



Wirtschaftsprüfungsgesellschaft

Datenschutzgrundverordnung DS GVO

Grundzüge der neuen Datenschutzregeln und die Umsetzung in der Vereinspraxis

Vortrag:

RA Wolfram Bauerhorst / WPK Beratung GmbH Wirtschaftsprüfungsgesellschaft Steuerberatungsgesellschaft

anlässlich der Mitgliederversammlung des Stadtverbands der Bürger- und Bezirksvereine Wuppertal e.V. am 05.06.2018



EU-Datenschutzgrundverordnung (DSGVO) – Grundsätze und Neuerungen



Wirtschaftsprüfungsgesellschaft

Am 25. Mai 2018 ist die EU-Datenschutzgrundverordnung (DSGVO) in Kraft getreten. Sie hat die bisher geltende EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) ersetzt. Im Unterschied zur bisherigen EU-Datenschutzrichtlinie gilt die DSGVO unmittelbar in der gesamten Europäischen Union.

Mit der umfassenden Reform des Datenschutzrechts auf EU-Ebene hat auch der nationale Gesetzgeber das Datenschutzrecht auf nationaler Ebene reformiert und den Anforderungen der DSGVO angepasst. So ist ebenfalls am 25. Mai 2018 das neue Bundesdatenschutzgesetz (BDSG-neu) in Kraft getreten und hat das alte BDSG abgelöst.



Grundsätze der Verarbeitung personenbezogener Daten nach Art 5 DSGVO



Wirtschaftsprüfungsgesellschaft

- **Rechtmäßigkeit**
 - Erlaubnis aus Gesetz oder Einwilligung
- **Zweckbindung**
 - eindeutig festgelegte Zwecke
- **Datensparsamkeit**
 - nur notwendige Daten
- **Richtigkeit**
 - Lösch- und Berichtigungspflichten
- **Integrität & Vertraulichkeit**
 - angemessene Sicherheit durch Schutzmaßnahmen
- **Transparenz**
 - Nachvollziehbarkeit der Datenverarbeitung



Rechtmäßigkeit der Datenverarbeitung

Artikel 6 DSGVO



Wirtschaftsprüfungsgesellschaft

Ausgestaltung als „Verbot mit Erlaubnisvorbehalt“

Die Verarbeitung personenbezogener Daten ist nur dann rechtmäßig, wenn entweder:

1. die betroffene Person ausdrücklich ihre Einwilligung gegeben hat (Art. 6 Abs. 1 a) DSGVO)

oder

2. eine gesetzliche Erlaubnis gemäß Art. 6 Abs. 1 b) bis f) DSGVO vorliegt.



Rechtsgrundlagen der Datenverarbeitung nach Artikel 6 DSGVO im Verein



Wirtschaftsprüfungsgesellschaft

Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen insbesondere Art. 6 Abs. 1 lit. b) und lit. f) DSGVO in Betracht.

Die Mitgliedschaft in einem Verein ist als Vertragsverhältnis zwischen den Mitgliedern und dem Verein anzusehen, dessen Inhalt im Wesentlichen durch die Vereinssatzung und sie ergänzende Regelungen (z.B. eine Vereinsordnung) vorgegeben wird. Eine Vereinssatzung bestimmt insoweit die Vereinsziele, für welche die Mitgliederdaten genutzt werden können.



Rechtmäßigkeit der Datenverarbeitung nach Artikel 6 DSGVO sowie Umfang



Wirtschaftsprüfungsgesellschaft

Ein Verein darf aufgrund des Art. 6 Abs. 1 lit. b) DSGVO beim Vereinsbeitritt (Aufnahmeantrag oder Beitrittserklärung) und während der Vereinsmitgliedschaft (nur) solche Daten von Mitgliedern erheben, die für die Begründung und Durchführung des zwischen Mitglied und Verein durch den Beitritt zustande kommenden rechtsgeschäftsähnlichen Schuldverhältnisses erforderlich sind. Damit dürfen alle Daten erhoben werden, die zur Verfolgung der Vereinsziele und für die Betreuung und Verwaltung der Mitglieder (wie etwa Name, Anschrift, in der Regel auch das Geburtsdatum, ferner Bankverbindung, Bankleitzahl und Kontonummer) notwendig sind. (Berechtigung im Kontext Datensparsamkeit /Datenminimierung)



Datenübermittlung an Dachverbände und andere Vereine



Wirtschaftsprüfungsgesellschaft

Dachverbände, bei denen ein Verein Mitglied ist, sind im Verhältnis zu seinen Mitgliedern datenschutzrechtlich Dritte. Personenbezogene Daten der eigenen Mitglieder dürfen an andere Vereine im Rahmen der Erforderlichkeit nur übermittelt werden, soweit diese dort benötigt werden, um die Vereinsziele des übermittelnden Vereins oder um die Ziele des anderen Vereins zu verwirklichen, etwa bei der überregionalen Organisation eines Turniers, und sofern keine Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (Art. 6 Abs. 1 lit. b) und lit f) DSGVO)



„Zweckbindung“

Artikel 5 Abs. 1b) DSGVO



Wirtschaftsprüfungsgesellschaft

Gemäß Art. 5 Abs. 1b) DSGVO darf die Verarbeitung personenbezogener Daten nur für „festgelegte, eindeutige und legitime Zwecke“ erfolgen.

