# Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag gemäß Art. 28 DSGVO

zwischen
**Betreiber von Sport- und Wellnessanlagen**
(nachfolgend „**Studio**“ oder “**Auftraggeber**” genannt)

und der

**Eurofit24 GmbH, Raboisen 5, 20095 Hamburg**
(nachfolgend „**Eurofit24**“ oder “**Auftragnehmer**” genannt)

**Präambel:**

Zwischen dem Studio und Eurofit24 besteht ein Partnerschaftsvertrag, im Zuge dessen Eurofit24 gemäß näher definierter Kriterien, Forderungen des Studios gegen dessen Mitglieder erwirbt (nachfolgend „**Partnerschaftsvertrag**“).

Flankierend zum Partnerschaftsvertrag erbringt Eurofit24 auf Basis dieser Vereinbarung zur Verarbeitung personenbezogener Daten im Auftrag (nachfolgend „**Vertrag**“) für das Studio technische Dienstleistungen zur Unterstützung des Studios bei der Kommunikation mit säumigen Kunden des Studios (nachfolgend „**Mitglieder des Studios**“).

Im Rahmen der Leistungserbringung nach dem Vertrag Partnerschaftsvertrag ist es erforderlich, dass der Auftragnehmer mit personenbezogenen Daten in Berührung kommt, für die der Auftraggeber als verantwortliche Stelle im Sinne der datenschutzrechtlichen Vorschriften fungiert (nachfolgend „**Auftraggeber-Daten**“ genannt). Diese Vereinbarung konkretisiert die datenschutzrechtlichen Rechte und Pflichten der Parteien im Zusammenhang mit dem Umgang des Auftragnehmers mit Auftraggeber-Daten.

## § 1 Gegenstand des Vertrags, Art der Daten, Kreis der Betroffenen

(1) Eurofit24 erbringt gegenüber dem Studio folgende technische Dienstleistungen:
Versendung von E-Mails/SMS an solche Mitglieder des Studios, die eine fällige Forderung des Studios zum Fälligkeitszeitpunkt nicht erfüllt haben. Die Versendung von E-Mails/SMS erfolgt im Namen des Studios, entsprechend inhaltlicher Vorgaben des Studios.

(2) Eurofit24 ist verpflichtet, sämtliche personenbezogene Daten, auf welche Eurofit24 im Zuge der Erfüllung der nach diesem Vertrag geschuldeten Leistungen Zugriff erlangt, nach Vorgaben des Studios streng räumlich getrennt von jedweden Daten von Eurofit24 sowie Daten Dritter zu verarbeiten.

(3) Von der Auftragsdatenverarbeitung sind Daten folgender Personengruppen betroffen:
Mitglieder des Studios.
Es handelt sich dabei ausnahmslos um folgende personenbezogenen Daten des vorbezeichneten Kreises der Betroffenen:
- Name des jeweiligen Mitglieds
- Adresse des jeweiligen Mitglieds
- offene Forderung und Fälligkeitstag
- Handynummer des jeweiligen Mitglieds und/oder
- E-Mailadresse des jeweiligen Mitglieds

(4) Zweck der Verarbeitung der vorbezeichneten Daten ist zum einen die Unterstützung des Studios bei der Verwaltung der mit den Mitgliedern des Studios geschlossenen Verträge(Mitgliederverwaltung).

## § 2 Weisungsbefugnis

(1) Eurofit24 verarbeitet Daten ausschließlich gemäß den Regelungen des mit dem Auftraggeber geschlossenen Vertrages sowie im Rahmen der vom Auftraggeber erteilten Weisungen. Eurofit24 verwendet die zur Datenverarbeitung überlassenen Daten nicht anderweitig und bewahrt sie nicht länger auf, als es der Auftraggeber bestimmt.

(2) Für die Zulässigkeit der Datenverarbeitung sowie für die Wahrung der Rechte der Personen, deren Daten verarbeitet werden (den Betroffenen) nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich.

