „eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.“ Art. 35 Abs. 7 DSGVO beschreibt dabei die Mindestinhalte dieser Datenschutz-Folgeabschätzung. Sofern Ihr Verein einen Datenschutzbeauftragten hat, haben Sie bei der Durchführung einer Datenschutz-Folgenabschätzung dessen Rat einzuholen.

  Die von Ihnen zu dokumentierende Folgenabschätzung enthält zumindest Folgendes:
  a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
  b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
  c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen

Benötigt unser Verein einen Datenschutzbeauftragten?

Schwierig für Vereine dürfte allen voran die Benennung eines Datenschutzbeauftragten werden, sofern dieser nach den gesetzlichen Vorgaben tatsächlich bestellt werden muss. Dies ist insbesondere von der Anzahl der (haupt-, neben- oder ehrenamtlich für den Verein tätigen) Personen die personenbezogene Daten verarbeiten und von der Art der Daten abhängig. Ob Sie als Verein einen Datenschutzbeauftragten benennen müssen, können Sie anhand folgenden Schemas prüfen (auf Basis der Regularien aus § 38 Abs. BDSG neu und Art. 37 Abs. 1 DSGVO):



Für Vereinsvertreter stellen sich hierbei insbesondere folgende Fragen:

- **Was bedeutet eine „ständige“ Verarbeitung der Daten?**

  Eine „ständige“ Beschäftigung setzt voraus, dass die Person sich für eine längere, meist unbestimmte Zeit mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt, ohne dass dies die ausschließliche Beschäftigung sein muss. Auch eine nur gelegentlich, etwa einmal im Monat anfallende Aufgabe erfüllt das Merkmal „ständig“, wenn die Person sie stets wahrzunehmen hat. Die Beschäftigung mit der Verarbeitung personenbezogener Daten muss zu einem regelmäßig wiederkehrenden und festen Bestandteil ihrer Aufgaben zählen. Der zeitliche Einsatz im Verhältnis zur Gesamtarbeitszeit ist ohne Relevanz.

- **Was bedeutet eine „automatisierte“ Verarbeitung der Daten?**

  Automatisierte Verarbeitung ist die Verarbeitung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen (z.B. Computern, Tabletts, Smartphones)

- **Wer zählt alles zu den Personen - auch bspw. der Übungsleiter der seine Trainingsgruppe per Serienmail anschreibt?**

  Durch den Begriff „Personen“ ist ausdrücklich geregelt, dass aus datenschutzrechtlicher Sicht allein die Anzahl der mit der automatisierten Verarbeitung personenbezogener Daten beschäftigten Personen entscheidend ist. Es kommt also nicht darauf an, welchen arbeitsrechtlichen Status diese Personen haben. Mitzuzählen sind vom Vorstand über Angestellte, Arbeiter, freie Mitarbeiter, Heimarbeitskräfte Auszubildende, bis hin zu Praktikanten und bei Vereinen ehrenamtlich Tätige. Bei der Berechnung der Anzahl der Personen sind aber nur die unmittelbar beim Verein Beschäftigten zu berücksichtigen.

Es darf vom Verein aber nur eine Person zum Datenschutzbeauftragten bestellt werden, die auf der Grundlage ihrer beruflichen Qualifikation und insbesondere des Fachwissens, das sie auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage ihrer Fähigkeit zur Erfüllung der ihr in Artikel 39 DSGVO genannten Aufgaben geeignet erscheint.

Nach Art. 37 Abs. 7 DSGVO müssen Sie die Kontaktdaten des bestellten Datenschutzbeauftragten der zuständigen Aufsichtsbehörde melden. I Für S-H das unabhängige Landeszentrum für Datenschutz Schleswig-Holstein.

Der Datenschutzbeauftragten hat insbesondere den Vorstand des Vereins hinsichtlich seiner Pflichten aus der DSGVO sowie der sonstigen Datenschutzvorschriften zu unterrichten und zu beraten sowie die Beschäftigten des Vereins, die Verarbeitungen durchführen. Der Datenschutzbeauftragte hat auch die Einhaltung der DSGVO, anderer Datenschutzvorschriften sowie der Strategien des Vereins für den Schutz personenbezogener Daten zu überwachen. Daraus ist zu entnehmen, dass auch nach der Bestellung eines Datenschutzbeauftragten die Verantwortlichkeit für die Einhaltung der Regelungen zum Datenschutz im Verein beim nach § 26 BGB vertretungsberechtigten Vorstand verbleibt.

Bei der Benennung von Datenschutzbeauftragten sind Interessenskonflikte zu vermeiden.