Eine Änderung des Verarbeitungszwecks ist grundsätzlich nur dann erlaubt, wenn sie mit dem ursprünglichen Erhebungszweck vereinbar ist.

Bei einer Änderung des Verarbeitungszweckes ist Art. 6 Abs. 4 DSGVO heranzuziehen, der Kriterien für die Beurteilung einer rechtmäßigen Datenverarbeitung bei Änderung des Verarbeitungszweckes aufstellt.



„Datensparsamkeit“

Artikel 5 Abs. 1c) DSGVO



Wirtschaftsprüfungsgesellschaft

Die Verarbeitung personenbezogener Daten muss gem. Art. 5 Abs. 1c) DSGVO „dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein“. Dieses Prinzip der Datenminimierung findet sich bereits in § 3a BDSG-alt und ist als zentraler Grundsatz des Datenschutzrechts in die DSGVO aufgenommen worden.

Aus „Datensparsamkeit“ wurde laut ausdrücklicher Erwähnung im Verordnungstext „Datenminimierung“



„Datensicherheit“

Artikel 5 Abs. 1f), Artikel 32 DSGVO



Wirtschaftsprüfungsgesellschaft

Die Gewährleistung der Datensicherheit ist ebenfalls in die DSGVO aufgenommen worden. Regelungen hierzu finden sich in Art. 5 Abs. 1f) und in Art. 32 DSGVO. Art. 32 DSGVO regelt die Pflicht des Verantwortlichen, Sicherheitsmaßnahmen im Zusammenhang mit der Verarbeitung personenbezogener Daten zu ergreifen. Dabei sind u.a. die Art, Umstände und der Zweck der Datenverarbeitung zu berücksichtigen, ebenso die Eintrittswahrscheinlichkeit und die Schwere des Risikos im Hinblick auf die Persönlichkeitsrechte des Betroffenen. Art. 32 Abs. 1 DSGVO nennt einzelne Maßnahmen, wie z.B. die Pseudonymisierung und die Verschlüsselung personenbezogener Daten.



Datenschutzverantwortung



Wirtschaftsprüfungsgesellschaft

Nach Art 5 Abs. 2 DSGVO hat der Verantwortliche die Einhaltung der Datenschutzvorschriften zu gewährleisten und muss diese nachweisen können.

Bei einem Verein ist der Vereinsvorstand verantwortlich, der den Verein nach § 26 Abs. 1 Satz 2 BGB nach außen vertritt. Bei ihm liegt daher die Datenschutzverantwortung in Bezug auf die Verwaltung der Mitgliedsdaten.



RECHENSCHAFTSPFLICHT nach Art 5 Abs. 2 DSGVO



Rechenschaftspflicht des Verantwortlichen / Abgrenzung zum Pflichtenkreis des Datenschutzbeauftragten



Wirtschaftsprüfungsgesellschaft

Art 5 Absatz 2 DSGVO (Textauszug):

„Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“

Wer ist Verantwortlicher?

Grundsatz : „Datenschutz ist Chefsache“



Datenschutzbeauftragter



Wirtschaftsprüfungsgesellschaft

Wenn mindestens 10 Personen im Verein ständig mit der Verarbeitung von Daten betraut sind, muss ein Datenschutzbeauftragter benannt werden (Art. 38 Abs. BDSG neu).

Diese Regelung galt bereits bisher, jedoch wurden die zukünftigen Aufgaben des Datenschutzbeauftragten verschärft. Aufgaben des Datenschutzbeauftragten sind u.a. „Beratung des Verantwortlichen“, die „Überwachung der Einhaltung der Verordnung“ sowie „Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter“ und die „Zusammenarbeit mit der Aufsichtsbehörde“.

Siehe auch: Kurzpapier Nr. 12 Datenschutzkonferenz „Datenschutzbeauftragte...“



Schaubild Notwendigkeit eines Datenschutzbeauftragten



Informationspflichten / Grundsätze



Wirtschaftsprüfungsgesellschaft

Der Verein ist verpflichtet, die Personen, deren Daten er verarbeitet, umfangreich zu informieren. Art. 13 DSGVO gibt hierzu eine genaue Liste der Informationen vor, die „der betroffenen Person zum Zeitpunkt der Erhebung“ mitzuteilen sind. Sofern diese Informationen den Personen, von denen bereits Daten erhoben wurden, noch nicht zur Verfügung gestellt wurden, muss dies aktiv durch den Verein (vor dem 25.5.2018) erfolgen.

Teilt der Verantwortliche die vorgesehenen Informationen nicht, nicht vollständig oder inhaltlich unrichtig mit, so verletzt er seine Informationspflichten. Das ist gemäß Art. 83 Abs. 5 lit. b) DSGVO bußgeldbewehrt.