(3) Eurofit24 wird den Auftraggeber bei der Erfüllung von Pflichten gegenüber den Betroffenen unterstützen.

(4) Der Auftraggeber erteilt alle Weisungen in der Regel schriftlich oder per E-Mail. Mündlich erteilte Weisungen müssen unverzüglich schriftlich oder per E-Mail bestätigt werden.

## § 3 Datenschutzbeauftragter von Eurofit24, Verzeichnis der Verarbeitungstätigkeit

(1) Bei Eurofit24 ist als betrieblicher Datenschutzbeauftragter bestellt:

| | |
|---|---|
| Name: | Marc Althaus - DS EXTERN GmbH |
| Kontakt: | Bredkamp 53a, 22589 Hamburg, https://www.dsextern.de/anfragen |

(2) Der Datenschutzbeauftragte hat die Ausführungen der EU-DSGVO sowie andere Vorschriften über den Datenschutz im Hinblick auf das Auftragsverhältnis sicherzustellen. Hierzu führt der Datenschutzbeauftragte regelmäßige Kontrollen durch. Über die Kontrollen wird ein Protokoll angefertigt. Stellt der Datenschutzbeauftragte im Rahmen seiner Aufgaben Unregelmäßigkeiten bei der Datenverarbeitung fest, so informiert er unverzüglich die Geschäftsführung von Eurofit24. Ein Wechsel des Datenschutzbeauftragten wird dem Studio unverzüglich mitgeteilt.

## § 4 Vertraulichkeit

(1) Eurofit24 darf ohne schriftliche Weisung des Studios die überlassenen personenbezogenen Daten nicht an Dritte weitergeben.

(2) Eurofit24 muss alle im Rahmen des Auftrages überlassenen Unterlagen, Dokumente und andere Informationsträger absolut vertraulich behandeln. Dies gilt auch für alle weiteren Informationen, die Eurofit24 bei der Durchführung des Auftrages bekannt werden. Diese Verpflichtung gilt während und auch nach Beendigung des Vertrages.

(3) Der Auftragnehmer verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers Vertraulichkeit im Sinne von Art. 28 Abs. 3 b) DSGVO zu wahren. Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet. Der Auftragnehmer überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

## § 5 Berichtigung, Sperrung und Löschung von Daten

In Bezug auf die Berichtigung, Sperrung und Löschung von Daten wird Eurofit24 nur auf Weisung des Auftraggebers tätig. Soweit ein Betroffener sich unmittelbar an Eurofit24 zwecks

Berichtigung oder Löschung seiner Daten wenden sollte, wird Eurofit24 dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

## § 6 Unterauftragsverhältnisse

(1) Zum Zeitpunkt des Abschlusses dieses Vertrages sind die in der Anlage 2 aufgeführten Unternehmen als Unterauftragnehmer für Teilleistungen für den Auftragnehmer tätig und verarbeiten und/oder nutzen in diesem Zusammenhang auch unmittelbar die Auftragsdaten. Für diese Unterauftragnehmer gilt die Einwilligung für das Tätigwerden als erteilt. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

(2) Der Auftragnehmer informiert den Auftraggeber über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung oder die Ersetzung von anderen als den in Anlage 2 genannten Unterauftragnehmern, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben. Gleiches gilt, wenn der Auftragnehmer zur Erfüllung seiner vertraglich übernommenen Leistungspflichten sonstige dritte Unternehmen zur Leistungserfüllung heranzieht. Hierbei muss jeder neue Unterauftragnehmer vor Beauftragung dem Auftraggeber schriftlich angezeigt werden, sodass der Auftraggeber gegen die Beauftragung innerhalb von 1 Woche nach Zugang der Anzeige Einspruch erheben kann.

(3) Verweigert der Auftraggeber durch seinen Einspruch die Zustimmung aus anderen als aus wichtigen Gründen, kann der Auftragnehmer den Vertrag mit dem Auftraggeber zum Zeitpunkt des geplanten Einsatzes des Unterauftragnehmers kündigen, ohne dass dem Auftraggeber gegen den Auftragnehmer in diesem Zusammenhang Schadensersatz- oder sonstige Zahlungsansprüche zustehen.

