EGYM

Datenschutz-Handbuch für Fitnesseinrichtungen

EGYM

Inhalt

A. Einleitung

Dieses Handbuch verschafft Ihnen eine erste Orientierung zum Thema Datenschutz. Neben allgemeinen Erläuterungen zu den wesentlichen Inhalten und Vorgaben des Datenschutzrechts möchten wir Ihnen außerdem eine Hilfestellung zu möglichen datenschutzrechtlichen Fragestellungen, die Sie oder Ihr Datenschutzbeauftragter im Zusammenhang mit der Nutzung der EGYM-Produktwelt in ihrer Fitnesseinrichtung geben.

Zu den Fitnesseinrichtungen zählen hier kommerzielle sowie unternehmenseigene Fitnessstudios und Physiotherapiepraxen. Zur Vereinfachung ist im Folgenden gleichermaßen von der Einrichtung oder dem Studio die Rede.

Bei Fragen zu den hier gegebenen Informationen und allen anderen datenschutzrechtlichen Themen bzgl. EGYM steht Ihnen unser Datenschutzbeauftragter gerne unter datenschutz@egym.de zur Verfügung.
Bitte beachten Sie: Dieses Handbuch stellt lediglich eine Orientierungshilfe dar und ist keine rechtsverbindliche Auskunft. Wir übernehmen keine Gewähr für die Vollständigkeit und Aktualität der Inhalte.

B. Handbuch

I. Allgemeine Fragen zum Datenschutz

1. Einführung

a) Was ist Datenschutz?

Datenschutz ist der Schutz des Bürgers vor Beeinträchtigungen seiner Privatsphäre durch unbefugte Erhebung, Speicherung und Weitergabe von Daten, die seine Person betreffen. Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollen gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten gewahrt bleiben.
Datenschutz gewährleistet dabei insbesondere den Schutz des Persönlichkeitsrechts und das Recht auf informationelle Selbstbestimmung. Beide Rechte beruhen auf Art. 1 und Art. 2 des Grundgesetzes.

Die neue Fassung des Bundesdatenschutzgesetzes (BDSG (neu)) legt unter Beachtung der Datenschutzgesetze der einzelnen Länder den Umgang mit personenbezogenen Daten fest. Es ergänzt die EU-weit geltende Datenschutz-Grundverordnung (DSGVO). Die neue Fassung des BDSG finden Sie unter https://dsgvo-gesetz.de/bdsg-neu/.

b) Welche Gesetze regeln den Datenschutz??

Die Datenschutz-Grundverordnung (DSGVO) ist eine Verordnung der EU, mit der die Regeln für die Verarbeitung von personenbezogenen Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Die DSGVO enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und sichert dadurch die Grundrechte und Grundfreiheiten, insbesondere das Recht auf informationelle Selbstbestimmung natürlicher Personen.

Ergänzend zur DSGVO findet in Deutschland das Bundesdatenschutzgesetz (BDSG (neu)) Anwendung, welches unter Beachtung der Datenschutzgesetze der einzelnen Länder den Umgang mit personenbezogenen Daten festlegt.

d) Was sind personenbezogene Daten?

Gemäß Art. 4 Abs. 1 DSGVO sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

Dazu zählen u. a.:

- Name, Alter, Familienstand, Geburtsdatum
- Anschrift, Telefonnummer, E-Mail-Adresse
- Kontonummer, Kreditkartennummer
- Personalausweisnummer, Sozialversicherungsnummer
- Kunden-/Lieferantendaten (z.B. Namen von Ansprechpartnern, E-Mail-Kontaktdaten)
- Personaldaten von Beschäftigten

Im Zusammenhang z.B. zu Ihrer Website relevant ist auch, dass z.B. IP-Adressen und Online-Identifier nach Auffassung der Rechtsprechung und der Aufsichtsbehörden personenbezogene Daten darstellen.

Auch Fotos, Videoaufnahmen, Röntgenbilder oder Audioaufzeichnungen können personenbezogene Daten darstellen, soweit hierüber eine Person identifizierbar ist.
In Ihrer Einrichtung speziell auch:

- Mitglieder-Stammdaten (Name, Adresse etc.)

- Check-in & Check-out-Zeiten
- Trainingspläne
- Trainingsaufgaben
- Ergebnisse aus Fitness- und Gesundheitstests

e) Was sind besondere Kategorien personenbezogener Daten und wie werden diese geschützt?

Einem besonderen Schutz unterliegen sog. besondere Kategorien personenbezogener Daten gem. Art. 9 DSGVO.

Hierzu zählen z.B. Angaben zur rassischen und ethnischen Herkunft oder **Gesundheitsdaten**. Letztere sind wohl die bedeutendsten für Fitnessstudios, da sich diese auf die körperliche und geistige Gesundheit einer Person beziehen und die Möglichkeit besteht, dass hieraus Informationen zum Gesundheitszustand einer Person hervorgehen oder Rückschlüsse auf den Gesundheitszustand gezogen werden können.

Wichtig: Dabei sollte der Begriff der Gesundheitsdaten nicht synonym mit Daten zu Krankheiten einer Person verstanden werden. Zu “Gesundheitsdaten” zählen nämlich gleichermaßen auch Angaben, Informationen und Daten, aus denen sich z.B. ein Rückschluss auf eine gute Gesundheit einer Person ergeben kann.