Die weiteren Aufgaben eines Datenschutzbeauftragten ergeben sich dabei insbesondere aus Art. 39 Abs. 1 DSGVO.

Was ist zu tun, um die Sicherheit der Daten zu gewährleisten?

Personenbezogene Daten sind insbesondere zu schützen vor:

- Eingriffen und unbefugten Zugriffen von Außenstehenden (z.B. keine personenbezogene Daten auf dem privaten Computer eines Vorstandsmitglieds, auf die dann auch unberechtigte Familienmitglieder des Vorstandsmitglieds Zugriff haben; Schutz vor Hackern die durch einen Angriff die Mitgliederdaten kopieren können, Weitergabe von E-Mailadressen in Adressfeldern von Serienmails an Personen die diese wiederum für andere Zwecke nutzen, oder Ähnliches)
- Bewusstem oder unbewusstem Zugriff bzw. Missbrauch personenbezogener Daten intern im Verein (z.B. unberechtigte Weitergabe von Mitgliederdaten an weitere Mitglieder, oder unberechtigte Einsicht in vertraulichen Schriftverkehr vom Mitgliede mit dem Vorstand, etc.) - siehe Art. 32. Abs. 4

Bisher haben § 9 BDSG in Verbindung mit der entsprechenden Anlage zum Gesetz einige Vorgaben hinsichtlich der zu treffenden Maßnahmen gegeben. Die DSGVO greift das Thema Datensicherheit nun insbesondere in Art. 32 auf und gibt vor, dass „der Verantwortliche und der Auftragsverarbeiter geeignete

technische und organisatorische Maßnahmen“ zu treffen haben, „um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.

Konkretisierungen, wie dies zu erfolgen hat und wie genau ein angemessenes Schutzniveau definiert ist, bleiben jedoch offen. Nach dem Willen des Gesetzgebers ist vielmehr in jedem Verein für jeden Einzelfall zu prüfen, wie genau bzw. was in der Praxis zur Gewährleistung der Datensicherheit umzusetzen ist.

Die Bewertung der Angemessenheit des Schutzes erfolgt dabei „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen“. Demnach sollte der Aufwand im Verhältnis zu dem angestrebten Schutzzweck stehen. Auch gilt es, sich bei der Schaffung der technischen Maßnahmen, z.B. Anschaffung eines neuen PCs oder eines neuen Routers, am Stand der Technik zu orientieren. Es sollte demnach nicht auf veraltete Systeme zurückgegriffen werden, sondern auf solche, die sich in der Praxis bewährt haben und den aktuellen Sicherheitsstandards entsprechen. Für Vereine, die dies bisher versäumt haben, bedeutet es nun in entsprechende Sicherheitsmaßnahmen (Firewalls, Antivirussystem, aktuelle Hardware, sichere Router, etc.) zu investieren.

Die Schutzziele, dies es zu verwirklichen gilt, ergeben sich aus Art. 32 Abs. 1 b) DSGVO:

- **Vertraulichkeit** der Daten, sodass unberechtigte Zugriffe ausgeschlossen sind.
- **Integrität** der Daten, sodass diese nicht unberechtigter Weise geändert oder gelöscht werden können.
- **Verfügbarkeit** der Daten, sodass diese durch unvorhergesehene Ereignisse wie beispielsweise Systemabstürze nicht zerstört oder verloren gehen.

Auch bei der Umsetzung der Datensicherheit hat der Verein wieder eine Nachweispflicht (nach Art. 5 Abs. 2 DSGVO) der getroffenen technischen und organisatorischen Maßnahmen.

Hinweis zur Nachweispflicht / Dokumentation: Zum Nachweis können nach Art. 32 Abs. 3 auch Zertifizierungen herangezogen werden. In unseren Arbeitsmaterialien haben wir Ihnen auch eine Vorlage zur Dokumentation der technischen und organisatorischen Maßnahmen zur Verfügung gestellt. Erstellen Sie sich zudem ein Konzept für die Zugriffberechtigungen zu den von Ihnen verarbeiteten personenbezogenen Daten und protokollieren Sie dies stets bei Änderungen, z.B. von Passwörtern, Personenwechsel, etc.