(4) Der Auftragnehmer muss jeden Unterauftragnehmer unter besonderer Berücksichtigung der Eignung hinsichtlich der Erfüllung der zwischen dem Auftraggeber und dem Auftragnehmer vereinbarten technischen und organisatorischen Maßnahmen gewissenhaft auswählen.

(5) Ist der Auftragnehmer im Sinne dieser Vereinbarung befugt, die Dienste eines Unterauftragnehmers in Anspruch zu nehmen, um bestimmte Verarbeitungstätigkeiten zur Erfüllung der gegenüber dem Auftraggeber bestehenden Leistungspflichten auszuführen, so werden diesem Unterauftragnehmer im Wege eines Vertrags dieselben Pflichten auferlegt, die in diesem Vertrag zwischen dem Auftraggeber und dem Auftragnehmer festgelegt sind. Dies gilt insbesondere hinsichtlich der Anforderungen an Vertraulichkeit, Datenschutz und Datensicherheit sowie den in diesem Vertrag beschriebenen Kontroll- und Überprüfungsrechten des Auftraggebers. Hierbei müssen ferner hinreichend Garantien dafür geboten werden, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen der DSGVO erfolgt.

(6) Durch schriftliche Aufforderung ist der Auftraggeber berechtigt, vom Auftragnehmer Auskunft über die datenschutzrelevanten Verpflichtungen des Unterauftragnehmers zu erhalten, erforderlichenfalls auch durch Einsicht in die relevanten Vertragsunterlagen. Unter den in § 8 dieses Vertrages geregelten Voraussetzungen müssen Vor-Ort Kontrollen des Auftraggebers beim Unterauftragnehmer möglich sein.

(7) Ein zustimmungspflichtiges Unterauftragsverhältnis liegt nicht vor, wenn der Auftragnehmer Dritte im Rahmen einer Nebenleistung zur Hauptleistung beauftragt, wie beispielsweise bei Personal-, Post- und Versanddienstleistungen. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen. Die Nebenleistungen sind vorab detailliert zu benennen.

## § 7 Hinweispflicht von Eurofit24

(1) Ist Eurofit24 der Ansicht, dass eine Weisung gegen das DSGVO oder andere Vorschriften über den Datenschutz verstößt, weist Eurofit24 der Auftraggeber unverzüglich darauf hin.
(2) Die Pflichten des Auftragnehmers bei Störungen, Verdacht auf Datenschutzverletzungen oder anderen Unregelmäßigkeiten bei der Verarbeitung ergeben sich aus § 10 dieses Vertrages.

## § 8 Kontrolle durch das Studio und Mitwirkungs- und Duldungspflichten

(1) Der Auftraggeber ist berechtigt, durch einen zur Geheimhaltung verpflichteten Bevollmächtigten, vor Beginn der Dienstleistung sowie regelmäßig während der Dauer der Dienstleistung in angemessenen Abständen die Einhaltung der technischen und organisatorischen Maßnahmen zum Datenschutz und die Datenverarbeitung von Eurofit24 und deren Unterauftragnehmern zu überprüfen.
(2) Anstatt einer Vor-Ort-Kontrolle darf Eurofit24 den Nachweis der Einhaltung der technischen und organisatorischen Maßnahmen auch durch die Vorlage eines geeigneten, aktuellen Prüfberichts von unabhängiger Personen (z.B. Wirtschaftsprüfer, Datenschutzbeauftragter oder Qualitätsauditoren) oder einer geeigneten Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit – z.B. nach BSI-Grundschutz – („Prüfungsberichts“) erbringen. Der Prüfungsbericht muss es dem Auftraggeber in angemessener Weise ermöglichen, sich von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen.