Auch in Ihrer Einrichtung verarbeiten Sie unter Umständen Gesundheitsdaten ihrer Mitglieder. Wenn Sie beispielsweise Fitness-, Belastungs- oder Leistungstests durchführen oder ggf. Vorerkrankungen und gesundheitliche Besonderheiten einer Person vermerken, um das Training der Person zu optimieren. Dasselbe gilt z.B. für die Gesundheitsanalyse durch einen Trainer Ihrer Einrichtung mithilfe der EGYM Trainer App.

Eine Verarbeitung von Gesundheitsdaten bedarf immer einer ausdrücklichen Einwilligung des Mitglieds, die sich konkret auf die Verarbeitung von Gesundheitsdaten beziehen muss.

f) Verantwortliche Stelle

Verantwortliche Stelle im Sinne der DSGVO ist jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

Konkret in Bezug auf die Verarbeitung der personenbezogenen Daten, die in Ihrer Einrichtung erhoben werden, entscheiden Sie über die Zwecke und Mittel der Verarbeitung und sind damit “Verantwortlicher” im Sinne von Art. 4 Nr. 7 DSGVO.

Zur **Abgrenzung der Verantwortlichkeiten zwischen EGYM und Einrichtung in den jeweiligen Verantwortungsbereichen siehe bitte auch die Informationen in Abschnitt II unten.**

2. Grundlegende Vorschriften der DSGVO

a) Grundsätze der Verarbeitung personenbezogener Daten gem. Art. 5 DSGVO

Als Studiobetreiber sind Sie für personenbezogene Daten verantwortlich, die bei Ihnen erhoben oder verarbeitet werden. Dazu müssen Sie nach Art. 5 Abs. 1 DSGVO unter anderem folgende Grundsätze bei der Verarbeitung personenbezogener Daten einhalten:

✓ **Rechtmäßigkeit der Verarbeitung**
Damit eine Verarbeitung rechtmäßig ist, müssen personenbezogene Daten mit der Einwilligung der betroffenen Person oder auf einer sonstigen zulässigen Rechtsgrundlage verarbeitet werden.

Stellen Sie sicher, dass vor jeder Verarbeitung eine Einwilligung eingeholt wurde oder für die Verarbeitung eine andere Rechtsgrundlage besteht, z.B. soweit die Verarbeitung für die Durchführung des Vertrags mit dem Mitglied Ihrer Einrichtung erforderlich ist, kann eine Verarbeitung auch hierauf gestützt werden. Wichtig: Für Gesundheitsdaten (z.B. Ergebnisse aus Fitnesstests etc.) benötigen Sie immer eine Einwilligung des Mitglieds.

✓ **Transparenz**
Alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten müssen leicht zugänglich, verständlich und in klarer und einfacher Sprache abgefasst sein.

Datenschutzhinweise des Studios oder ähnliche Erläuterungen zum Datenschutz müssen für das Mitglied jederzeit abrufbar / einsehbar sein und dürfen nicht versteckt oder schwer zu finden sein.

✓ **Zweckbindung**
Die Zwecke der Verarbeitung müssen bereits bei der Erhebung personenbezogener Daten festgelegt, eindeutig und legitim sein. Eine Weiterverarbeitung zu anderen Zwecken ist gleichwohl möglich, sofern die Zwecke der Weiterverarbeitung nicht mit den ursprünglichen Erhebungszwecken unvereinbar sind und eine Rechtsgrundlage hierfür vorliegt.

Nutzen Sie beispielsweise E-Mail-Adressen nicht für Werbung, wenn dafür keine Einwilligung eingeholt wurde.

✓ **Datenminimierung**
Personenbezogene Daten müssen dem Zweck angemessen und für die Erreichung des Zwecks erforderlich sein sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.

Fragen Sie sich beispielsweise: Brauche ich tatsächlich die Telefonnummern der Mitglieder, wenn diese praktisch nie angerufen werden müssen?

✓ **Richtigkeit der Datenverarbeitung**
Personenbezogene Daten müssen sachlich richtig und auf dem neuesten Stand sein.

Gemeint ist damit, dass diejenigen Daten auf dem aktuellen Stand zu sein haben, die für eine vertragsmäßige Erfüllung benötigt werden, also müssen beispielsweise die Trainingspläne beim richtigen Mitglied hinterlegt werden.

✓ **Speicherbegrenzung**
Sobald die Speicherung für den Verarbeitungszweck nicht mehr erforderlich ist, müssen personenbezogene Daten gelöscht oder die Identifizierung der betroffenen Person aufgehoben werden.

Löschen Sie die Mitgliederdaten bzw. sperren (also so, dass Sie diese nicht mehr nutzen können) Sie die vertragsbezogenen Daten unter Beachtung der gesetzlichen Aufbewahrungspflichten (z.B. § 257 HGB) , wenn der Mitgliedsvertrag mit Ihrer Fitnesseinrichtung abgelaufen ist.

✓ **Integrität und Vertraulichkeit**
Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet. Dies umfasst u.a. den Schutz vor unbefugter und unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, Zerstörung oder Schädigung. Hierfür sind technische und organisatorische Maßnahmen zu treffen. Nähere Informationen finden Sie hier (S. 29).

