Vereinbarung über die Auftragsverarbeitung von personenbezogenen Daten

ClubDesk für Vereine im Europäischen Wirtschaftsraum (EWR) (Mitgliedstaaten der Europäischen Union sowie Island, Liechtenstein und Norwegen)

zwischen dem

auftraggebenden Verein

mit Sitz im EWR

– nachstehend „Auftraggeber“ genannt –

und der

reeweb AG

Wettsteinplatz 7

4058 Basel

Schweiz

– nachstehend „Auftragnehmer“ genannt –

1. Gegenstand und Dauer des Auftrags, Anwendung der DSGVO

1.1. Gegenstand des Auftrags

Der Gegenstand des Auftrags ist die Bereitstellung der Software ClubDesk zur Verwaltung von Vereinsdaten als Dienstleistung über das Internet (Software-as-a-Service) gemäß dem online zwischen Auftraggeber und Auftragnehmer nach Maßgabe der Allgemeinen Geschäftsbedingungen abgeschlossenen Hauptvertrag.

Die inhaltliche Verwaltung der Vereinsdaten und die Verantwortung für die Zulässigkeit der Datenverarbeitung, also die Frage, ob bestimmte Daten überhaupt verarbeitet werden dürfen, obliegt dem Auftraggeber. Der Auftragnehmer verarbeitet im Rahmen der getroffenen Vereinbarungen lediglich die vom Auftraggeber eingegebenen Daten in dessen Auftrag.

Der Auftraggeber hat auch zu verantworten, ob und gegebenenfalls welche personenbezogenen Daten in Community-Foren von ClubDesk eingestellt werden dürfen. Der Auftraggeber empfiehlt, hier allenfalls den Betroffenen selbst seine personenbezogenen Daten einstellen zu lassen. Der Auftraggeber weist darauf hin, dass diese Daten von allen Nutzern des entsprechenden Community Forums, also gegebenenfalls allen Nutzern von ClubDesk, auch solchen von anderen Auftraggebern, gesehen werden können.

Die vorliegende Vereinbarung regelt in diesem Zusammenhang die Rechte und Pflichten von Auftraggeber und -nehmer im Rahmen einer Verarbeitung personenbezogener Daten im Auftrag.

1.2. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) richtet sich nach der Laufzeit des Hauptvertrags.

1.3. Anwendung der DSGVO

Für den Auftraggeber als Verein mit Sitz im Europäischen Wirtschaftsraum (EWR) gilt europäisches Datenschutzrecht, insbesondere ab dem 25.05.2018 die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutzgrundverordnung – nachstehend „DSGVO“ genannt). Für den Auftragnehmer mit Sitz in der Schweiz finden diejenigen Regelungen der DSGVO Anwendung, auf die diese Vereinbarung verweist.

1.4. Lokalisierung der Datenverarbeitung

Die Datenverarbeitung durch den Auftragnehmer erfolgt in der Schweiz. Die Europäische Kommission hat mit ihrer Entscheidung vom 26.07.2000 festgestellt, dass in der Schweiz für sämtliche unter die (Datenschutz-)Richtlinie 95/46/EG fallenden Tätigkeiten ein angemessenes Datenschutzniveau besteht (Entscheidung 200/518/EG, Amtsblatt der EG v. 25.08.2000, S. 1-3). Diese Feststellung bleibt auch unter Geltung der DSGVO nach deren Art. 45 Abs. 9 in Kraft bis gegebenenfalls eine neue Entscheidung ergeht. Die Verwaltung von Vereinsdaten fällt unter die genannte Datenschutzrichtlinie, weshalb die Schweiz auch insoweit über ein angemessenes Datenschutzniveau verfügt.

Die Verlagerung der Datenverarbeitung in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum durch den Auftragnehmer ist zulässig. Jede Verlagerung in ein anderes Drittland als die Schweiz bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der Artikel 44 ff. DSGVO erfüllt sind.