Weitere praktische Umsetzungstipps, die Sie bezüglich Ihrer IT-Infrastruktur des Vereins prüfen sollten:

- Verschlüsselung der Infrastruktur: z.B. WLAN Verschlüsselung nach den neuesten Standards, E-Mailverschlüsselung mit STARTSSÖ, Webseiten mit SSL-Zertifikaten (insb. bei der Möglichkeit Daten über die Webseite zu erfassen, wie bspw. Kontaktformularen), Absicherung externer Netzwerkzugriffe via VPN, etc.
- Passwortschutz auf sämtlichen Geräten, auf denen personenbezogene Daten gespeichert sind bzw. mit den auf diese Zugegriffen werden kann: PCs, USB-Sticks, einzelne Daten wie Mitgliederlisten als Excel, Mitgliederverwaltungsprogramme, etc.
- Durchführen regelmäßiger Sicherheitsupdates
- Absperren von Schränken in denen sensible Unterlagen gelagert sind
- Der Klassiker: E-Mailadresse bei Serienmails immer in BCC (Blindkopie)
- Erstellung eines Datensicherungskonzeptes (externe Festplatte, Datenserver mit RAID-System, USB-Stick, etc.) und Durchführung regelmäßiger Backups
- Zugangsberechtigungen für Räume und Büros (Schließsysteme, etc.)

Was ist zu tun, wenn eine Datenschutzverletzung auftritt?

Für den Fall, dass es in Ihrem Verein zu einer Verletzung des Schutzes personenbezogener Daten kommt (z.B. Hackangriff auf den PC mit Mitgliederdaten, Verlieren eines USB-Stick mit Bankdaten, Unbefugte haben plötzlich Zugang zu Daten, o.Ä.) die voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, sind Sie verpflichtet unaufgefordert und zügig die folgenden Punkte zu erledigen:

1. Meldung an die Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO)

Nach Art. 33 Abs. 1 DSGVO besteht auch für Vereine die Pflicht, eine „Verletzung des Schutzes personenbezogener Daten ... unverzüglich und möglichst binnen 72 Stunden, nachdem ... die Verletzung bekannt wurde, der ... zuständigen Aufsichtsbehörde“ zu melden.

Tipp: Überlegen Sie sich bereits jetzt, wie Sie in einem solchen Fall vorgehen. Organisieren Sie im Vorfeld einen entsprechenden Prozess mit den nötigen Dokumenten (insb. Vorlage für ein Schreiben an die Meldebehörde) und legen Sie zuständige Personen fest. Auch sollten Sie regeln, wie diese Personen von der Schutzverletzung erfahren. Mindestinhalte der Meldung sind in Art 33 Abs. 3 DSGVO geregelt.

2. Meldung an die betreffende Person bzw. betreffenden Personen (Art. 34 Abs. 1 DSGVO)

Wenn „die Wahrscheinlichkeit eines hohen Risikos für die Rechte und Freiheiten der betreffenden Personen“ besteht, müssen Sie diese ebenfalls über die Verletzung deren personenbezogenen Daten informieren. Dies gilt nach Art. 34 Abs. 3 lit. a) DSGVO nicht, sofern „der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung betroffenen personenbezogenen Daten angewandt wurden“. Mindestinhalte der Information an die betroffenen Personen sind in Art. 33 Abs. 3 b) bis d) DSGVO vorgegeben. Geben Sie dabei zudem mit an, was Sie unternommen haben, um möglichst weiteren Schaden abzuwenden.

3. Dokumentation (Art. 33 Abs. 5 DSGVO)

Schließlich sind Sie verpflichtet, alle im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten zu dokumentieren, was Sie nach Kenntnis von der Datenschutzverletzung unternommen haben, welche Auswirkungen diese Schutzverletzung hat und welche Maßnahmen Sie zur Abhilfe getroffen haben. Diese Dokumentation muss so gewissenhaft erstellt werden, dass der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen des Art. 33 DSGVO möglich ist. Dies sollten Sie gleichzeitig in Sinne Ihrer eigenen Absicherung schriftlich durchführen.

Wo finden wir weitere Informationen?

Einige Mustervorlagen und Arbeitshilfen haben wir Ihnen unter folgender Internetseite zusammengestellt: http://vereinsservice.lsvs.de → Aktuelles → Aktuelle Themen

Weitere externe Informationen und Links:

- Praxishilfen der Gesellschaft für Datenschutz und Datensicherheit e.V.: https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo

Für die im Vorherigen gemachten Ausführungen und Hinweise kann aufgrund der für jeden einzelnen Fall erforderlichen Prüfung und stetiger Änderungen bei der Rechtsprechung keine Haftung übernommen werden.

*Dieses Informationsblatt ist in Zusammenarbeit mit der **RKPN.de-Rechtsanwaltskanzlei Patrick R. Nessler**, Kastanienweg 15 in 66386 St. Ingbert entstanden. Wir bedanken uns für die Unterstützung und die Ausführungen. Sie finden die Kanzlei im Internet unter: www.rkpn.de*