Informationspflichten / Inhalt



Wirtschaftsprüfungsgesellschaft

- * Name und Kontaktdaten des Verantwortlichen sowie ggf. seines Vertreters
- * Kontaktdaten des Datenschutzbeauftragten
- * Zwecke der Verarbeitung (im Einzelnen aufzählen), insbesondere Darstellung berechtigter Interessen im Sinne des Art. 6 Abs. 1 lit. f) DSGVO
- * Rechtsgrundlage der Verarbeitung
- * Empfänger oder Kategorien von Empfängern (z.B. Weitergabe personenbezogener Daten an eine Versicherung, an den Dachverband, an alle Vereinsmitglieder, im Internet)
- * Absicht über Drittlandtransfer (z.B. bei Mitgliederverwaltung in der Cloud), sowie Hinweis auf (Fehlen von) Garantien zur Datensicherheit
- * Speicherdauer der personenbezogenen Daten
- * Belehrung über Betroffenenrechte (Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht gegen Verarbeitung)
- * Hinweis auf jederzeitiges Widerrufsrecht der Einwilligung
- * Hinweis auf Beschwerderecht bei einer Aufsichtsbehörde

Siehe auch: Kurzpapier Nr. 10 Datenschutzkonferenz „Informationspflichten bei Dritt- und Direkterhebung“



Meldepflicht bei DS-Verletzungen



Wirtschaftsprüfungsgesellschaft

Nach Art. 33 Abs. 1 DSGVO besteht nun 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.

Dies bedeutet, dass jeder Verein im Vorfeld einen Prozess, ein Muster für die Meldung und die zuständige Person bestimmen sollte. Mindestinhalte der Meldung sind in Art 33 Abs. 3 DSGVO geregelt.

Siehe auch: Bayerisches Landesamt für Datenschutzaufsicht „Umgang mit Datenpannen“

→ www.lida.bayern.de



Auskunftsrecht nach Art 15 DSGVO

Nach Art. 15 Abs. 1 DSGVO steht betroffenen Personen ein Auskunftsrecht zu. Zum einen kann die betroffene Person von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene Daten verarbeitet werden. Auch eine Negativauskunft ist erforderlich, wenn keine Daten verarbeitet oder personenbezogene Daten unumkehrbar anonymisiert wurden.

Zum anderen kann die betroffene Person ganz konkret Auskunft darüber verlangen, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden (z. B. Name, Vorname, Anschrift, Geburtsdatum, Beruf, medizinische Befunde).

Siehe auch: Kurzpapier Nr. 6 Datenschutzkonferenz „Auskunftsrecht der betroffenen Person, Art. 15 DS-GVO“

→ www.bfdi.bund.de

Datenschutzhinweis in der Beitrittserklärung eines Vereins (Bsp.)



Wirtschaftsprüfungsgesellschaft

Datenschutz:

Ich erkläre mich damit einverstanden, dass vorstehende Daten für vereinsinterne Zwecke in einer EDV-gestützten Mitglieder- und Beitragsdatei gespeichert werden. Im Übrigen wird auf § ... der Vereinssatzung verwiesen. Ohne dieses Einverständnis kann eine Mitgliedschaft nicht begründet werden.



Beispiel für eine Datenschutzklausel in der Vereinssatzung



Wirtschaftsprüfungsgesellschaft

§ ... Beginn der Mitgliedschaft – Datenschutz

(1) Mit dem Beitritt erklärt sich das Mitglied einverstanden, dass die im Zusammenhang mit der Mitgliedschaft benötigten personenbezogenen Daten unter Berücksichtigung der Vorgaben des Bundesdatenschutzgesetzes und der Datenschutz-Grundverordnung per EDV für den Verein erhoben, verarbeitet und genutzt werden. Dabei handelt es sich um: Name, Anschrift, Familienstand, Beruf, Telefon, Abteilung und Bankverbindung. Ohne dieses Einverständnis ist eine Aufnahme in den Verein nicht möglich.

(2) Die überlassenen personenbezogenen Daten dürfen ausschließlich für Vereinszwecke verwendet werden. Hierzu zählen insbesondere die Mitgliederverwaltung, die Durchführung des Sport- und Spielbetriebs, die Veröffentlichung in der Vereinszeitung sowie interne Aushänge am „Schwarzen Brett“. Eine anderweitige Verarbeitung oder Nutzung, insbesondere die Übermittlung an Dritte, ist zulässig, soweit sie der Erfassung oder der Erlangung von Start- und Spielberechtigungen beim zuständigen Sportverband dient, im Übrigen nicht zulässig.



Schriftliche Regelungen zum Datenschutz: Datenschutzordnung



Wirtschaftsprüfungsgesellschaft

Den Verein trifft die Pflicht, die Grundzüge der Datenerhebung, -verarbeitung und -nutzung schriftlich festzulegen. Entsprechende Datenschutzregelungen können entweder in die Vereinssatzung aufgenommen oder in einem gesonderten Regelwerk niedergelegt werden.