✓ **Rechenschaftspflicht**
Der Verantwortliche ist für die Einhaltung der hier genannten Grundsätze nicht nur verantwortlich, sondern muss diese auch auf Nachfrage nachweisen können.

Im Falle einer Kontrolle durch die Aufsichtsbehörde oder eines Auskunftsverlangen eines Studiomitglieds muss die Einhaltung der Grundsätze nachgewiesen werden.

b) Bestehen einer Rechtsgrundlage für die Verarbeitung

Die Verarbeitung personenbezogener Daten ist **nur** zulässig, soweit der Betroffene in die Verarbeitung eingewilligt hat oder die Verarbeitung durch eine sie deckende Rechtsvorschrift legitimiert ist (sog. Erlaubnistatbestand). Diese finden sich in Art. 6 Abs. 1 DSGVO.

Hierunter fällt beispielsweise die Verarbeitung für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist oder wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist oder ein berechtigtes Interesse des Verantwortlichen besteht.

Wichtig: Für die Verarbeitung von Gesundheitsdaten (siehe oben) ist im Fitnessstudiokontext immer eine Einwilligung des Mitglieds erforderlich, die sich konkret auf die Verarbeitung von Gesundheitsdaten beziehen muss und für die im Übrigen dieselben Anforderungen gemäß Art. 7 DSGVO gelten.

c) Betroffenenrechte

Im Folgenden soll ein Überblick über die Rechte der Betroffenen gem. Art. 12 ff. DSGVO gegeben werden, die einer betroffenen Person die Ausübung ihrer gesetzlichen Rechte erleichtert. Dazu zählen:

✓ **Informationspflichten**
Art. 13 und Art. 14 DSGVO sehen einen umfangreichen Katalog von Informationspflichten vor.
Im Allgemeinen geht es dabei um die Informationspflicht bei bzw. vor Erhebung von personenbezogenen Daten bei der betroffenen Person (z.B. in den Datenschutzhinweisen) und die Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.
Bitte entnehmen Sie den Gesetzestexten zu Art. 13 und Art. 14, welche Informationen bereitgestellt werden müssen.

Informieren Sie Ihre Mitglieder beispielsweise Datenschutzhinweise auf der Webseite (für Websitebesucher) und als Anlage zum Mitgliedsvertrag (für Studiomitglieder). In Bezug auf die Nutzung der EGYM-Dienste durch Ihre Einrichtung haben wir Ihnen einen Passus vorbereitet, den Sie für Ihre

Datenschutzhinweise für Studiomitglieder verwenden können. Diesen finden Sie unten in Ziffer II Punkt 6.

✓ **Auskunftsrecht**
Betroffene Personen haben ein Recht auf Auskunft gegenüber dem Verantwortlichen über die von ihnen verarbeiteten personenbezogenen Daten. Mitglieder können beispielsweise Auskunft verlangen, welche personenbezogenen Daten von ihnen gespeichert und verwendet werden (z.B. Name, Anschrift, E-Mail-Adresse, besondere Kategorien personenbezogener Daten (S. 9), …)

Gerne können Sie sich an EGYM wenden, wenn ihre Mitglieder bei Ihnen Auskunft über die bei EGYM gespeicherten Daten verlangen.

✓ **Recht auf Löschung („Recht auf Vergessenwerden“)**
Betroffene haben außerdem das Recht, die Löschung ihrer Daten zu verlangen. Das ist zum Beispiel dann möglich, wenn diese zu dem Zweck, zu dem sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr erforderlich sind, sie unrechtmäßig verarbeitet wurden oder die einmalig gegebene Einwilligung widerrufen wurde.
Wichtig dabei ist, dass laut DSGVO keine Vernichtung notwendig ist, sondern eine Unkenntlichmachung ausreicht, die eine weitere Verwendung ausschließt. Als besondere Ausformung besteht nun auch das ausdrückliche „Recht auf Vergessenwerden“, wenn die verantwortliche Stelle die zu löschenden Daten öffentlich gemacht oder an Dritte übermittelt hat.

Verlangt ein Mitglied die Löschung beziehungsweise Unkenntlichmachung der Daten, so müssen diese gänzlich aus den eigenen Systemen entfernt werden, da für die weitere Verwendung keine Rechtsgrundlage mehr besteht, soweit keine gesetzlichen Aufbewahrungspflichten für (Teile) der Daten bestehen, z.B. aus § 257 HGB. In diesem Fall muss auch EGYM als verarbeitende Stelle ebenfalls informiert werden, soweit Daten betroffen sind, die EGYM für das Studio als sog. Auftragsverarbeiter verarbeitet Daten der Betroffenen Person.

✓ **Recht auf Berichtigung**
Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger beziehungsweise die Vervollständigung unvollständiger personenbezogener Daten zu verlangen.

Auch hier ist eine Mitteilung an EGYM bei solchen Daten essentiell, die EGYM im Auftrag des Studios als Auftragsverarbeiter verarbeitet, um die Fehlerhaftigkeit an allen Stellen zu beseitigen

✓ **Recht auf Einschränkung der Verarbeitung**
Unter den in Art. 18 genannten Voraussetzungen (z.B. während Verantwortlicher die Richtigkeit der Daten überprüft oder als Alternative zur Löschung bei vorliegender unrechtmäßiger Verarbeitung) hat die betroffene Person das Recht, von dem Verantwortlichen die Einschränkung der Verarbeitung zu verlangen.