## § 9 Festlegung der technischen und organisatorischen Maßnahmen

(1) Der Auftragnehmer trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko für die Rechte und Freiheiten der Betroffenen angemessenes Schutzniveau zu 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 im Sinne von Art. 32 Abs. 1 DSGVO zu berücksichtigen. Die konkreten, vom Auftragnehmer ergriffenen technischen und organisatorischen Maßnahmen werden in Anlage 1 aufgelistet.
(2) Da die technischen und organisatorischen Maßnahmen dem technischen Fortschritt und der technologischen Weiterentwicklung unterliegen, darf der Auftragnehmer andere und gleichwertige Maßnahmen umzusetzen, sofern dabei das Sicherheitsniveau der in Anlage 1 festgelegten Maßnahmen nicht unterschritten wird. Wesentliche Änderungen der Maßnahmen müssen vom Auftragnehmer dokumentiert und dem Auftraggeber auf Anforderung zur Verfügung gestellt werden.

## § 10 Mitteilungs- und Unterstützungspflichten des Auftragnehmers bei Datensicherheitsvorfällen

(1) Der Auftragnehmer informiert den Auftraggeber unverzüglich, wenn er oder eine bei ihm beschäftigte Person gegen Vorschriften zum Schutz personenbezogener Daten, gegen Festlegungen nach diesem Vertrag oder gegen eine vom Verantwortliche erteilte Weisung verstoßen hat, wenn Anhaltspunkte dafür bestehen, dass ein Dritter – egal aus welchem Grund – unrechtmäßig Kenntnis von Auftragsdaten erlangt haben könnte, oder wenn in sonstiger Weise eine Gefährdung für die Integrität oder Vertraulichkeit der Auftragsdaten eingetreten ist („Datensicherheitsvorfall“).
(2) Die Information über den Datensicherheitsvorfall hat Angaben über den Zeitpunkt und die Art des Vorfalls (einschließlich einer Information, welche Auftragsdaten in welcher Form betroffen sind), das betroffene EDV-System, die betroffenen Personen, den Zeitpunkt der Entdeckung, denkbare nachteilige Folgen des Datensicherheitsvorfalls sowie die vom Auftragnehmer

ergriffenen Maßnahmen und alle sonstigen in Art. 33 Abs. 3 DS-GVO bezeichneten Informationen zu enthalten. Der Auftragnehmer hat des Weiteren konkret mitzuteilen, ob eine Verletzung des Schutzes personenbezogener Daten voraussichtlich zu einem Risiko für Rechte und Freiheiten natürlicher Personen im Sinne des Art. 33 Abs. 1 Satz 1 DS-GVO führt und ob das Risiko voraussichtlich hoch im Sinne von Art. 34 Abs. 1 DS-GVO ist.

(3) Eine erste Information des Auftraggebers hat unverzüglich, eine dezidierte Information, die sämtliche Informationen gemäß vorstehendem Abs. (2) enthalten muss, soweit möglich, innerhalb von 24 Stunden nach Kenntniserlangung von dem Datensicherheitsvorfall, zu erfolgen.

(4) Der Auftragnehmer wird nach Bekanntwerden eines Datensicherheitsvorfalls unverzüglich sämtliche zumutbaren Maßnahmen ergreifen, um die entstandenen Gefährdungen für die Integrität oder Vertraulichkeit der Auftragsdaten zu minimieren und zu beseitigen, die Auftragsdaten zu sichern und mögliche nachteilige Folgen für Betroffene zu verhindern oder in ihren Auswirkungen so weit wie möglich zu begrenzen.

(5) Der Auftragnehmer ist verpflichtet, den Auftraggeber im Falle eines Datensicherheitsvorfalls bei seinen diesbezüglichen Aufklärungs-, Abhilfehandlungen, einschließlich aller Handlungen zur Erfüllung gesetzlicher Verpflichtungen, auf erstes Anfordern, im Rahmen des Zumutbaren, zu unterstützen.