Für Letzteres gibt es keine feste Bezeichnung; am gebräuchlichsten sind noch die Begriffe „Datenschutzordnung“, „Datenschutzrichtlinie“ oder „Datenverarbeitungsrichtlinie“. Die Datenschutzordnung kann, wenn die Vereinssatzung nichts anderes bestimmt, vom Vorstand oder von der Mitgliederversammlung beschlossen werden und muss nicht die Qualität einer Satzung haben.

Auszug aus: „Datenschutz im Verein nach der Datenschutzgrundverordnung (DS-GVO)“ Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg

(Extra: Generator Grundmuster Datenschutzerklärung Internetseite -> anwalt.de)



Einwilligung zur Verwendung von Personenabbildungen (Beispiel)



Wirtschaftsprüfungsgesellschaft

Hiermit willige ich, Herr/Frau ...wohnhaft ...geb. am ...

Erziehungsberechtigte(r) von: (Name des minderjährigen Kindes)

in die Anfertigung, Nutzung und Veröffentlichung von Bildern von mir/meines minderjährigen Kindes ...durch ...ein.

Die Einwilligung gilt für die Verwendung der Fotos für nachfolgende Zwecke:

1. Veröffentlichung und Verbreitung in den Publikationen des Vereins;
2. Veröffentlichung im Internet auf den Internetseiten des Vereins;
3. Information der Presse zur Berichterstattung über ...

Die Einräumung der Rechte erfolgt vergütungsfrei und umfasst das Recht zur Bearbeitung, soweit die Bearbeitung nicht entstellend ist. Meine Einwilligung ist bei Einzelabbildungen jederzeit für die Zukunft widerruflich. Bei Mehrpersonenabbildungen ist meine Einwilligung unwiderruflich, sofern nicht eine Interessenabwägung eindeutig zu meinen Gunsten ausfällt. Im Fall des Widerrufs dürfen entsprechende Einzelabbildungen zukünftig nicht mehr für die o.g. Zwecke verwendet werden und sind unverzüglich aus den entsprechenden Veröffentlichungen zu löschen.

Ort, Datum, Unterschrift



Textauszüge DSGVO



Wirtschaftsprüfungsgesellschaft

- Art 5 Grundsätze für die Verarbeitung personenbezogener Daten
- Art 6 Rechtmäßigkeit der Verarbeitung
- Art 7 Bedingungen für die Einwilligung
- Art 8 Einwilligung eines Kindes



Artikel 5 DSGVO (Textauszug)

Grundsätze für die Verarbeitung personenbezogener Daten



Wirtschaftsprüfungsgesellschaft

(1) Personenbezogene Daten müssen

- a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);
- b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);
- c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);
- d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);
- e) 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);
- f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).



Artikel 6 DSGVO (Textauszug)

Rechtmäßigkeit der Verarbeitung



Wirtschaftsprüfungsgesellschaft

„ (1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

- a) Die betroffene Person hat ihre **Einwilligung zu der Verarbeitung** der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;
- b) die **Verarbeitung ist für die Erfüllung eines Vertrags**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen **erforderlich**, die auf Anfrage der betroffenen Person erfolgen;
- c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
- d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;
- f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung. ...“



Einwilligung Artikel 7 DSGVO (Textauszug)



Wirtschaftsprüfungsgesellschaft

Bedingungen für die Einwilligung

- (1) Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche **nachweisen** können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.
- (2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, so muss das Ersuchen um 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. Teile der Erklärung sind dann nicht verbindlich, wenn sie einen Verstoß gegen diese Verordnung darstellen.
- (3) Die **betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen**. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
- (4) Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, muss dem Umstand in größtmöglichem Umfang Rechnung getragen werden, ob unter anderem die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung zu einer Verarbeitung von personenbezogenen Daten abhängig ist, die für die Erfüllung des Vertrags nicht erforderlich sind.



Einwilligung eines Kindes

Artikel 8 DSGVO (Auszug)



Wirtschaftsprüfungsgesellschaft

Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft

(1) Gilt Artikel 6 Absatz 1 Buchstabe a bei einem Angebot von Diensten der Informationsgesellschaft, das einem Kind direkt gemacht wird, so ist die Verarbeitung der personenbezogenen Daten des Kindes **rechtmäßig, wenn das Kind das sechzehnte Lebensjahr vollendet hat**. Hat das Kind noch nicht das sechzehnte Lebensjahr vollendet, so ist diese Verarbeitung nur rechtmäßig, sofern und soweit diese **Einwilligung durch den Träger der elterlichen Verantwortung für das Kind** oder mit dessen Zustimmung erteilt wird.

...