Der Auftraggeber stimmt der Einschaltung der Firma Freshworks Inc., Kalifornien, USA, durch den Auftragnehmer zum Betrieb des Support-Systems freshdesk zu. Die Firma Freshworks Inc. ist nach dem EU-US Privacy Shield zertifiziert und verfügt dementsprechend über ein angemessenes Datenschutzniveau:

https://www.privacyshield.gov/participant?id=a2zt0000000GnbQAAS&status=Active

Diese Firma hat nur Zugriff auf solche personenbezogenen Daten, die im Rahmen der Supportanfragen des Auftraggebers für die Bearbeitung durch den Auftragnehmer relevant sind, insbesondere solche, die vom Auftraggeber in Supportanfragen eingestellt werden.

Die vom Auftragnehmer verarbeiteten Daten sind für jeden, der über eine entsprechende Zugangskennung verfügt, weltweit über das Internet abrufbar. Der Auftragnehmer wird keine Abrufe außerhalb der Schweiz oder des Europäischen Wirtschaftsraums vornehmen. Dem Auftraggeber obliegt es, selbst dafür Sorge zu tragen, dass Abrufe durch ihn oder auf seine Veranlassung hin auch in örtlicher Hinsicht den rechtlichen Vorschriften genügen.

2. Konkretisierung des Auftragsinhalts

2.1. Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten

Die Datenverarbeitung dient der Verwaltung von Vereinen wie im Hauptvertrag vereinbart. Hierzu kann beispielsweise die Verwaltung von Mitgliedern, Interessenten, Veranstaltungsteilnehmer, Lieferanten und Terminen gehören. Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber sind im Hauptvertrag konkreter beschrieben.

2.2. Art/Kategorien der Daten

Gegenstand der Erhebung, Verarbeitung oder Nutzung sind beliebige Datenarten/-kategorien, je nachdem, wie die flexiblen ClubDesk-Funktionalitäten vom Auftraggeber gemäß dem Hauptvertrag konfiguriert und verwendet werden. Insbesondere kommen folgende Datenkategorien in Betracht:

- Stammdaten der Betroffenen, v.a. der Vereinsmitglieder, darunter
  - Adresse und Telefonnummer
  - Bankverbindung
- Abrechnungsdaten (wie z.B. Stand des Beitragskontos, Stand von Debitoren-/Kreditoren- und Lohnkonten)
- Qualifikationsdaten (wie z.B. Teilnahme an Veranstaltungen sowie Wettkämpfen und Ergebnisse hierbei, Fortbildungen von Mitarbeitern)

2.3. Kreis/Kategorien der Betroffenen

Der Kreis bzw. die Kategorien der durch diese Auftragsverarbeitung Betroffenen umfasst beliebige Personen, je nachdem, wie die flexiblen ClubDesk-Funktionalitäten vom Auftraggeber gemäß dem Hauptvertrag konfiguriert und verwendet werden. Insbesondere kommen folgende Personenkategorien in Betracht:

- Mitglieder des Vereins
- Interessenten
- Veranstaltungsteilnehmer
- Mitarbeiter
- Lieferanten/Dienstleister

3. Beschreibung der zu treffenden technischen und organisatorischen Datenschutz- und Datensicherheitsmaßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere

hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit eine Prüfung des Auftraggebers Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit der Datenverarbeitung gemäß Anlage 1 dieser Vereinbarung herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme, insbesondere unter Berücksichtigung der Organisationskontrolle, Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle sowie des Trennungsgebots. 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 zu berücksichtigen.

(3) 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 dem Auftraggeber unverzüglich mitzuteilen.

4. Berichtigung, Sperrung und Löschung von Daten; Rechte der Betroffenen

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder sperren bzw. deren Verarbeitung einschränken. Zulässig ist die Sperrung des Zugangs des Auftraggebers zu ClubDesk durch den Auftragnehmer, soweit dies nach den Allgemeinen Geschäftsbedingungen von ClubDesk insbesondere im Fall des Gebührenrückstandes oder bei begründetem Verdacht auf eine missbräuchliche Nutzung zulässig ist.

(2) Soweit sich eine betroffene Person bezüglich ihrer Datenschutzrechte, insbesondere auf Auskunft, Berichtigung, Löschung und Sperrung, unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen an den Auftraggeber weiterleiten und/oder den Betroffenen an den Auftraggeber verweisen. Der Auftragnehmer selbst wird keine Entscheidung über die Berechtigung von Ersuchen der Betroffenen treffen und insbesondere auch keine Auskunftsverlangen von Betroffenen beantworten.

