Vereinbarung über die Auftragsverarbeitung von personenbezogenen Daten (AVV)

ClubDesk für Vereine im Europäischen Wirtschaftsraum (EWR) sowie für Vereine mit Sitz in der Schweiz

(EWR: Mitgliedstaaten der Europäischen Union sowie Island, Liechtenstein und Norwegen)

zwischen dem

Auftraggebender Verein

– als Verantwortlicher nachfolgend „Kunde“ genannt –

und der

reeweb ag (Entwickler von ClubDesk)

Picassoplatz 8

4052 Basel

Schweiz

– als Auftragsverarbeiterin nachfolgend „reeweb“ genannt –

1. Gegenstand und Dauer des Auftrags, Anwendung Datenschutzrecht

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 zwischen Kunde und reeweb nach Maßgabe der Allgemeinen Geschäftsbedingungen online abgeschlossenen Vertrag.

Die inhaltliche Verwaltung der Vereinsdaten und die Verantwortung für die Zulässigkeit der Datenverarbeitung, also die Frage, ob bestimmte Daten (beispielsweise Kontaktdaten von Mitgliedern) überhaupt verarbeitet werden dürfen, obliegt dem Kunden bzw. der vertretungsberechtigten Person. Reeweb verarbeitet im Rahmen der getroffenen Vereinbarungen lediglich die vom Kunden eingegebenen Daten in dessen Auftrag und nach seiner Weisung.

Die vorliegende Vereinbarung regelt die Rechte und Pflichten von Kunde und reeweb im Rahmen einer Verarbeitung personenbezogener Daten im Auftrag. Die Bestimmungen finden Anwendung auf alle Tätigkeiten, die mit dem Vertrag im Zusammenhang stehen und bei denen reeweb und seine Beschäftigten oder durch reeweb Beauftragte mit personenbezogenen Daten in Berührung kommen, die vom Kunden stammen oder für den Kunden erhoben wurden.

1.2. Dauer des Auftrags

Die Dauer dieses Auftrags (Laufzeit) richtet sich nach der Laufzeit des Hauptvertrags. Im Zweifel gilt eine Kündigung des Hauptvertrags auch als Kündigung dieses Vertrags und eine Kündigung dieses Vertrages als Kündigung des Hauptvertrages.

Bei einfachen – also weder vorsätzlichen noch grob fahrlässigen – Verstößen setzt der Kunde reeweb zunächst eine angemessene Frist, innerhalb welcher reeweb den Verstoß abstellen kann. Das Recht zu einer außerordentlichen Kündigung dieses Vertrages aus wichtigem Grund bleibt unberührt.

1.3. Anwendung der DSGVO

Für den Kunden als Verein mit Sitz im Europäischen Wirtschaftsraum (EWR) oder für Vereine mit Mitgliedern aus dem EWR gilt die Datenschutzgrundverordnung (nachstehend „DSGVO“ genannt). Ansonsten findet das für den Kunden anwendbare Datenschutzrecht Anwendung. reeweb mit Sitz in der Schweiz hält die jeweils auf sie anwendbaren Datenschutzbestimmungen ein.

1.4. Ort der Datenverarbeitung

Die Datenverarbeitung durch reeweb erfolgt in der Schweiz. Die Europäische Kommission hat mit ihrer Entscheidung vom 26.07.2000 festgestellt, dass in der Schweiz ein angemessenes Datenschutzniveau besteht.

Die Verlagerung der Datenverarbeitung und Datenhaltung in einem Mitgliedsstaat der Europäischen Union, in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum durch reeweb sowie in einem Land mit einem Angemessenheitsbeschluss ist zulässig. Die allfällige Weiterübermittlung an Unter-Auftragsbearbeiter in Staaten ohne angemessenes Datenschutzniveau wird durch den Abschluss von EU-Standardvertragsklauseln (Modul 3) sichergestellt. Sollte reeweb in Zukunft auch gestützt auf andere gesetzlich zulässige Transfermechanismen Daten übermitteln, teilt sie dies der Kundin vorab mit.

2. Konkretisierung des Auftragsinhalts

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

Die Datenverarbeitung dient der Verwaltung von Vereinen oder Gruppen wie im Vertrag vereinbart. Hierzu kann beispielsweise die Verwaltung von Mitgliedern, Interessenten, Veranstaltungsteilnehmer, Lieferanten und Terminen gehören. Umfang, Art und Zweck der Verarbeitung personenbezogener Daten durch reeweb für den Kunde sind in der Datenschutzerklärung konkreter beschrieben.