Weiterführende Informationen / Quellen



Wirtschaftsprüfungsgesellschaft

Quelle	
<ul style="list-style-type: none"> - Datenschutzgrundverordnung - DSGVO mit Erwägungsgründen - Bundesdatenschutzgesetz BDSG (neu) 	
<p>Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg www.baden-wuerttemberg.datenschutz.de</p>	<p>„Orientierungshilfe für Vereine unter der Datenschutz-Grundverordnung“ Datenschutz im Verein nach der Datenschutzgrundverordnung (DSGVO)</p>
<p>Dr. Thomas Schwenke datenschutz-generator.de</p>	<p>Generator für DSGVO-Datenschutzerklärungen – Lizenz für Unternehmen, kostenlos für Privatpersonen, z.B. Blogger und Kleinunternehmer.</p>
<p>Datenschutzkonferenz Website: www.bfdi.bund.de</p>	<p>Kurzpapiere der Datenschutzkonferenz zu diversen Themen</p>
<p>Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen www.lidi.nrw.de</p>	<p>Datenschutz-Grundverordnung im Verein Fragen an die Landesbeauftragte für Datenschutz Nordrhein-Westfalen Umfangreiche Hinweise + Verlinkung auf Kurzpapiere der Datenschutzkonferenz (DS Behörden Bund und Länder)</p>



Erforderliche Maßnahmen



Wirtschaftsprüfungsgesellschaft

Das Bayerische Landesamt für Datenschutzaufsicht hat in einem Zehn-Punkte-Papier exemplarisch für einen Verein die wesentlichen DSGVO-Anforderungen zusammengestellt. Die Zusammenstellung kann als Muster herangezogen werden, um die aktuell notwendigen Schritte zur Erfüllung der Anforderungen nach der DSGVO zu gewährleisten. (**ANLAGE 1 zu dieser Präsentation**)

Zu den Einzelpunkten werden jeweils unter Verlinkung auf die entsprechenden Kurzpapiere der Datenschutzkonferenz umfangreiche Erläuterungen gegeben.

Wesentliche Punkte sind dabei:

- die Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten Art 30 DSGVO,
- die Datenschutzverpflichtung von Beschäftigten sowie
- die Anpassung der Verträge zur Auftragsverarbeitung

Siehe hierzu: Darstellungen Bayerisches Landesamt für Datenschutzaufsicht unter www.la.da.bayern.de



Vielen Dank für Ihre Aufmerksamkeit



Wirtschaftsprüfungsgesellschaft



Kontakt:

Wolfram Bauerhorst
Rechtsanwalt (Syndikusanwalt)
Fachanwalt für Steuerrecht

WPK Beratung GmbH
Wirtschaftsprüfungsgesellschaft
Steuerberatungsgesellschaft
Heinz-Fangman-Straße 4, 42287 Wuppertal

Telefon: 0202 / 269 106 - 32
Telefax: 0202 / 269 106 - 88

wolfram.bauerhorst@w-pk.de



Anlagen / Verweise



Wirtschaftsprüfungsgesellschaft

-
- Anlage 1: Arbeitspapier „Anforderungen der Datenschutz-Grundverordnung“ (www.lida.bayern.de)
 - Anlage 2: Muster zu einem Verzeichnis von Verarbeitungstätigkeiten im Verein (www.lida.bayern.de)
 - Anlage 3: Beispiel ausführliches Verarbeitungsverzeichnis (www.lida.bayern.de)
 - Anlage 4: Verweis (screenshot) auf www.anwalt.de zu Muster-Datenschutzerklärung





Anforderungen der Datenschutz-Grundverordnung (DS-GVO) an kleine Unternehmen, Vereine, etc.

Muster 1: Verein

Hinweis:

Jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet, ist ein sog. *Verantwortlicher*. Dieser ist insb. dafür verantwortlich, dass er die Anforderungen der DS-GVO einhält. In der folgenden Übersicht werden die *wesentlichen* Anforderungen exemplarisch zusammengestellt – ohne Anspruch auf Vollständigkeit. Zu beachten ist daher, dass nicht jeder Verantwortliche pauschal alle diese Anforderungen erfüllen muss und sich auch der Umfang, wie die einzelnen Anforderungen konkret berücksichtigt werden müssen, fallbezogen unterscheidet. In diesem Muster wird deshalb der vereinfachte Regelfall angenommen. Erläuterungen zu den jeweiligen Anforderungen sind auf der Rückseite dieses Papiers zu finden.

Kurzbeschreibung des Vereins

Ein kleiner Sportverein hat 200 Mitglieder, einen ersten Vorstand, einen Kassier sowie einen Schriftführer (Vorstand im Sinne des BGB) sowie fünf Personen, die nach der sog. Übungsleiterpauschale bezahlt werden. Die Mitgliederverwaltung erfolgt durch den Schriftführer selbst. Die Verwaltung der Mitgliedsbeiträge erfolgt dagegen durch den Kassier. Der Verein betreibt zudem eine kleine Webseite, die bei einem Dienstleister gehostet ist, mit Mitgliederfotos.

Wesentliche Verarbeitungstätigkeiten sind z. B.:

- Lohnabrechnung (über einen externen Dienstleister)
- Mitgliederverwaltung
- Betrieb der Webseite des Sportvereins (über Hosting-Paket eines externen Dienstleisters)
- Veröffentlichung von Mitgliederfotos auf der eigenen Webseite
- Beitragsverwaltung

Wesentliche DS-GVO-Anforderungen für den Verein

A Datenschutzbeauftragter (DSB)

Muss ein DSB vom Verein benannt werden?

