MUSTER

DFB GMBH & CO. KG

Vertrag zur Auftragsverarbeitung i.S.d. Art. 28 DSGVO

zwischen

[Vereinsname]
[Vereinsanschrift]

- Nachstehend **Auftraggeber** genannt -

und

DFB GmbH & Co. KG
Kennedyallee 274
60528 Frankfurt am Main

- Nachstehend **Auftragnehmer** genannt -

Version 1.1 – 27.01.2022

Präambel

Im Rahmen des zwischen Auftraggeber und Auftragnehmer bestehenden Hauptvertrags erhebt, verarbeitet oder nutzt der Auftragnehmer personenbezogene Daten im Auftrag des Auftraggebers. Die Inhalte dieser Anlage gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen im Auftrag vorgenommen wird, und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Diese Auftragsverarbeitung im Sinne von Art. 28 DSGVO wird durch die nachfolgende Vereinbarung entsprechend den gesetzlichen Vorschriften konkretisiert und geregelt.

Es gelten die Begriffsbestimmungen der DSGVO.

Diese Vereinbarung wird mit ihrer Unterzeichnung wesentlicher Bestandteil des zugrundeliegenden Nutzungsvertrags, der mit Bestätigung der Allgemeinen Geschäftsbedingungen abgeschlossen wird. Gleiches gilt für alle Anlagen, auf welche diese Vereinbarung ausdrücklich Bezug nimmt.

1) Gegenstand und Dauer des Auftrags

Der Gegenstand der Auftragsverarbeitung richtet sich nach den Regelungen des zugrundeliegenden Hauptvertrages. Die Dauer des Auftrags (Laufzeit) entspricht der Laufzeit des Hauptvertrages. Die Möglichkeit zur fristlosen Kündigung bleibt hiervon unberührt.

2) Verantwortlichkeit

(1) Der Auftragnehmer verarbeitet auf Basis der vorliegenden Vereinbarung personenbezogene Daten im Auftrag des Auftraggebers. Der Auftraggeber ist der für die Datenverarbeitung Verantwortliche i.S.d. Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO).

(2) Aufgrund dieser Verantwortlichkeit kann der Auftraggeber auch während der Laufzeit des Vertrages und nach Beendigung des Vertrages die Berichtigung, Löschung, Sperrung und Herausgabe von Daten verlangen.

3) Art & Zweck der Auftragsverarbeitung, Art der Daten und Kreis der Betroffenen

(1) Art und Zweck der vorgesehenen Verarbeitung von personenbezogenen Daten durch den Auftragnehmer für den Auftraggeber sind konkret beschrieben im Hauptvertrag. Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Artt. 44 ff. DS-GVO erfüllt sind.

(2) Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenkategorien:

- Vereinsmitglieder
- Vereinsmitarbeiter
- Lieferanten
- Sponsoren
- Personen, die in einer sonstigen Geschäftsbeziehung mit dem Verein stehen, z.B. Mäzene
- Personen, die in einer sonstigen Beziehung mit dem Verein stehen, z.B. Pressekontakte, Spender

4) Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Der Auftragnehmer hat die Sicherheit dem Artt. 28 Abs. 3 lit. c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen und aufrechtzuerhalten. Dies bedeutet, dass in Abstimmung mit dem Auftraggeber solche Maßnahmen zu treffen sind, die die Datensicherheit und ein dem Risiko angemessenes

Schutzniveau hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme gewährleisten.

Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Dies beinhaltet insbesondere

die Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

a) Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die personenbezogenen Daten verarbeitet und genutzt werden, zu verwehren (Zutrittskontrolle):

Dies wird dadurch gewährleistet, dass die Verarbeitungssysteme (Server und Datenspeicher) in einem mit Zutrittskontrollsystemen ausgestatteten Rechenzentrum betrieben werden.

b) zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle):

Der Zugang zu den Daten erfolgt mit einem durch Kennung und Kennwort geschütztes Zugangsverfahren. Mit einer Kennung sind Rollen und Datenrechte verbunden. Der Anwender kann nur im Rahmen dieser Rechte auf die Daten zugreifen, Administratoren können ebenfalls nur kennwortgeschützt auf die Verarbeitungssysteme zugreifen. Für die Kennungsvergabe an Mitarbeiter des Auftraggebers ist der Auftraggeber verantwortlich.

c) dafür Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle):

Die Rollen und Rechteverwaltung erfolgt über die Benutzerverwaltung der jeweiligen Anwendung. Anwender haben nur im Rahmen ihrer Rolle Zugriff auf die Daten. Verpflichtung der Bearbeiter auf das Datenschutzgesetz und datenschutzrechtliche Belehrung. Übertragungen zum Standort des Auftraggebers bzw. der Mitarbeiter des Vereins erfolgen verschlüsselt (https).

d) dafür Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Trennungskontrolle):

Auf die Daten kann nur im Rahmen der definierten Rollen und Rechte mit Kennung und Passwort zugegriffen werden.

e) die Daten, soweit möglich pseudonym zu verarbeiten.