Dies kann beispielsweise zur Überbrückung verlangt werden, wenn unrichtige Daten im Umlauf sind und Zeit zur Berichtigung beansprucht wird. Auch in diesem Fall muss EGYM als verarbeitende Stelle informiert werden.

✓ **Widerspruchsrecht**
Betroffene Personen haben außerdem ein Widerspruchsrecht gegen eine an sich rechtmäßige Verarbeitung ihrer Daten. Liegt die Datenverarbeitung beispielsweise im öffentlichen Interesse, dürfen diese Daten nur noch verarbeitet werden, wenn zwingende berechtigte Gründe für die Verarbeitung nachweisbar sind, „die die Interessen, Rechte und Freiheiten des Betroffenen überwiegen“ (Art. 21 Abs. 1 DSGVO).

Die Verarbeitung durch Studios basiert zwar grundsätzlich auf der Einwilligung der Mitglieder (Widerruf möglich), in wenigen Fällen kann allerdings auch der Widerspruch gegen die Verarbeitung erfolgen. EGYM muss hier ebenso in den Prozess eingebunden werden, um die weitere Verarbeitung stoppen zu können.

✓ **Recht auf Datenübertragbarkeit**
Das Recht auf Datenübertragung gibt betroffenen Personen unter bestimmten Voraussetzungen einen Anspruch, eine Kopie der sie betreffenden personenbezogenen Daten in einem üblichen und maschinenlesbaren Dateiformat zu erhalten.
Der Nutzer hat damit beispielsweise das Recht, Daten von einem Fitnessstudio zu einem anderen „mitzunehmen“.

Fragen Sie hierzu bei EGYM an, um einen Auszug aller bei EGYM verarbeiteten Daten für das Mitglied zu erhalten. Personenbezogene Daten, die in Ihren Systemen gespeicherte sind, müssen Sie dem Mitglied auf Anfrage ebenfalls zur Verfügung stellen.

d) Welche weiteren Pflichten haben verantwortliche Stellen?

- Bestellung eines Datenschutzbeauftragten, soweit für Ihre Einrichtung erforderlich (siehe Art. 37 DSGVO iVm. § 38 BDSG): Der Datenschutzbeauftragte im Unternehmen sorgt im Rahmen seiner Tätigkeiten für ein angemessenes Schutzniveau. und geeignete Maßnahmen, die der Wahrung des Grundsatzes der Datenvermeidung und Datensparsamkeit dienen.

- Erstellung eines Verzeichnisses über Verarbeitungstätigkeiten gemäß Art. 30 DS-GV

- Durchführung und Dokumentation von Vorabkontrollen bei automatisierten Verarbeitungen mit besonderen Risiken für Betroffene gemäß Art. 35 DS-GVO

- Durchführung datenschutzrechtlicher Mitarbeiterschulungen

- Prüfung, Definition und Dokumentation von angemessenen, technischen und organisatorischen Sicherheitsmaßnahmen zum Schutz der von der Einrichtung verarbeiteten personenbezogenen Daten gemäß Art. 32 DS-GVO

e) Was ist Auftragsverarbeitung?

Man spricht von einer Auftragsverarbeitung, wenn personenbezogene Daten durch eine andere Stelle im Auftrag und auf Weisung eines datenschutzrechtlichen Verantwortlichen für diesen verarbeitet werden. Dies darf nur auf Grundlage eines Vertrags nach Maßgabe von Art. 28 DS-GVO erfolgen. Der Auftragsverarbeiter handelt dabei immer streng weisungsgebunden, d.h. er darf nur im Rahmen der Weisung des Auftraggebers handeln. Für die Verarbeitung der Daten durch den Auftragsverarbeiter/Auftragnehmer werden diesem daher selbstständige datenschutzrechtliche Pflichten auferlegt (z.B. Führung von Verfahrensverzeichnissen, Zusammenarbeit mit der Aufsichtsbehörde, Datensicherheit durch technische und organisatorische Maßnahmen…)

Beispiele für die typischen Fälle von Auftragsverarbeitungen sind:

- Cloud-Computing
- Wartung von IT-Systemen oder Telekommunikationsanlagen
- externer Support
- Kontakterhebung durch ein Callcenter

f) Wer kontrolliert Unternehmen bei der Erfüllung ihrer Datenschutzaufgaben?

Jede Aufsichtsbehörde muss „in ihrem Hoheitsgebiet“ die Anwendung der DSGVO überwachen und durchsetzen. Dies wird durch stichprobenartige Kontrollen bei Unternehmen erreicht.

Für jedes Bundesland ist eine bestimmte Aufsichtsbehörde zuständig. Der Ansprechpartner für Unternehmen mit Hauptsitz in Bayern ist beispielsweise das bayerische Landesamt für Datenschutzaufsicht.

g) Was muss ich tun bei Datenpannen?

Im Falle der Verletzung des Schutzes personenbezogener Daten, gesetzlich in Ziffer 4 Nr. 12 DS-GVO definiert als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden (z.B. durch einen Hacker-Angriff, Verlust eines Datenträgers oder mobilen Endgeräts) können Melde- und Benachrichtigungspflichten entstehen.