(6) Der Auftragnehmer ist verpflichtet, unverzüglich nach Kenntniserlangung von einem Datensicherheitsvorfall eine Analyse der Ursachen durchzuführen, diese zu dokumentieren und dem Auftraggeber die Dokumentation auf Verlangen auszuhändigen. Stellt der Auftragnehmer im Rahmen der Analyse fest, dass die technischen und organisatorischen Maßnahmen die bislang zum Schutz der Auftragsdaten ergriffen wurden, nicht ausreichen um ein angemessenes Schutzniveau herzustellen, wird er auf eigene Kosten erforderliche zusätzliche technischen und organisatorischen Maßnahmen umzusetzen.

## § 11 Vergütung

Die seitens des Auftraggebers gegenüber Eurofit24 für die nach diesem Vertrag zu erbringenden Dienstleistungen geschuldete Vergütung ist Bestandteil einer gesonderten Vergütungsvereinbarung. Wird keine gesonderte Vergütungsvereinbarung geschlossen, ist die nach diesem Vertrag zu erbringende Dienstleistung mit der im Partnerschaftsvertrag geregelten Vergütung mit abgegolten.

## § 12 Laufzeit dieses Vertrages

(1) Dieser Vertrag beginnt mit Unterzeichnung und wird für die Dauer der Laufzeit des Partnerschaftsvertrages abgeschlossen (auflösende Befristung).

(2) Die fristlosen Kündigungsrechte der Parteien bleiben hiervon unberührt. Der Auftraggeber ist berechtigt, diesen Vertrag fristlos zu kündigen, wenn ein schwerwiegender Verstoß von Eurofit24 gegen die anzuwendenden Datenschutzvorschriften oder gegen Pflichten aus diesem Vertrag vorliegt, Eurofit24 eine Weisung des Auftraggebers nicht ausführen kann oder will oder die Wahrnehmung von Kontrollrechten durch den Auftraggeber vertragswidrig verweigert.

(3) Jede Partei ist berechtigt, diesen Vertrag mit einer Frist von zwei Wochen zum Ende eines Kalendermonats zu kündigen, wenn die Durchführung des Hauptvertrages und/oder die Durchführung dieses Vertrages von einer hierfür zuständigen Aufsichtsbehörde (insbesondere der zuständigen Datenschutzbehörde) beanstandet wird und eine von dieser Behörde zur Abstellung festgestellter Mängel gesetzte Frist erfolglos verstreicht oder mindestens eine der Parteien von der hierfür zuständigen Behörde die weitere Durchführung des Partnerschaftsvertrages und/oder dieses Vertrages untersagt wird.

(4) Jede Kündigung bedarf der Schriftform.

## § 13 Regelungen zur Berichtigung, Löschung und Sperrung von Daten

(1) Eurofit24 hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder zu sperren, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

(2) Bei Beendigung dieses Vertrags oder früher nach Aufforderung durch den Auftraggeber muss Eurofit24 sämtliche Unterlagen und Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber aushändigen oder nach vorheriger Zustimmung datenschutzgerecht vernichten.

(3) Dokumentationen, die für Eurofit24 als Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, dürfen durch Eurofit24 entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufbewahrt werden.

## § 14 Sonstiges

(1) Mündliche Nebenabreden sind nicht getroffen. Änderungen und Ergänzungen dieses Vertrages bedürfen der in § 28 Abs. 9 DSGVO geregelten Form. Dies gilt auch für eine Änderung des vorgenannten Formerfordernisses selbst.

(2) Sollte eine Bestimmung des Vertrages unwirksam sein oder werden, so verpflichten sich die Parteien, die unwirksame Bestimmung durch eine wirksame Regelung zu ersetzen, die dem wirtschaftlichen Willen der Parteien möglichst nahekommt. Das Gleiche gilt im Falle einer Regelungslücke.

(3) Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Hamburg. Die Parteien vereinbaren die Anwendbarkeit des deutschen Rechts.

Hamburg, 17.05.2018
.....
Ort, Datum


.....
Eurofit24 (Auftragnehmer)

**Anlage 1: Technisch organisatorische Maßnahmen**

**Maßnahmen zur Gewährung von Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)**

**1. Zutrittskontrolle**

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen zu verwehren, mit denen personenbezogene Daten verarbeitet oder genutzt werden.

