

Merkblatt zur Verpflichtung auf Vertraulichkeit

Alle Mitarbeiter/innen des Bayerischen Fußball-Verbandes e. V., sowie die im Bayerischen Fußball-Verband e. V. ehrenamtlich tätigen Mitarbeiter/Mitarbeiterinnen und Funktionsträger/Funktionsträgerinnen, die Daten über Einzelpersonen verarbeiten oder von diesen Daten Kenntnis erlangen, sind nach § 5 Bundesdatenschutzgesetz, bzw. ab dem 25.05.2018, nach Art 32 (4) Datenschutz-Grundverordnung auf die Vertraulichkeit verpflichtet.

Jede/r einzelne Mitarbeiter/in des Bayerischen Fußball-Verbandes e. V sowie jede/r ehrenamtlich Tätige wird bei der Aufnahme seiner/ihrer Tätigkeit auf das Datengeheimnis verpflichtet. Diese Verpflichtung besteht auch nach Beendigung der Tätigkeit fort.

Diese Verpflichtung auf das Datengeheimnis beinhaltet keinerlei Kundgabe eines Misstrauens gegenüber einzelnen Mitarbeitern/Mitarbeiterinnen oder ehrenamtlich Tätigen, sondern entspricht alleine den gesetzlichen Vorgaben des Bundesdatenschutzgesetzes (BDSG) bzw. der Datenschutz-Grundverordnung (DSGVO). Für die Ausführungen in diesem Merkblatt gelten die in der Anlage beigefügten Hinweise und Begriffsbestimmungen.

Keine im Bayerischen Fußball-Verbandes e. V tätige Person, gleichgültig ob Mitarbeiter/Mitarbeiterin oder ehrenamtlich Tätige/r darf personenbezogene Daten unbefugt zu einem anderen, als dem zur jeweiligen rechtmäßigen vertraglichen Aufgabenerfüllung gehörenden Zweck erheben, verarbeiten, anderen bekannt bzw. zugänglich machen oder in sonstiger Weise nutzen. Auch darf nicht absichtlich oder unabsichtlich die Sicherheit der Verarbeitung so verletzt werden, dass es zu Vernichtung, Verlust, Veränderung, unbefugter Offenlegung oder unbefugtem Zugang zu den personenbezogenen Daten kommt.

Personenbezogene Daten dürfen auch nicht für private Zwecke genutzt werden. Deshalb ist es grundsätzlich verboten, personenbezogene Daten des Unternehmens auf Datenträger, USB-Sticks, Hotspots, Online-Speichermedien (Clouds), Dropbox oder mobile DV-Systeme (Notebooks) zu kopieren und diese Datenträger aus dem Unternehmen herauszubringen. Auch die Anfertigung von Screenshots ist nicht zulässig.

Ferner werden alle Mitarbeiter/innen des Bayerischen Fußball-Verbandes e. V., sowie die im Bayerischen Fußball-Verband e. V. ehrenamtlich tätigen Mitarbeiter/innen und Funktionsträger/innen, darüber belehrt, dass die Daten des Bayerischen Fußball-Verbandes e. V., seiner Vereinsmitglieder und seiner Funktionäre, die aufgrund der Tätigkeit beim Bayerischen Fußball-Verband e. V. auf einem privaten Rechner übernommen werden, so handzuhaben sind, dass diese Daten vor dem Zugriff Dritter (auch Familienmitgliedern) geschützt sind. Dies gilt auch für Daten in schriftlicher Form.

Das Verbot der Bekanntgabe von personenbezogenen Daten gilt gleichermaßen für die Weitergabe dieser Daten an externe Stellen, wie auch an andere Mitarbeiter/innen des Bayerischen Fußball-Verbandes e. V, die für die Erledigung ihrer vertragsgemäßen Aufgaben diese Daten nicht benötigen.