- ja
 nein (weniger als 10 Personen im regelmäßigen Umgang mit personenbezogenen Daten)

B Verzeichnis von Verarbeitungstätigkeiten

Ist ein solches Verzeichnis erforderlich?

- ja (wegen der regelmäßigen Verarbeitung personenbezogener Daten)
 nein

C Datenschutz-Verpflichtung von Beschäftigten

Ist eine solche Verpflichtung durchzuführen?

- ja (da alle Mitarbeiter mit personenbezogenen Daten umgehen)
 nein

D Information- und Auskunftspflichten

Bestehen irgendwelche Informationspflichten?

- ja (insb. in der Vereinssatzung sowie auf der Webseite in der Datenschutzerklärung)
 nein

E Löschen von Daten

Gibt es eine Anforderung zur Datenlöschung?

- ja (aber erst nach Ablauf gesetzlicher Aufbewahrungspflichten)
 nein

F Sicherheit

Müssen die Daten besonders gesichert werden?

- ja
 nein (etablierte Standardmaßnahmen sind ausreichend, um die Daten effektiv zu schützen)

G Auftragsverarbeitung

Ist ein Vertrag zur Auftragsverarbeitung notwendig?

- ja (sowohl mit dem Hosting-Anbieter als auch mit dem externen Lohnabrechner)
 nein

H Datenschutzverletzungen

Müssen bestimmte Vorfälle gemeldet werden?

- ja (aber nur bei relevanten Risiken – eine einfache Online-Meldung beim BayLDA ist möglich)
 nein

I Datenschutz-Folgeabschätzung (DSFA)

Muss eine DSFA vom Verein durchgeführt werden?

- ja
 nein (da kein hohes Risiko bei der Datenverarbeitung im Verein besteht)

J Videoüberwachung (VÜ)

Besteht eine Ausschilderungspflicht bezüglich VÜ?

- ja
 nein (da keine Videoüberwachung im Verein durchgeführt wird)



📘 Erläuterungen zu den Anforderungen

A Datenschutzbeauftragter (DSB)

In aller Regel ist nur dann ein DSB zu benennen, wenn *mindestens 10 Personen* ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind. „Ständig beschäftigt“ ist, wer z. B. permanent Mitgliederverwaltung macht – „nicht ständig beschäftigt“ ist dagegen bspw., wer als Übungsleiter nur mit den Namen seiner Mannschaft umgeht.

⇒ DSK-Kurzpapier Nr. 12: www.lda.bayern.de/media/dsk_kpnr_12_datenschutzbeauftragter.pdf

B Verzeichnis von Verarbeitungstätigkeiten

Vereine, die regelmäßige Mitgliederverwaltung und Beitragsabrechnung machen, müssen ein – vom Umfang her sehr überschaubares – Verzeichnis ihrer Verarbeitungstätigkeiten führen.

⇒ BayLDA Muster-Verzeichnis für kleine Vereine: www.lda.bayern.de/media/muster_1_verein_verzeichnis.pdf

⇒ DSK-Kurzpapier Nr. 1: www.lda.bayern.de/media/dsk_kpnr_1_verzeichnis_verarbeitungstaetigkeiten.pdf

⇒ DSK-Muster-Verzeichnis allgemein: www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf

C Datenschutz-Verpflichtung von Beschäftigten

Bei der Aufnahme der Tätigkeit sind Beschäftigte, die mit personenbezogenen Daten umgehen, zu informieren und dahingehend zu verpflichten, dass die Verarbeitung der personenbezogenen Daten auch durch sie nach den Grundsätzen der DS-GVO erfolgt.

⇒ BayLDA Info-Blatt zur Verpflichtung: www.lda.bayern.de/media/info_verpflichtung_beschaefigte_dsgvo.pdf

D Informations- und Auskunftspflichten

Jeder Verantwortliche hat den betroffenen Personen schon bei der Datenerhebung bestimmte Informationen über die Verarbeitung ihrer Daten zu geben. Ein Verein muss bspw. Informationen auf der Homepage und der Satzung leicht zugänglich bereithalten. Die betroffenen Personen (z. B. Vereinsmitglieder) haben auch das Recht, Auskunft über die Verarbeitung ihrer Daten zu erhalten.

⇒ DSK-Kurzpapier Nr. 6: www.lda.bayern.de/media/dsk_kpnr_6_auskunftsrecht.pdf

⇒ DSK-Kurzpapier Nr. 10: www.lda.bayern.de/media/dsk_kpnr_10_informationspflichten.pdf

E Löschen von Daten

Sobald keine gesetzliche Grundlage (z. B. steuerliche Aufbewahrungspflicht) mehr für die Speicherung von personenbezogenen Daten besteht, sind diese zu löschen. In der Regel ist dies bspw. erst der Fall nach Ausscheiden eines Vereinsmitglieds.