(3) Der Auftragnehmer wird den Auftraggeber bei der Erfüllung der Ansprüche von Betroffenen im Rahmen seiner Möglichkeiten unterstützen, sofern der Auftraggeber die Ansprüche nicht ohne Mitwirkung den Auftragnehmer erfüllen kann. Der Auftragnehmer kann vom Auftraggeber eine angemessene Zusatzvergütung des durch die Mitwirkung begründeten Aufwandes verlangen.

(4) Wendet sich ein Betroffener direkt an den Auftragnehmer wegen einer angenommenen Datenschutzverletzung und erlangt Schadensersatz von diesem, hat der Auftraggeber dem Auftragnehmer den dadurch entstandenen Schaden zu ersetzen, soweit der Auftragnehmer dem Auftraggeber nach den Vorschriften dieser Vereinbarung sowie des Hauptvertrages für diese Datenschutzverletzung nicht gehaftet hätte, insbesondere wenn er sich an die Vereinbarung und die Weisungen des Auftraggebers gehalten hat.

5. Kontrollen und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat neben den Regelungen dieses Auftrags die an seinem Sitz in der Schweiz geltenden gesetzlichen Regelungen zum Datenschutz einzuhalten. Aus diesem Zusammenspiel von vertraglichen und gesetzlichen Regelungen ergeben sich insbesondere folgende Pflichten des Auftragnehmers:

1. Der Auftragnehmer ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Fragen zum Datenschutz können an datenschutz@clubdesk.com gerichtet werden.
2. 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. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.
3. Der Auftragnehmer kontrolliert regelmäßig die technischen und organisatorischen Maßnahmen der Datensicherheit, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den für ihn geltenden datenschutzrechtlichen Anforderungen erfolgt.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.

(3) Der Auftraggeber stimmt der Beauftragung des nachfolgenden Unterauftragnehmers zu, mit welchem vom Auftragnehmer eine Vereinbarung entsprechend dieser Vereinbarung getroffen wurde:

Firma Unterauftragnehmer	Anschrift/Land	Art des Unterauftrages
Nine Internet Solutions AG	Albisriederstrasse 243a 8047 Zürich Schweiz	Hosting (Bereitstellung von Servern in einem Rechenzentrum)
Freshworks Inc.	1250 Bayhill Drive, Suite 315, San Bruno, CA 94066, USA	Betrieb der Cloud-basierten Support-Software „freshdesk“

(4) Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:

- eine vertragliche Vereinbarung mit dem Unterauftragnehmer entsprechend dieser Vereinbarung zugrunde gelegt wird,

- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab unter Angabe des Zeitpunkts der Weitergabe der Daten schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Weitergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt.

Ein Einspruch des Auftraggebers gilt als außerordentliche Kündigung des Hauptvertrages auf den Zeitpunkt unmittelbar vor der Weitergabe. Nach diesem Zeitpunkt ist keine weitere Nutzung der Leistungen des Auftragnehmers durch den Auftraggeber mehr möglich. Vor Übergabe an den Unterauftragnehmer werden die Daten des Auftraggebers durch den Auftragnehmer gelöscht. Dem Auftraggeber obliegt es, selbst eine etwaige Datensicherung in seinen eigenen Systemen vor diesem Zeitpunkt durchzuführen.

(5) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(6) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die besonderen Voraussetzungen für eine Verlagerung in ein Drittland durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 außerhalb der EU/des EWR eingesetzt werden sollen. Sitz der Unterauftragnehmer oder Dienstleister im Sinne von Abs. 1 S. 2 in der Schweiz, gelten die besonderen Anforderungen entsprechend Abschnitt 1.4 als erfüllt.