2.2. Art und Kategorien der personenbezogenen Daten

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

- Stammdaten der Betroffenen, v.a. der Vereinsmitglieder, darunter
  - Adresse und Telefonnummer
  - E-Mail-Adresse
  - 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 und Kategorien der Betroffenen

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

- Mitglieder des Vereins / der Gruppe
- Interessenten und Gäste
- Sponsoren und Gönner
- Veranstaltungsteilnehmer
- Mitarbeiter
- Lieferanten/Dienstleister

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

(1) Die erforderlichen technischen und organisatorischen Maßnahmen zum angemessenen Schutz der Daten des Kunden sind gemäß Anlage von reeweb beschrieben. Bei Akzeptanz durch den Kunden werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit eine Prüfung des Kunden Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) reeweb hat die Sicherheit der Datenverarbeitung gemäß Anlage 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 reeweb gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind dem Kunden unverzüglich in Textform mitzuteilen.

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

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

(2) Soweit sich eine betroffene Person (z.B. ein Vereinsmitglied) bezüglich ihrer Datenschutzrechte, insbesondere auf Auskunft, Berichtigung, Löschung und Sperrung gem. anwendbarem Datenschutzrecht, unmittelbar an reeweb wendet, wird reeweb dieses Ersuchen an den Kunden weiterleiten und/oder den Betroffenen an den Kunden verweisen und gleichzeitig diesen über die Betroffenenanfrage informieren. Reeweb selbst wird keine Entscheidung über die Berechtigung von Ersuchen der Betroffenen treffen und insbesondere auch keine Auskunftsverlangen von Betroffenen beantworten.

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

(4) Wendet sich ein Betroffener direkt an reeweb wegen einer angenommenen Datenschutzverletzung und erlangt Schadensersatz von diesem, hat der Kunde reeweb den dadurch entstandenen Schaden zu ersetzen, soweit reeweb dem Kunden 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 Kunden gehalten hat. Dies gilt im Falle einer gegen reeweb verhängten Geldbuße entsprechend.

5. Kontrollen und sonstige Pflichten von reeweb

Reeweb 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 von reeweb:

1. Reeweb ist nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet. Fragen zum Datenschutz können an datenschutz@clubdesk.com gerichtet werden.
2. Reeweb setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die in Schriftform auf Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden oder einer gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Ferner wird reeweb die Einhaltung dieser Verpflichtung mit der gebotenen Sorgfalt sicherstellen.

Reeweb und jede reeweb unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Kunden verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. In einem solchen Fall teilt reeweb dem Kunden diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet.

3. Reeweb 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 für die Dauer der Verarbeitung der Kundendaten erfolgt.
4. Reeweb führt ein Verzeichnis zu allen Kategorien der im Auftrag des Kunden durchgeführten Tätigkeiten der Verarbeitung.

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 reeweb 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. Reeweb ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Kunden auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Kunde stimmt hiermit allgemein der Beauftragung von Unterauftragnehmern zu, mit welchem von reeweb eine Vereinbarung entsprechend dieser Vereinbarung getroffen wurde. Eine Liste der aktuellen Dienstleister finden Sie auf der Webseite von reeweb unter www.clubdesk.com/unterauftragnehmer.

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

- eine vertragliche Vereinbarung mit dem Unterauftragnehmer mit dieser Vereinbarung vergleichbar zugrunde gelegt wird,
- reeweb eine solche Auslagerung auf Unterauftragnehmer dem Kunden eine angemessene Zeit vorab (in der Regel zwei (2) Monate) unter Angabe des Zeitpunkts der Weitergabe der Daten schriftlich oder in Textform anzeigt und
- der Kunde nicht bis zum Zeitpunkt der Weitergabe der Daten gegenüber reeweb schriftlich oder in Textform begründeten Einspruch gegen die geplante Auslagerung erhebt.

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

(4) Die Weitergabe von personenbezogenen Daten des Kunden an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet. Kommt ein Unterauftragnehmer seinen Datenschutzpflichten nicht nach, so haftet reeweb gegenüber dem Kunden für die Einhaltung der Pflichten jenes Unterauftragnehmers.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR/Schweiz stellt reeweb die besonderen Voraussetzungen für eine Verlagerung in ein Drittland durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister für Nebenleistungen im Sinne des vorstehenden Absatz 1 Satz 2 außerhalb der EU/des EWR/Schweiz eingesetzt werden sollen.