Die Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

f) dafür Sorge zu tragen, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle):

Übertragungen zum Standort des Vereins bzw. der Mitarbeiter des Vereins erfolgen verschlüsselt (https).

g) dafür Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem relevante personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

Wesentliche Datenveränderungen und Eingaben werden protokolliert.

h) dafür Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Vereins verarbeitet werden können (Auftragskontrolle):

Die Verarbeitung erfolgt durch den Auftraggeber selbst über einen internetbasierten Zugriff (https). Mitarbeiter des Auftragnehmers sind angewiesen nur im Auftrag des Auftraggebers tätig zu werden.

Die Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

i) dafür Sorge zu tragen, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle):

Die Daten werden durch regelmäßige Datensicherungen geschützt und auf gesicherten Online-Storagesystemen (Raid) gespeichert.

(2) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

5) Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Ist der Auftraggeber aufgrund geltender Datenschutzgesetze gegenüber einer Einzelperson verpflichtet, Auskünfte zur Erhebung, Verarbeitung oder Nutzung von Daten dieser Person zu geben, wird der Auftragnehmer den Auftraggeber dabei unterstützen, diese Informationen bereitzustellen, vorausgesetzt:

- der Auftraggeber hat den Auftragnehmer hierzu schriftlich aufgefordert und

- der Auftraggeber erstattet dem Auftragnehmer die durch diese Unterstützung entstandenen Kosten falls der Umfang über Einzelanfragen hinausgeht.

6) Weitere Pflichten des Auftragnehmers

(1) Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen Daten, soweit nicht anders vereinbart, nur im Rahmen der Weisungen des Auftraggebers einschließlich der in dieser Vereinbarung eingeräumten Befugnisse verarbeiten, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

(2) Der Auftragnehmer hat neben der Einhaltung der Regelungen diese Vereinbarung die gesetzlichen Pflichten gemäß Artt. 28 bis 33 DS-GVO einzuhalten. Diese sind insbesondere:

a) Die Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Artt. 38 und 39 DS-GVO ausübt. Der Auftragnehmer teilt auf Anforderung dem Auftraggeber die Kontaktdaten des betrieblichen Datenschutzbeauftragten mit.

b) Die Wahrung der Vertraulichkeit gemäß Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO (Datengeheimnis). Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden, sowie darüber hinaus mit den Bestimmungen dieser Vereinbarung und der aufgrund dessen erteilten Weisungen vertraut gemacht wurden. Entsprechende Nachweise hat er dem Auftraggeber auf dessen Verlangen vorzulegen. Die Verpflichtung auf das Datengeheimnis besteht auch nach Beendigung der Tätigkeit fort.

c) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diese Vereinbarung beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

d) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines

Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

e) Der Auftragnehmer wird den Auftraggeber bei dessen Datenschutz-Folgeabschätzung und bei vorherigen Konsultationen mit der Aufsichtsbehörde angemessen unterstützen.

f) Sofern die Untertsützung durch den Auftragnehmer über ein normales Maß hinausgeht kann der Auftragnehmer seine hieraus entstandenen Kosten dem Auftraggeber gegenüber geltend machen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Die Erfüllung der vorgenannten Pflichten ist vom Auftragnehmer zu kontrollieren und in geeigneter Weise nachzuweisen.

i) Der Auftragnehmer wird vom Auftraggeber zum Zwecke der Sicherstellung des Datenschutzes und der Sicherheit der DFBnet-Systeme ermächtigt, alle notwendigen Maßnahmen zu ergreifen, um Sicherheitslücken festzustellen und zu schließen. Hierzu können auch die Durchführung geplanter Eindringversuche oder die Überprüfung der Sicherheit von Kennungen und Passworten gehören. Hierdurch gewonnene Erkenntnisse dürfen ausschließlich zur Erhöhung der Sicherheit des Systems genutzt werden.

7) Unterauftragsverhältnisse

(1) Der Auftragnehmer ist berechtigt, Aufträge im Rahmen der Tätigkeiten der Auftragsverarbeitung an geeignete Unterauftragnehmer weiterzugeben. Dies gilt insbesondere für die Hosting-Leistungen des Rechenzentrumsbetriebs.

(2) Der Auftragnehmer hat die vertraglichen Vereinbarungen mit den Unterauftragnehmern so zu gestalten, dass sie den Bestimmungen dieser Vereinbarung und den dazu erteilten Weisungen zwischen Auftraggeber und Auftragnehmer entsprechen. Auf Verlangen des Auftraggebers hat der Auftragnehmer Einsicht in die bestehenden Vereinbarungen mit den Unterauftragnehmern zu gewähren.