(7) Eine weitere Auslagerung durch den Unterauftragnehmer bedarf der ausdrücklichen Zustimmung des Hauptauftragnehmers (mind. Textform). Die vertraglichen Regelungen in der Vertragskette sind auch dem weiteren Unterauftragnehmer aufzuerlegen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach diesem Vertrag überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(2) Der Auftragnehmer ist berechtigt, nach eigenem Ermessen unter Berücksichtigung der gesetzlichen Verpflichtungen des Auftraggebers, Informationen nicht zu offenbaren, die sensibel im Hinblick auf die Geschäfte des Auftragnehmers sind oder durch deren Offenbarung der Auftragnehmer gegen gesetzliche oder andere vertragliche Regelungen verstoßen würde. Der Auftraggeber ist nicht berechtigt, Zugang zu Daten oder Informationen über andere Kunden des Auftragnehmers, zu Informationen hinsichtlich Kosten sowie zu sämtlichen anderen vertraulichen Daten des Auftragnehmers, die nicht unmittelbar relevant für die vereinbarten Kontrollzwecke sind, zu erhalten.

(3) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen (Auftragskontrolle) im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Der Auftraggeber hat den Auftragnehmer rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren.

(4) Nach Wahl des Auftragnehmers kann der Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen anstatt durch eine Vor-Ort-Kontrolle auch durch die Vorlage eines geeigneten, aktuellen Testats, von Berichten oder Berichtsauszügen unabhängiger Instanzen (z.B. Wirtschaftsprüfer,

Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudits – z.B. nach ISO 27001 oder gemäß Art. 42 DS-GVO – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Auftraggeber in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Als Nachweis kommt auch die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO in Betracht.

(5) Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten zur Vertraulichkeit zu verpflichten. Der Auftragnehmer ist ebenfalls berechtigt, von dem Dritten vor Prüfung eine Vertraulichkeitsverpflichtung zu verlangen, welche es untersagt, dass dem Auftraggeber andere als datenschutzrelevante Umstände zum Auftrag und Dritten beliebige im Rahmen der Beauftragung und Prüfung festgestellten Umstände mitgeteilt werden. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen.

(6) Für die Unterstützung im Rahmen von Kontrollen des Auftraggebers kann der Auftragnehmer eine angemessene Zusatzvergütung für den dadurch begründeten Aufwand verlangen.

8. Mitteilung bei Verstößen des Auftragnehmers und Unterstützung des Auftraggebers

(1) Der Auftragnehmer erstattet in allen Fällen dem Auftraggeber eine Meldung, 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.

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

(3) Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten und dieser Vereinbarung bei der Einhaltung der gesetzlichen Pflichten zur Sicherheit personenbezogener Daten, der Meldepflichten bei Datenpannen, der Datenschutz-Folgeabschätzungen und der vorherige Konsultationen. Hierzu gehören insbesondere

- 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;
- die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
- 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;
- die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
- die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(4) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung des Hauptvertrages enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine angemessene Zusatzvergütung für den dadurch begründeten Aufwand beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Auftraggebers. Der Auftraggeber hat seine Weisungen automatisiert über die gemäß dem Hauptvertrag bereitgestellten Funktionen der Software ClubDesk, deren kundenseitigen Eingaben und Konfigurationen, zu erteilen.

(2) Der Auftragnehmer ist nicht verpflichtet andersartige Einzelweisungen auszuführen. Ausgenommen hiervon ist die Einzelweisung zum Löschen aller im Auftrag des Auftraggebers verarbeiteter Daten, welche der Auftragnehmer immer auszuführen hat, wenn sichergestellt ist, dass diese vom Auftraggeber bzw. einer für diesen vertretungsberechtigten Person stammt. Mündliche Einzelweisungen bestätigt der Auftraggeber unverzüglich mindestens in Textform. Eine Löschung bedarf immer der Weisung zumindest in Textform. Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Einzelweisung nach diesem Absatz verstoße gegen Datenschutzvorschriften. Führt der Auftragnehmer eine Einzelweisung nach diesem Absatz aus, ist er berechtigt, eine angemessene Zusatzvergütung für den dadurch begründeten Aufwand zu verlangen.

10. 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. Daneben darf der Auftragnehmer Kopien der Daten des Auftraggebers für Softwaretests (z.B. Datenmigration bei neuen Releases) und für Support (z.B. Debugging auf Testsystemen) verwenden.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung des Hauptvertrages – hat der Auftragnehmer sämtliche in seinen Besitz gelangten personenbezogenen Daten aus dem Verantwortungsbereich des Auftraggebers, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen. Es obliegt dem Auftraggeber seine Daten vor Vertragsende bzw. vor Erteilung einer Löschungsweisung auf eigenen Systemen selbst zu sichern.