⇒ DSK-Kurzpapier Nr. 11: www.lda.bayern.de/media/dsk_kpnr_11_vergessenwerden.pdf

F Sicherheit

Um die personenbezogenen Daten bei der Verarbeitung zu schützen, sind Standardmaßnahmen im Regelfall ausreichend. Dazu gehören u.a. aktuelle Betriebssysteme und Anwendungen, Passwortschutz, regelmäßige Backups, Virens Scanner und Benutzerrechte. Soweit private PCs genutzt werden, ist sicherzustellen, dass nur berechtigte Personen auf die Daten zugreifen können.

⇒ BayLDA-Kurzpapier Nr. 1: www.lda.bayern.de/media/baylda_ds-gvo_1_security.pdf

G Auftragsverarbeitung

Sobald Verantwortliche Dienstleistungen (z. B. Buchhaltung) in Anspruch nehmen, um personenbezogene Daten in ihrem Auftrag durch andere Unternehmen verarbeiten zu lassen, ist ein schriftlicher Vertrag zur Auftragsverarbeitung erforderlich.

⇒ DSK-Kurzpapier Nr. 13: www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf

⇒ BayLDA-Formulierungshilfe zum Vertrag: www.lda.bayern.de/media/muster_adv.pdf

H Datenschutzverletzungen

Kommt es bei der Verarbeitung personenbezogener Daten zu Sicherheitsvorfällen (z. B. Diebstahl, Hacking, Fehlversendung, Verlust von Geräten mit unverschlüsselten Vereinsdaten), so bestehen gesetzliche Meldepflichten: Die Aufsichtsbehörde ist im Regelfall darüber in Kenntnis zu setzen, betroffene Personen dagegen nur bei hohem Risiko.

⇒ BayLDA-Kurzpapier Nr. 8: www.lda.bayern.de/media/baylda_ds-gvo_8_data_breach_notification.pdf

⇒ BayLDA-Online-Service zur Meldung: www.lda.bayern.de/de/datenpanne.html

I Datenschutz-Folgeabschätzung (DSFA)

Hat eine Verarbeitung personenbezogener Daten ein hohes Risiko für die betroffenen Personen, so muss das spezielle Instrument der Datenschutz-Folgenabschätzung durchgeführt werden. Ein solch hohes Risiko ist jedoch der Ausnahmefall und nicht die Regel.

⇒ DSK-Kurzpapier Nr. 5: www.lda.bayern.de/media/dsk_kpnr_5_dsfa.pdf

J Videoüberwachung

Führt ein Verantwortlicher eine Videoüberwachung durch, ist im Normalfall eine entsprechende Hinweisbeschilderung erforderlich, um die betroffenen Personen über die Videoaufnahmen zu informieren.

⇒ DSK-Kurzpapier Nr. 15: www.lda.bayern.de/media/dsk_kpnr_15_videoeuberwachung.pdf



Muster 1: Verein – Verzeichnis von Verarbeitungstätigkeiten

Verantwortlicher:

TSV Waldermühl e.V.
Steinbauerstr. 45a
98123 Sonsthausen

Tel. 0981/123456-0
E-Mail: team@waldermuehler-tsv.de
Web: www.waldermuehler-tsv.de

Vorstand: Dieter Eckbauer-Düppels, geb. 03.12.1952

Verarbeitungstätigkeit	Ansprechpartner	Datum der Einführung	Zwecke der Verarbeitung	Kategorie betroffene Personen	Kategorie von personenbez. Daten	Kategorie von Empfängern	Drittlands-transfer	Löschfristen	Technische/organisatorische Maßnahmen
Lohnabrechnung (über externen Dienstleister)	Herbert Bauer 0981/123456-1 herbert@waldmuehler-tsv.de	02.03.2018	<ul style="list-style-type: none"> Auszahlung der Löhne/Gehälter Abfuhr Sozialabgaben u. Steuern 	Beschäftigte	<ul style="list-style-type: none"> Name und Adressen der Beschäftigten ggf. Religionszugehörigkeit Eindeutige Kennzahlen zur Steuer/ Sozialabgaben 	Externer Dienstleister	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
Mitgliederverwaltung	Herbert Bauer 0981/123456-1 herbert@waldmuehler-tsv.de	02.03.2018	Verwaltung der Vereinstätigkeiten	Mitglieder	<ul style="list-style-type: none"> Name und Adressen Eintrittsdatum Sportbereiche 	Keine	Keine	2 Jahre nach Beendigung der Vereinsmitgliedschaft	Siehe IT-Sicherheitskonzept
Betrieb der Webseite des Sportvereins (über Hosting-Dienstleister)	Max Meier 0981/123456-0 max@waldmuehler-tsv.de	28.02.2018	Außendarstellung	<ul style="list-style-type: none"> Mitglieder Webseitenbesucher 	IP-Adressen	Keine	Keine	IP-Adresse nach 30 Tagen	Siehe IT-Sicherheitskonzept + HTTPS-Verschlüsselung
Veröffentlichung von Fotos der Mitglieder auf der Webseite	Max Meier 0981/123456-0 max@waldmuehler-tsv.de	20.02.2018	Außendarstellung	Mitglieder	Fotos von Vereinstätigkeiten	Keine	Keine	Wenn Einwilligung widerrufen - unverzüglich	Siehe IT-Sicherheitskonzept
Beitragsverwaltung	Herbert Bauer 0981/123456-1 herbert@waldmuehler-tsv.de	22.02.2018	Vereinsfinanzierung	Mitglieder	Bankverbindung	Steuerberater	Keine	10 Jahre (Gesetzliche Aufbewahrungsfrist)	Siehe IT-Sicherheitskonzept
...