7. Kontrollrechte des Kunden

(1) Reeweb stellt sicher, dass sich der Kunde von der Einhaltung der Pflichten von reeweb nach diesem Vertrag überzeugen kann. Reeweb verpflichtet sich, dem Kunden auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

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

(3) Der Kunde hat das Recht, im Einvernehmen mit reeweb Überprüfungen (Auftragskontrolle) im Rahmen der üblichen Geschäftszeiten auf eigene Kosten, ohne Störung des Betriebsablaufs und unter strikter Geheimhaltung von Betriebs- und Geschäftsgeheimnissen von reeweb durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen, sofern dieser nicht in einem Wettbewerbsverhältnis zu reeweb steht. Der Kunde hat reeweb rechtzeitig (in der Regel mindestens vier Wochen vorher) über alle mit der Durchführung der Kontrolle zusammenhängenden Umstände zu informieren.

(4) Nach Wahl von reeweb 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 DSGVO – („Prüfungsberichts“) erbracht werden, wenn der Prüfungsbericht es dem Kunde in angemessener Weise ermöglicht, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Als Nachweis kommt auch die Einhaltung genehmigter Verhaltensregeln in Betracht.

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

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

8. Mitteilung bei Verstößen durch reeweb und Unterstützung des Kunden

(1) Reeweb erstattet in allen Fällen dem Kunden eine unverzügliche Meldung, wenn durch ihn, durch die bei ihm beschäftigten Personen oder durch die ihm zugewiesenen Unterbeauftragten Verstöße gegen Vorschriften zum Schutz personenbezogener Daten des Kunden oder gegen die im Auftrag getroffenen Festlegungen vorgefallen sind und diese reeweb bekannt werden. Der Inhalt der Meldungen richten sich nach dem anwendbaren Datenschutzrecht.

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

(3) Reeweb unterstützt den Kunden 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 vorherigen Konsultationen mit der Aufsichtsbehörde. 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.

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

9. Weisungsbefugnis des Kunden

(1) Der Umgang mit den Daten erfolgt ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisung des Kunden, sofern nicht gesetzliche Vorschriften den Weisungen entgegenstehen. Reeweb teilt diese rechtlichen Anforderungen dem Kunden mit, es sei denn der Mitteilung steht ein wichtiges öffentliches Interesse entgegen. Der Kunde hat seine allgemeinen Weisungen automatisiert über die gemäß dem Hauptvertrag bereitgestellten Funktionen der Software ClubDesk, deren kundenseitigen Eingaben und Konfigurationen, zu erteilen.

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

(3) Weisungsberechtigte Personen sind diejenigen, die den Kunden wirksam vertreten können.

10. Löschung personenbezogener Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Kunden nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind. Daneben darf reeweb Kopien der Daten des Kunden für Softwaretests (z.B. Datenmigration bei neuen Releases) und für Support (z.B. Debugging auf Testsystemen) verwenden.

(2) Nach Aufforderung durch den Kunden und frühestens nach Abschluss der vertraglich vereinbarten Arbeiten (d.h. mit Beendigung des Vertrages gemäß der geltenden AGB) hat reeweb sämtliche in seinen Besitz gelangten personenbezogenen Daten aus dem Verantwortungsbereich des Kunden, die im Zusammenhang mit dem Auftragsverhältnis stehen, datenschutzgerecht zu löschen. Dies gilt auch für Vervielfältigungen der Kundendaten bei reeweb, wie etwa Datensicherungen. Es obliegt dem Kunden, seine Daten vor Vertragsende bzw. vor Erteilung einer Löschungsweisung auf eigenen Systemen selbst zu sichern. Reeweb wird dem Kunden die Löschung in Textform bestätigen.

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

11. Sonstiges

Soweit in dieser Vereinbarung keine Sonderregelungen enthalten sind, gelten die Bestimmungen des Vertrages gemäß der geltenden AGB, insbesondere die Haftungsbegrenzungen gemäß Ziff. 14 der AGB.

Basel, 15.09.2023

12. Anlage – Technisch-organisatorische Maßnahmen

1. Vertraulichkeit

- 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

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

  Sichere Web-Verbindung mit Applikationsservern über HTTPS – auch für die Vereins-Webseiten, die in der Software ClubDesk angelegt werden.

  Sicherer Versand und Empfang von E-Mails mittels TLS (falls der empfangende bzw. sendende E-Mail-Server dies unterstützt). Weiter setzt ClubDesk verschiedene Technologien ein, um die Integrität und Authentizität von E-Mails und deren Absender zu sichern: Domain-based Message Authentication (DMARC), Domain Keys Identified Mail (DKIM) und Sender Policy Framework (SPF). Für den unverschlüsselten Versand von E-Mails (falls ein empfangender bzw. sendender E-Mail-Server TLS nicht unterstützt) durch den Kunden mittels der entsprechenden Funktionalität von ClubDesk ist der Kunde 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

- 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

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

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- 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:
  z.B. vordefinierte Rollen für typische Funktionen innerhalb eines Vereines;

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