(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.

11. Sonstiges

Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Hauptvertrages.

12. Anlage – Technisch-organisatorische Maßnahmen

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

- Zutrittskontrolle (kein unbefugter Zutritt zu Datenverarbeitungsanlagen):

reeweb ag: Keine Datenspeicherung bei reeweb ag, Software und Daten werden vollständig in externem Rechenzentrum gehostet (Produktion und Testsysteme);

Rechenzentrum: Kein unbefugter Zutritt zu Datenverarbeitungsanlagen; Videoüberwachung und mehrstufiges Zutrittskontrollprinzip gewährleistet physikalische Sicherheit;

- Zugangskontrolle (keine unbefugte Systembenutzung):

  Sichere Kennwörter (Mindestlänge von 8 Zeichen für Administrator-Passwörter für ClubDesk, Zahl und Sonderzeichen erforderlich, etc.), automatische Sperrmechanismen (Benutzerkonten werden nach 10 fehlgeschlagenen Logins automatisch gesperrt), nur Hashwert von Passwörtern wird gespeichert;

- Zugriffskontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems):

  ClubDesk bietet umfangreiches Rollensystem für bedarfsgerechte Zugriffsrechte einzelner Benutzer eines Vereins, Protokollierung von Logins und schreibenden Zugriffen (Änderungen an Daten werden historisiert abgelegt, inkl. Zeitstempel und Benutzer);

- Trennungskontrolle (getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurde):

  Daten werden pro Verein in eigener Datenbank mit separatem Datenbank-Login abgelegt;

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

- Weitergabekontrolle (kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport):

  Sichere Web-Verbindung mit Applikationsservern über HTTPS.

  E-Mail-Versand ist ungesichert (keine Verschlüsselung der E-Mails). E-Mails zur Registrierung, Passwort-Wiederherstellung etc., werden vom Auftragnehmer aber immer nur mit Links auf verschlüsselte Webseiten, die zeitlich begrenzt gültig sind, versandt. Für den unverschlüsselten Versand von E-Mails durch den Auftraggeber mittels der entsprechenden Funktionalität von ClubDesk ist der Auftraggeber selbst verantwortlich.

- Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind):

  Protokollierung von Logins und schreibenden Zugriffen: Änderungen an Daten werden historisiert abgelegt, inkl. Zeitstempel und Benutzer;

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

- Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust):

  reeweb ag: u.a. Spiegeln von Festplatten (RAID), tägliche Backups in Rechenzentrum, Firewall, Virenschutz bei hochgeladenen Dateien, externe Überwachung wichtiger Software- und Hardwarekomponenten mit SMS-Alarmierung an 3rd-Level Support;

  Rechenzentrum: Brandmelder; redundante, vollständig getrennte Leitungen für Energie und Daten; Internet ausfallsicher, Netzkomponenten redundant; unterbruchsfreie Stromversorgung (USV); modernste Datensicherung: mehrfach gesichert, örtlich getrennt in verschiedenen Brandschutzzonen;

- Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

  Dank Backups und standardisiertem Server-Setup kann Betrieb im Notfall rasch wieder hergestellt werden.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

- Datenschutz-Management:
  Bestimmungen bzgl. Datenschutz in sämtlichen Arbeitsverträgen und Richtlinien auf internem Wiki; Geschäftsleitung ist sensibilisiert für das Thema Datenschutz;

- Incident-Response-Management:
  Externes Support-Incident-Tool, in dem alle Support-Anfragen verwaltet und überwacht werden;

- Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO):
  z.B. vordefinierte Rollen für typische Funktionen innerhalb eines Vereines;

- Auftragskontrolle (keine Datenverarbeitung im Auftrag ohne entsprechende Weisung des Auftraggebers):
  Eindeutige Vertragsgestaltung, strenge Auswahl und Kontrolle des Rechenzentrums.

Basel, 15.11.2018

reeweb ag, Wettsteinplatz 7, 4058 Basel, Schweiz