Auszug aus dem IT-Sicherheitskonzept (enthält technische und organisatorische Maßnahmen):

- ✓ Automatische Updates im Betriebssystem aktivieren
- ✓ Standard-Gruppenverwaltung (z. B. in Windows)
- ✓ Automatische Updates des Browsers aktivieren
- ✓ Aktueller Virenschanner/Sicherheitssoftware
- ✓ Backups regelmäßig, z. B. einmal wöchentlich auf externe Festplatte
- ✓ Papieraktenvernichtung mit Standard-Shredder

Verzeichnis von Verarbeitungstätigkeiten Verantwortlicher gem. Artikel 30 Abs. 1 DSGVO	Vorblatt
Angaben zum Verantwortlichen Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc. Name Straße Postleitzahl Ort Telefon E-Mail-Adresse Internet-Adresse	
Angaben zum ggf. gemeinsam mit diesem Verantwortlichen Name Straße Postleitzahl Ort Telefon E-Mail-Adresse	
Angaben zum Vertreter des Verantwortlichen Name und Kontaktdaten natürliche Person/juristische Person/Behörde/Einrichtung etc. Name Straße Postleitzahl Ort Telefon E-Mail-Adresse	
Angaben zur Person des Datenschutzbeauftragten * (extern mit Anschrift) * sofern gem. Artikel 37 DS-GVO benannt Anrede Titel Name, Vorname Straße Postleitzahl Ort Telefon E-Mail-Adresse	

Verarbeitungstätigkeit:		lfd. Nr.:
Benennung: _____		_____
Datum der Einführung:		Datum der letzten Änderung:
Verantwortliche Fachabteilung Ansprechpartner Telefon E-Mail-Adresse (Art. 30 Abs. 1 S. 2 lit a)		
Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b)		
Optional: Name des eingesetzten Verfahrens		
Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c)	<input type="checkbox"/> Beschäftigte <input type="checkbox"/> Interessenten <input type="checkbox"/> Lieferanten <input type="checkbox"/> Kunden <input type="checkbox"/> Patienten <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	
Beschreibung der Kategorien von personenbezogenen Daten (Art. 30 Abs. 1 S. 2 lit. c)	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> Besondere Kategorien personenbezogener Daten (Art. 9): <input type="checkbox"/>	

Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offen gelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d)	<input type="checkbox"/> intern (Zugriffsberechtigte) Abteilung/ Funktion
	<input type="checkbox"/> extern Empfängerkategorie
	<input type="checkbox"/> Drittland oder internationale Organisation (Kategorie)
ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation (Art. 30 Abs. 1 S. 2 lit. e)	<input type="checkbox"/> Datenübermittlung findet nicht statt und ist auch nicht geplant <input type="checkbox"/> Datenübermittlung findet wie folgt statt:
Nennung der konkreten Datenempfänger	<input type="checkbox"/> Drittland oder internationale Organisation (Name)
Sofern es sich um eine in Art. 49 Abs. 1 Unterabsatz 2 DS-GVO genannte Datenübermittlung handelt.	Dokumentation geeigneter Garantien
Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f)	

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 Abs.1 DSGVO (Art. 30 Abs. 1 S. 2 lit. g)
Siehe TOM-Beschreibung in den „Hinweisen zum Verzeichnis von Verarbeitungstätigkeiten“, Ziff. 6.7. und 6.8

.....
 Verantwortlicher

.....
 Datum

.....
 Unterschrift



Muster-Datenschutzerklärung für Websites

Websites speichern inzwischen immer mehr Daten von Usern. Nicht nur durch Formulare oder Shop-Systeme, sondern auch über verschiedene eingebundene Tools und Funktionen (z. B. Google Analytics oder Facebook) werden Daten von Besuchern verarbeitet. Über die Nutzung und Speicherung der Daten muss der User laut Datenschutzrecht und TMG informiert werden.

Mit unserer Muster-Datenschutzerklärung bieten wir Ihnen ein nützliches Tool, um sich eine eigene Datenschutzerklärung mit nur wenigen Klicks selbst zu erstellen.

Datenschutzerklärung erstellen

Bitte wählen Sie hier die für Sie relevanten Angaben aus.

Allgemein

- Allgemeine Datenschutzerklärung
- Datenschutzerklärung für Cookies

Google

- Datenschutzerklärung für Google Analytics
- Datenschutzerklärung für Google AdSense
- Datenschutzerklärung für Google +1

Facebook

- Datenschutzerklärung für Facebook

Twitter

- Datenschutzerklärung für Twitter

[DATENSCHUTZERKLÄRUNG ERSTELLEN](#)