(3) Zum Zeitpunkt des Abschlusses dieses Vertrages schon bestehende Vertragsverhältnisse mit Unterauftragnehmern sind von dieser Vereinbarung nicht berührt. Der Auftragnehmer ist aber verpflichtet auch diese bestehenden Verträge zum nächst möglichen Zeitpunkt entsprechend der Regeln dieses Vertrages anzupassen soweit dies wirtschaftlich vertretbar ist.

8) Kontrollrechte des Auftraggebers

(1) Der Auftraggeber hat das Recht, sich regelmäßig von den technischen und organisatorischen Maßnahmen des Auftragnehmers zu überzeugen und die Ergebnisse zu dokumentieren. Diese Pflicht zur Überprüfung überträgt der Auftraggeber auf seinen Fußball-Landesverband. Dieser prüft den Auftragnehmer. Der Fußball-Landesverband kann die Prüfungspflicht auf den DFB e.V. übertragen. Mit der Überprüfung durch den zuständigen Landesverband bzw. den DFB e.V. kommt der Auftraggeber seiner gesetzlichen Prüfungspflicht nach. Bei Bedarf kann er vom Fußball-Landesverband bzw. dem DFB e.V. eine Bescheinigung über die Durchführung der Prüfung sowie das Ergebnis der Prüfung anfordern.

Die Übertragung der Überprüfungspflicht schließt nicht aus, dass der Auftraggeber auch selbst die Überprüfung durchführen kann.

(2) Für den Fall, dass der Auftraggeber die Prüfung selbst durchführt, verpflichtet sich der Auftragnehmer dem Auftraggeber auf schriftliche Anforderung innerhalb einer angemessenen Frist alle Auskünfte zu geben, die zur Durchführung einer Kontrolle erforderlich sind. Die Kosten des Verfahrens trägt der Auftraggeber.

(3) Die Kontrolle kann gemeinschaftlich mit den anderen Verbänden, die DFBnet nutzen, durch einen von den Verbänden benannten Verantwortlichen durchgeführt werden. Die Dokumentation kann durch

ein gemeinsames Testat erfolgen. Ist der Auftraggeber nicht Mitglied in einem Fußball-Landesverband kann er von der Möglichket Gebrauch machen, die Überprüfung selbst durchzuführen.

9) Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) dem Auftraggeber Meldung zu erteilen, wenn durch ihn oder die bei ihm beschäftigten Personen Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Auftraggebers oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind oder für deren bevorstehendes Auftreten konkrete Anhaltspunkte vorliegen. Die Meldung hat unverzüglich mit Bekanntwerden des Verstoßes bzw. der Anhaltspunkte, aber mindestens innerhalb von 48 Stunden zu erfolgen und hat alle Informationen zu enthalten, um den Auftraggeber in die Lage zu versetzten, die Meldepflicht gemäß Artt. 33 und 34 DS-GVO zu beurteilen, die möglichen Folgen einzuschätzen und entsprechende Gegenmaßnahmen einzuleiten.

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

10) Rechte und Pflichten des Auftraggebers; Weisungsbefugnis

(1) Der Auftraggeber hat das Recht, dem Auftragnehmer hinsichtlich der Auftragsverarbeitung Weisungen zu erteilen. Die Erteilung von Weisungen hat mindestens in Textform zu erfolgen.

(2) Der Auftraggeber ist bezüglich der zu verarbeitenden Daten für die Einhaltung der einschlägigen Datenschutzgesetze verantwortlich. Ebenso verpflichtet sich der Auftraggeber zur Einhaltung der Bestimmungen der AGB der DFB GmbH & Co. KG zur Nutzung von DFBnet Verein und DFBnet Finanz. Der Auftraggeber sichert zu, Inhaber der Rechte zu sein, über die er vertraglich verfügt.

(3) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er bei der Prüfung der Auftragsergebnisse Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(4) Der Auftraggeber legt die Maßnahmen zur Rückgabe der überlassenen Datenträger und/oder Löschung der gespeicherten Daten nach Beendigung des Auftrages vertraglich oder durch Weisung fest.

11) Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen

oder datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

12) Informationspflichten, Schriftformklausel, Rechtswahl

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren. Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit an den Daten ausschließlich beim Auftraggeber als „Verantwortlichem“ im Sinne der DS-GVO.

(2) Änderungen und Ergänzungen dieser Anlage und aller ihrer Bestandteile - einschließlich etwaiger Zusicherungen dem Auftragnehmer - bedürfen einer schriftlichen Vereinbarung und des ausdrücklichen Hinweises darauf, dass es sich um eine Änderung bzw. Ergänzung dieser Bedingungen handelt. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Alle Bestimmungen des Vertrags im Übrigen bleiben unberührt. Das gilt auch und insbesondere für die Regelung zum Gerichtsstand, Erfüllungsort, zum geltenden Recht und für die salvatorische Klausel.

Für den Auftraggeber

Vertragsabschluss online durch:
Datum (Zeitstempel):