Wenn die Datenpanne zu einem Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt, dann…

Art. 33 Meldung der Datenpanne an die zuständige Aufsichtsbehörde

Die Aufsichtsbehörde ist unverzüglich und möglichst binnen 72 Stunden über die Datenschutzverletzung zu informieren.

Wenn die Datenpanne zu einem hohes Risiko für die persönlichen Rechte und Freiheiten des Betroffenen führt, ist neben der Meldung an die Aufsichtsbehörde (siehe oben) dann zusätzlich...

Art. 34 Benachrichtigung der Datenpanne an die Betroffenen nach DSGVO

Der Betroffene ist unverzüglich gem. Art. 34 über die Datenschutzverletzung in klarer und einfacher Sprache zu unterrichten.

II. Auftragsverarbeitung durch EGYM für die Einrichtung / Abgrenzung eigenständige Verantwortlichkeit von EGYM

1. Studiodaten vs. EGYM-Daten

a) Studiodaten (EGYM als Auftragsverarbeiter)

Im Rahmen der Leistungserbringung durch EGYM für die Einrichtung, also immer dann wenn die Einrichtung EGYM Produkte wie die EGYM Cloud, Trainer App und Branded Member App von EGYM bezieht, verarbeitet EGYM im Auftrag der Einrichtung bestimmte personenbezogene Daten von Mitgliedern/Nutzer der Einrichtung. Deshalb schließt EGYM mit allen Einrichtungen eine sog. Auftragsverarbeitungs-Vereinbarung nach Maßgabe von Art. 28 Abs. 3 DS-GVO ab.

Die Auftragsverarbeitung durch EGYM für die Einrichtung bezieht sich dabei auf die Verarbeitung personenbezogener Daten im Rahmen der Nutzung bestimmter Funktionalitäten der EGYM Produkte durch die Einrichtung sowie im Falle der Integration mit der Studioverwaltungssoftware bzw. Member Management Software ("MMS") der Einrichtung an die EGYM Cloud auf die Übermittlung und Verarbeitung von personenbezogenen Daten von Mitgliedern/Nutzern der Einrichtung durch EGYM im Auftrag der Einrichtung. Insoweit ist EGYM Auftragsverarbeiter gemäß Art. 28 DS-GVO und die Einrichtung als "Herr der Mitgliedsdaten" Verantwortlicher für die Datenverarbeitung gemäß Art. 4 Nr. 7 DS-GVO.

Mitgliedsdaten sind dabei die vom Studio selbst erhobenen Daten und/oder im Rahmen der Nutzung der EGYM Trainer App von Trainern ihrer Einrichtung erfassten Daten ihrer Mitglieder (Stammdaten, Mitgliedsdaten, Vertragsdaten, Check-in Daten, Daten aus Fitness- und Gesundheitstests, die das Studio z.B. über die EGYM Trainer App durchführt etc.; bei der Branded Member App z.B. auch Daten zu Kursbuchungen etc.), mit denen Sie diese optimal und effizient betreuen können. Wir sprechen insoweit auch von "Studiodaten", da diese Daten eng mit dem Vertragsverhältnis zwischen Einrichtung und Mitglied verbunden sind. Da EGYM nicht Partei dieses Vertragsverhältnisses zwischen Einrichtung und Mitglied ist, maßt sich EGYM nicht an, "Herr dieser Daten" zu sein und verarbeitet diese Daten ausschließlich und streng weisungsgebunden im Auftrag des Studios als Auftragsverarbeiter.

b) EGYM-Daten (EGYM als datenschutzrechtlich selbständig Verantwortlicher)

Neben der Datenintegration über das MMS und der Zur-Verfügung-Stellung bestimmter Funktionalitäten der EGYM Produkte, verarbeitet EGYM personenbezogene Daten der

Mitglieder/Nutzer der Einrichtung aber auch auf Basis eines eigenen Vertragsverhältnisses zwischen EGYM und den Mitgliedern/Nutzern als eigenständig Verantwortlicher, soweit das Mitglied/der Nutzer einen EGYM Nutzeraccount nach Maßgabe der Nutzungsbedingungen und den Datenschutzhinweisen von EGYM erstellt, z.B. wenn das Mitglied an einer EGYM Kraftmaschine, in der Branded Member App oder im Fitness Hub einen EGYM Nutzeraccount erstellt. In diesem Rahmen ist dann alleine EGYM datenschutzrechtlich Verantwortlicher für die von Nutzern erhobenen und verarbeiteten Daten und hat insoweit EGYM alle Verpflichtungen gemäß der Datenschutzgesetze in eigener Verantwortung einzuhalten und zu erfüllen.