Alle Geschäftsräume befinden sich in einem räumlich abgeschlossenen Bereich im 1. OG. Der Eingang zum Büro ist mit einem Schließsystem und Sicherheitsschlüssel sowie über Transponderkarten gesichert. Die Eingangstür ist permanent verschlossen. Die Zutrittsberechtigungen sind beschränkt. Über die an die Mitarbeiter ausgegebenen Schlüssel und Transponderkarten können nur bestimmte Türen geöffnet werden.
Die Schlüssel- und Transpondervergabe wird protokolliert. Der Serverraum verfügt über ein zusätzliches Schloss. Zutritt zu diesem Raum haben nur die Personen der Leitungsebene und der Systemadministration. Andere Mitarbeiter haben keinen Zutritt. Alle Mitarbeiter sind angewiesen die Laptops nach in personalisierten Schränken zu verschließen. Ein Zutritt für Wartungspersonal findet immer nur unter Aufsicht statt. Akten und Datenträger mit personenbezogenen Daten werden verschlossen aufbewahrt, wenn die entsprechenden Räume nicht besetzt sind.

**2. Zugangskontrolle**

Ziel der Zugangskontrolle ist es, mit Hilfe geeigneter Maßnahmen zu verhindern, dass Unbefugte Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet oder genutzt werden, nutzen können.

Der Schutz der Serversysteme vor unberechtigtem Zugang wird durch redundant ausgelegte Firewalls (basierend auf Packet-Filter) und Load-balancer bewerkstelligt. Es wurden restriktive Firewall-Regeln implementiert. Ein automatisiertes Patch-Management ist aktiv. Weitere Maßnahmen zur Zugangskontrolle sind Intrusion-Detection-Systeme (Snort, Fail2Ban, Rootkit-Detection).
Alle Systeme sind mit einem Passwortschutz versehen. Eine Passwortrichtlinie wurde erstellt und in allen Systemen implementiert. Alle Mitarbeiter sind angehalten, den unbefugten Zugang zu IT-Systemen durch geeignete Mittel wie u. a. Sperrung des Bildschirms und Verschlüsselung von Daten zu verhindern. Sämtliche Administrationstätigkeiten auf den externen Servern erfolgen über verschlüsselte Verbindungen.
Externe Verbindungen zum Unternehmensnetzwerk werden über verschlüsselte VPN-Verbindungen hergestellt.
Eine Firewall ist eingerichtet und wird von der IT-Abteilung administriert. Ungenutzte Netzwerkanschlüsse sind deaktiviert.

**3. Zugriffskontrolle**

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass nur die zur Benutzung der Datenverarbeitungssysteme Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden personenbezogenen Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

Ein Zugriffsberechtigungskonzept wurde erstellt und implementiert. Mitarbeiter haben nur Zugriff auf die Daten, die sie zur Erfüllung ihrer Aufgaben benötigen. Die Zugriffsberechtigungen werden dokumentiert und technisch durch die Nutzung eines Verzeichnisdienstes implementiert.

Unberechtigte Zugriffe auf Daten werden zudem durch folgende Maßnahmen verhindert:

- Einsatz einer Sicherheitssoftware gegen Viren, Trojaner und andere Schadsoftware
- restriktive Vergabe von Zugriffsberechtigungen für Systemdateien
- datenschutzkonformes Datenträger- und Aktenvernichtungskonzept

Berechtigungsstufen werden ausschließlich analog zu den Aufgaben vergeben, mit denen der Mitarbeiter betraut ist. Der Systemzugriff auf die Server ist neben zentralen Firewallregeln mit personalisiertem Private-Key-Verfahren geschützt.

**4. Trennungsgebot**

Ziel des Trennungsgebots ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können (Zweckbindung).