Verstöße gegen datenschutzrechtliche Vorschriften können mit einem Bußgeld sanktioniert werden oder, falls Strafvorschriften betroffen sind, Geld- oder Freiheitsstrafen zur Folge haben. Ferner kann betroffenen Person durch die unzulässige Verarbeitung ihrer personenbezogenen Daten ein Anspruch auf Schadenersatz sowohl für materielle wie für immaterielle Schäden zustehen.

Ein Verstoß gegen die Vertraulichkeits- und Datenschutzvorschriften stellt zudem einen Verstoß gegen arbeitsvertragliche Pflichten dar, der entsprechend geahndet werden kann.

Es wird darauf hingewiesen, dass die Verpflichtung auf Einhaltung der Vertraulichkeit auch nach Ende des Beschäftigungsverhältnisses/Ehrenamtsverhältnisses fortbesteht.

Verpflichtung von Mitarbeitern auf das Datengeheimnis

Herr/Frau

erklärt:

1. In Bezug auf die Vertraulichkeit und Integrität personenbezogener Daten die Vorgaben der geltenden Datenschutzvorschriften einzuhalten.
2. Eine Kopie dieser Niederschrift und der Anlage erhalten zu haben.
3. Zur Kenntnis genommen zu haben, dass die Einhaltung dieser Verpflichtungserklärung Teil der arbeitsvertraglichen Pflichten ist und sonstige Geheimhaltungsvorschriften unberührt lässt.

Ort

Datum

Unterschrift des/der Mitarbeiters/Mitarbeiterin
bzw. des/der ehrenamtlich Tätigen

1. Original: Ablage beim BFV
2. Kopie: Mitarbeiter/in

Anlage zur Verpflichtung auf die Vertraulichkeit

Im Folgenden erhalten Sie einen groben Überblick über das datenschutzrechtliche Regelwerk und die relevantesten einschlägigen Normen. Bitte beachten Sie, dass die Darstellung lediglich exemplarisch und nicht abschließend ist.

Begriffsbestimmungen

Art. 4 Nr. 1 DS-GVO: „Personenbezogene Daten“ [sind] alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Art. 4 Nr. 2 DS-GVO: „Verarbeitung“ [meint] 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.

Grundsätze der Verarbeitung

Art. 5 Abs. 1 lit. a DS-GVO: Personenbezogene Daten müssen [...] 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“).

Art. 5 Abs. 1 lit. b) DS-GVO: Personenbezogene Daten dürfen 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“).

Art. 5 Abs. 1 lit. c) DS-GVO: dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“).

Art. 5 Abs. 1 lit. d) DS-GVO: 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“).

Art. 5 Abs. 1 lit. e) DS-GVO: 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 (Speicherbegrenzung).

Art. 5 Abs. 1 lit. f) DS-GVO: Personenbezogene Daten müssen [...] 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“).

Art. 29 DS-GVO: Der Auftragsverarbeiter und jede dem Verantwortlichen oder dem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zur Verarbeitung verpflichtet sind.

Art. 32 Abs. 2 DS-GVO: Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.

Art. 33 Abs. 1 Satz 1 DS-GVO: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der [...]

zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Haftungsregeln

Art. 82 Abs. 1 DS-GVO: Jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.

Art. 83 Abs. 1 DS-GVO: Jede Aufsichtsbehörde stellt sicher, dass die Verhängung von Geldbußen gemäß diesem Artikel für Verstöße gegen diese Verordnung [...] in jedem Einzelfall wirksam, verhältnismäßig und abschreckend ist.

Strafvorschriften

§ 42 BDSG: Strafvorschriften

(1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe wird bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer großen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
 2. auf andere Art und Weise zugänglich macht
- und hierbei gewerbsmäßig handelt.

(2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
 2. durch unrichtige Angaben erschleicht
- und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

§ 202a Abs. 1 StGB: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

§ 303a Abs. 1 StGB: Wer rechtswidrig Daten [...] löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.