Es wäre nämlich für die Einrichtung nicht interessengerecht und entspricht auch nicht den tatsächlichen Gegebenheiten, der Einrichtung die Verantwortung für Datenverarbeitungen aufzuerlegen, die außerhalb ihrer eigenen Sphäre erfolgen und mit dem eigentlichen Verhältnis zwischen Einrichtung und Mitglied nichts zu tun haben. EGYM bietet den Nutzern mit dem Connected Training Floor die Möglichkeit, das eigene Training sowohl innerhalb der Einrichtung über die EGYM Kraftgeräte als auch durch die EGYM Fitness App und durch Branded Member App zu tracken und aufzuzeichnen, soweit der Nutzer sich dafür entscheidet, diese auf den Endnutzer ausgerichteten EGYM-Produkte zu nutzen. Für die datenschutzrechtlich ordnungsgemäße Verarbeitung der Nutzerdaten ist bei EGYM-Daten also alleine EGYM verantwortlich und nicht die Einrichtung.

c) Mirror-Opt-in (Datenaustausch/ Synchronisierung EGYM Profil / Studio-Profil)

Eine Besonderheit stellt der sog. “Mirror-Opt-in” dar. Nutzer/Mitglieder haben ein Interesse daran, dass sie z.B. Trainingspläne, die der Trainer der Einrichtung für sie in der EGYM Trainer App (Studio-Daten) erstellt hat, jederzeit auch in ihrer Branded Member App oder Fitness App (EGYM-Daten) aufrufen können. Umgekehrt haben Nutzer/Mitglieder auch ein Interesse daran, z.B. von EGYM erfasste Daten wie z.B. das BioAge (EGYM-Daten) mit ihrem Trainer in der Einrichtung zu teilen, damit der Trainer/die Einrichtung das Mitglied noch individueller und zielgerichteter betreuen kann.

Dafür haben wir den sog. Mirror-Opt-in kreiert, mit dem der Nutzer/das Mitglied freiwillig/optional und ausdrücklich darin einwilligen kann, dass die EGYM- und Studiodaten zu den vorgenannten Zwecken wechselseitig synchronisiert und aktualisiert werden. Der Nutzer/das Mitglied kann diese Einwilligung natürlich jederzeit ohne Nachteile befürchten zu müssen, widerrufen.

2. Auftragsverarbeitung durch EGYM für das Studio

In folgendem Modell können Sie sehen, wie die Auftragsverarbeitung durch EGYM erfolgt. Über die Studioverwaltungssoftware werden die erhobenen Daten an den EGYM Server übermittelt. Dort werden sie verarbeitet und in der Trainer App bereitgestellt. Dieser Vorgang kann nur durchgeführt werden, wenn EGYM vom Studio als Auftragsverarbeiter verpflichtet wird.

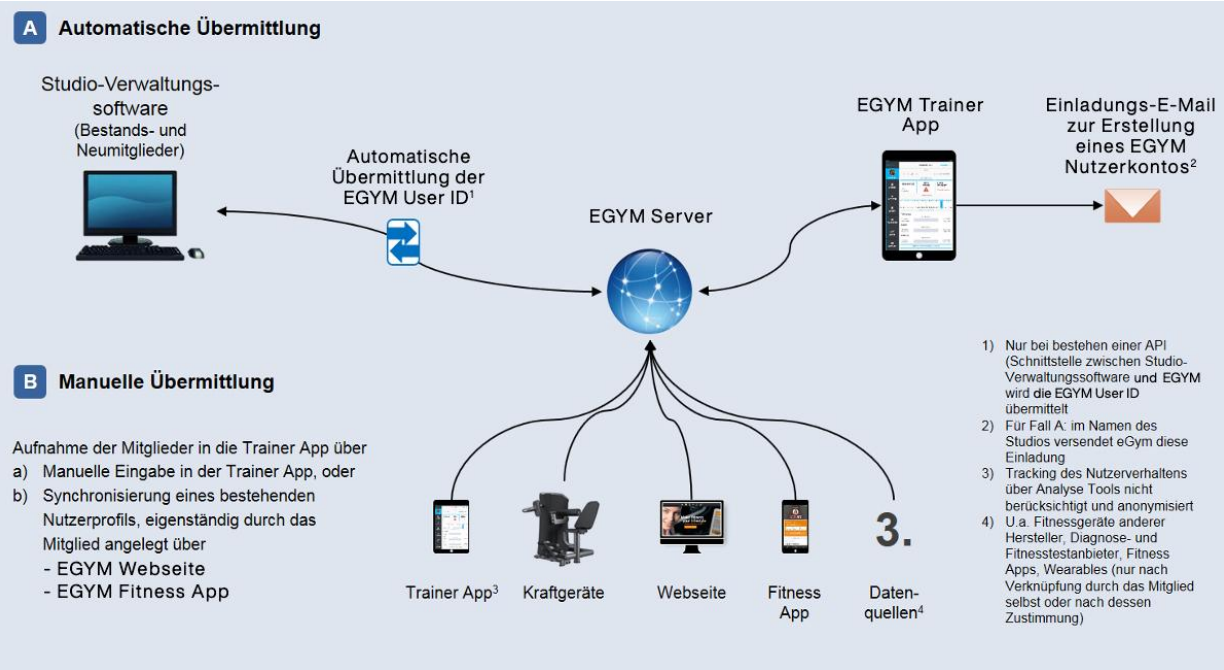
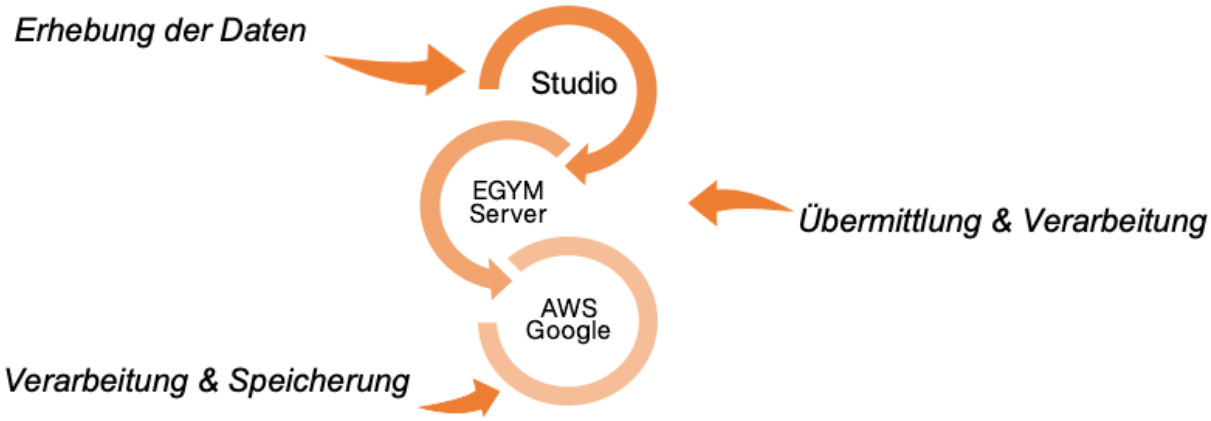