Generell werden Daten, die zu unterschiedlichen Zwecken erhoben wurden, entsprechend gekennzeichnet und getrennt gespeichert.
Kundendaten werden logisch getrennt in mandantenfähiger Form in den Datenbanken der EuroFit24 verarbeitet und gespeichert.

**5. Pseudonymisierung**

Ziel der Pseudonymisierung ist die Verarbeitung personenbezogener Daten in einer Weise, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Alle Daten die zu Wartungs- und Testzwecken durch Mitarbeiter der EuroFit24 verarbeitet werden, werden ausschließlich pseudonymisiert oder anonymisiert verarbeitet.

**Maßnahmen zur Gewährung von Integrität (Art. 32 Abs. 1 lit b DS-GVO)**

**1. Weitergabekontrolle**

Ziel der Weitergabekontrolle ist es, zu gewährleisten, 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.

Maßnahmen der Weitergabekontrolle:
Die Mitarbeiter sind angewiesen, personenbezogene Daten und andere sensible Daten auf elektronischem Wege nur verschlüsselt zu übertragen. Daten in Papierform oder als Datenträger werden blickdicht verschlossen durch Kuriere transportiert. Die Aushändigung und der Empfang der Daten werden dokumentiert.

**2. Eingabekontrolle**

Ziel der Eingabekontrolle ist es, dass nachträglich festgestellt werden kann, ob und von wem personenbezogene Daten in die Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

Maßnahmen der Eingabekontrolle:
Veränderungen von personenbezogenen Daten und Daten der Kunden werden protokolliert. Die Mitarbeiter werden regelmäßig zum ordnungsgemäßen Einsatz der Programme geschult, um Eingabefehler zu vermeiden.

**Maßnahmen zur Gewährleistung von Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)**

**1. Verfügbarkeitskontrolle**

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

Maßnahmen der Verfügbarkeitskontrolle:
Beide Rechenzentren verfügen über ausreichend dimensionierte Klimatisierung und Stromversorgung (einschließlich Schutz vor Stromausfall durch USV und Notstromaggregate).

Brandschutz und Brandbekämpfung
RZ1

- Überwiegender Einsatz von nichtbrennbaren, halogenfreien Materialien mit niedriger Rauchentwicklung
- Strikte Trennung von Lager- und Colocationflächen
- Einteilung des Gebäudes in unabhängige versiegelte Brandabschnitte
- „Very Intelligent Early Warning (V.I.E.W.)"-Brandfrühwarnsystem
- Entrauchungssystem bei Feueralarm
- Doppelt verriegelte Trockenrohr-Sprinkleranlage

RZ2

- Brandfrüherkennungssystem
- Inergen-Löschgasanlage
- Strikte Trennung von Lager- und Colocationflächen
- Einteilung des Gebäudes in unabhängige versiegelte Brandabschnitte

Die Verfügbarkeit der auf den Servern gespeicherten Kundendaten wird durch die folgenden Maßnahmen sichergestellt:

- Segmentierung der Netzwerke und strikte Trennung der unterschiedlichen Datenströme ( IP-Management-, Backup-LAN usw.)
- tägliches Backup der eigenen Systeme
- Einsatz von Firewalls an relevanten Netzwerkpunkten
- Netzwerküberwachung durch hauseigenes NOC („Network Operation Center")
- ausschließliche Verwendung von Markenkomponenten

Die Verfügbarkeit der externen Netzwerkanbindung wird durch eine Carrier-neutrale und redundante IP-Anbindung der Rechenzentren, redundante Glasfaserzuführung durch unterschiedliche Lieferanten der physikalischen Zugangsleitungen und BGP-Sessions zu Artfiles, Telia und Level3 bewerkstelligt.

Der Dienstleister Corpex überwacht auftragsgemäß die von EuroFit24 gemietete Hardware, die Erreichbarkeit des Betriebssystems sowie weitere mit EuroFit24 besprochene Dienste 24 Stunden am Tag in einem Intervall von 60 Sekunden. Im Falle einer Störung wird ein Techniker umgehend alarmiert, um das Problem innerhalb der festgeschriebenen Reaktionszeiten zu beheben.