Abb.: Übermittlung personenbezogener Daten über und in die EGYM Trainer App

3.) Was bedeutet die Auftragsdatenverarbeitung für Studios?

Durch die Vereinbarung zur Auftragsverarbeitung zwischen EGYM und dem Studio wird die Rechtsgrundlage für die Übermittlung der im Studio erhobenen Daten und Verarbeitung durch EGYM festgelegt (siehe oben “Studiodaten”).

Weiterhin verarbeiten und speichern die externen Dienstleister **Amazon Webservices (AWS)** und **Google Ireland Ltd.** im Rahmen von deren sicheren Cloud-Lösungen als sog. Subunternehmer n deren Rechenzentren die Daten auf Grundlage einer Vereinbarung zur Auftragsdatenverarbeitung mit EGYM.



Die Rechenzentren der genannten Dienstleister befinden sich **innerhalb der EU/ dem EWR**. Wir haben mit beiden Dienstleistern die sog. “EU-Option” vereinbart. Siehe dazu bzgl. der Auswirkungen des EuGH Schrems II Urteils vom 16.07.2020 und die unsererseits durchgeführte Risikoanalyse die weiteren Informationen unten.

4. Liegt auch dann eine Auftragsverarbeitung durch EGYM vor, wenn durch meine Einrichtung gar keine MMS-Anbindung an die EGYM Cloud erfolgt?

Richtig ist, dass die Anbindung zwischen der Mitgliederverwaltungssoftware zwischen dem Fitnessstudio und EGYM sicher einen der Hauptanwendungsfälle für die Auftragsverarbeitung durch EGYM für das Studio darstellt.

Jedoch verarbeitet EGYM auch unabhängig von einer solchen Anbindung und wie in der Auftragsverarbeitungs-Vereinbarung auch näher beschrieben, personenbezogene Daten von Mitgliedern des Fitnessstudios im Auftrag und im Rahmen der Weisungen des Fitnessstudios und ist in diesem Zusammenhang entsprechend eine Auftragsverarbeitungs-Vereinbarung zwischen dem Fitnessstudio und EGYM erforderlich.

So geht zwar jeder Nutzer, der an einem EGYM Kraftgerät trainiert und dabei einen EGYM-Nutzeraccount anlegt, immer ein eigenständiges Vertragsverhältnis mit EGYM ein, für das ausschließlich EGYM vertrags- und datenschutzrechtlich verantwortlich ist und nicht das Fitnessstudio, insbesondere da diese Verarbeitungen personenbezogener Daten außerhalb des Einfluss- und Verantwortungsbereichs des Fitnessstudios liegen und es damit nicht interessengerecht ist, hierfür dem Studio die Verantwortung aufzuerlegen.

Andererseits gibt es aber auch Verarbeitungen personenbezogener Daten konkret in der EGYM Trainer App, auf die EGYM keinerlei Einfluss hat und bei denen es auch aus Sicht des Nutzers um reine, dem Studio zuzuordnende Verarbeitungen handelt. Dabei handelt es sich im Wesentlichen um solche Verarbeitungen und Daten, die der Trainer im Fitnessstudio im Rahmen der Nutzung der EGYM Trainer App selbst hinterlegt, korrigiert, ergänzt etc., also beispielsweise die Anlage von Trainingsplänen für das Mitglied und die Verwaltung dieser Pläne durch den Trainer, die Durchführung und Speicherung der Ergebnisse von Leistungs-, Gesundheits- und Fitnesstests, die der Trainer durchführt und hierbei die Funktionalitäten der Trainer App nutzt, Aktualisierung von Mitgliederdaten etc., also Verarbeitungen, die unabhängig von einem Vertragsverhältnis zwischen EGYM und dem Studio-Mitglied alleine in der Sphäre des Studios und seiner Trainer liegen.

Für diese Verarbeitungen stellt EGYM mit der Trainer App zwar die technische Infrastruktur zur Verfügung, hat aber keinen Einfluss auf das ob und wie der Verarbeitung (nur die Trainer im Einflussbereich/Verantwortungsbereich des Studios). Entsprechend ist die Trainer App daher wie eine klassische "Software as a Service“-Lösung zu bewerten, die Funktionalitäten bereitstellt, in deren Rahmen EGYM Daten streng weisungsgebunden im Auftrag des Studios verarbeitet.