Auf Seiten der EuroFit24 sind weiterhin Sicherungsmaßnahmen wie Virenschutz und eine Firewall vorhanden. Beide werden regelmäßig aktualisiert. Eine Vertretungsregelung stellt die Verfügbarkeit in Abwesenheitsfällen sicher.

**Rasche Wiederherstellbarkeit (Artikel 32 Abs. 1 lit. c DSGVO)**

Es existiert ein regelmäßig laufender Prozess, der die Wiederherstellbarkeit der gesicherten Daten überprüft. Bei nicht erfolgreicher Wiederherstellbarkeit wird eine Benachrichtigung ausgelöst, die zeitnah abgearbeitet wird, um die Wiederherstellbarkeit wieder garantieren zu können.

Die Wiederherstellbarkeit von gesicherten Daten ist in den meisten Fällen innerhalb von 12 Stunden möglich. In besonderen Konstellationen kann die Wiederherstellung der Daten bis zu 24 Stunden dauern.

**Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Artikel 32 Abs. 1 lit. d DSGVO; Artikel 25 Abs. 1 DSGVO)**

**1. Managementverfahren, datenschutzfreundliche Voreinstellungen**

EuroFit24 hat zusammen mit dem Datenschutzbeauftragten ein internes Datenschutz-Management-System installiert, in dem die Datenverarbeitungen und deren entsprechende Informationen dokumentiert werden. Mit Marc Althaus wurde ein externer Datenschutzbeauftragter bestellt und in die Prozesse mit eingebunden.

**2. Auftragskontrolle**

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Studios und der Vorgaben des Art. 28 DSGVO verarbeitet werden.

Maßnahmen der Auftragskontrolle:
Bei der Vergabe von Aufträgen, die die Verarbeitung von personenbezogenen Daten beinhalten, werden die Anforderungen des Art. 28 DSGVO überwacht. Dies erfolgt u. a. durch die Schulung der Mitarbeiter, die Aufträge vergeben, die Erstellung eines Mustervertrages und die Prüfung aller Verträge vor Vergabe durch den Datenschutzbeauftragten. Sämtliche Aufträge werden schriftlich erteilt. Der Datenschutzbeauftragte begleitet den gesamten Prozess und unterstützt die Fachabteilung bei der Kontrolle des Auftragnehmers. Bei der Erfüllung von Aufträgen gemäß Art. 28 DSGVO als Auftragnehmer wird die Kontrolle der vertraglich zugesicherten datenschutzrechtlichen Rahmenbedingungen durch den Datenschutzbeauftragten überwacht.

**Anlage 2: Zugelassene Subunternehmen gem. Ziffer 6**

| Name | Anschrift | Auftragsinhalt |
|---|---|---|
| Magicline GmbH | Raboisen 6<br>20095 Hamburg<br>Deutschland | Übermittlung von Daten zum Factoring |
| CORPEX Internet GmbH | Schauenburgerstraße 6<br>20095 Hamburg<br>Deutschland | Hosting der Infrastruktur |
| Tennis Point, s.r.o. | Za plavárňou 3937/1<br>Žilina 010 08<br>Slovakia | Unterstützung der Backend-Entwicklung |
| Pay Due Inkasso GmbH | Hauptstraße 38a<br>7000 Eisenstadt<br>Österreich | Übergabe von Akten an das Inkasso |
| V.O.P GmbH & Co. KG | Hauptstraße 62<br>56745 Bell<br>Deutschland | Übergabe von Akten an das Inkasso |
| GTX GmbH | Erftstraße 19a<br>50672 Köln<br>Deutschland | SMS-Dienstleister zum Versenden von Nachrichten an Mitglieder |
| Deutsche Post AG | Öhlmühlweg 12<br>61462 Königstein | Versand von Briefen per ePost-Schnittstelle |
| CRIF Bürgel GmbH | Radlkoferstraße 2<br>81373 München | Adressermittlung |