Im Ergebnis ist daher auch bei Nutzung der EGYM Trainer App ohne MMS Anbindung immer eine Auftragsverarbeitung-Vereinbarung zwischen EGYM und dem Studio erforderlich.

5. Warum liegt keine gemeinsame Verantwortlichkeit gemäß Art. 26 DS-GVO vor?

Wir sehen bei EGYM im Hinblick auf die tatsächliche Ausgestaltung der Datenflüsse und im Hinblick auf das Geschäftsmodell von EGYM eine Ausgestaltung als gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO mit Studios aktuell nicht als einen Ansatz, der den beiderseitigen Interessen Rechnung trägt und sind der Ansicht, dass der auch vor Inkrafttreten der DSGVO erneut geprüfte Ansatz einer (teilweisen) Auftragsverarbeitung und im Übrigen einer getrennten Verantwortlichkeit (siehe oben) den tatsächlichen Abläufen, Datenflüssen und den Verantwortlichkeitsbereichen des Studios und EGYM eher gerecht wird.

Im Einzelnen:

- Gemeinsam mit einem Dritten ist nach Maßgabe der Rechtsprechung des EuGH verantwortlich, wer diesem aus eigenen wirtschaftlichen Interessen ermöglicht, personenbezogene Daten aus der eigenen Verantwortungssphäre zu verarbeiten und das Interesse des Dritten dahin geht, über dieselben Daten auch für eigene wirtschaftliche Zwecke verfügen zu können. Dafür haben wir auch berücksichtigt,

dass die Rechtsprechung nicht voraussetzt, dass die andere Partei zwingend Zugriff auf die Daten haben muss, um als gemeinsam Verantwortlicher zu gelten:

- Studio vs. EGYM: Nicht zutreffend, da Daten im Zusammenhang mit der Mitgliedschaft des Studiomitglieds beim Studio für EGYM nicht von (wirtschaftlichem) Interesse sind und diese von EGYM ausschließlich weisungsgebunden als Auftragsverarbeiter für das Studio für ausschließlich eigene Zwecke des Studios (Betreuung der Studio-Mitglieder) verarbeitet werden.

- EGYM vs. Studio: Erklärt z.B. an den EGYM-Kraftgeräten: Ob ein Studiomitglied die EGYM-Kraftgeräte nutzt, entscheidet das Studiomitglied selbst. D.h. von Studiomitgliedern, die nie EGYM-Geräte benutzen bzw. benutzen wollen, liegt entsprechend nie eine eigenständige Verantwortlichkeit von EGYM vor. Das Studio ermöglicht EGYM damit nicht Daten aus der eigenen Verantwortungssphäre im Studio zu verarbeiten, bloß weil EGYM Geräte im Studio aufgestellt werden, sondern handelt es sich um ein separates System im Studio und schließen die Mitglieder im Rahmen des eigenständigen Logins an den Maschinen ein eigenes Vertragsverhältnis mit EGYM nach Maßgabe der EGYM Nutzungsbedingungen und Datenschutzerklärung von EGYM ab. Die Geräte sind EGYM-gebrandet und der Nutzer sieht auf dem Screen, dass es sich hier um ein Standalone-Angebot eines Dritten handelt. Die damit im Zusammenhang stehenden Daten verarbeitet EGYM als eigenständig Verantwortlicher, weil das Studio nachvollziehbarer weise für die von EGYM eigenständig verarbeiteten Daten nicht als Verantwortlicher in die mögliche Haftung genommen werden sollte, zumal der Nutzer als EGYM-Mitglied weitreichende Möglichkeiten hat, auch sein Training außerhalb des Studios, z.B. via App zu tracken oder über Schnittstellen zu Drittgeräten, soweit der Nutzer diese Verbindung selbständig freigibt und darin einwilligt. D.h. auch aus Sicht des Betroffenen handelt es sich hier nicht um Daten, für die mehrere Parteien die Zwecke und Mittel festlegen.

  In diesem Zusammenhang kann sich der Nutzer auch dazu entscheiden, Trainingsdaten, die aus der Nutzung der Kraftgeräte resultieren, mit dem Studio zu teilen, um sich beispielsweise gezielt von Trainern betreuen zu lassen. Hierfür muss der Nutzer allerdings eine ausdrückliche Einwilligung in die Übermittlung/Synchronisation dieser als Gesundheitsdaten anzusehenden Daten erteilen, dass diese Daten mit dem Studio geteilt werden dürfen und in der Trainer App für den jeweiligen Trainer einsehbar sind. Der Trainer bzw. das Studio kann dann auf Basis dieser Daten das Training entsprechend anpassen, Empfehlungen aussprechen und Trainingspläne aktualisieren und tut dies wiederum als eigenständig Verantwortlicher. Die Rechtsgrundlage für die Übermittlung ist die ausdrückliche Einwilligung des Nutzers von einem Verantwortlichen an einen anderen Verantwortlichen, die der Betroffene selbst in absolut freier Entscheidung erteilen kann oder nicht und die er jederzeit mit einem Klick widerrufen kann. Damit wird auch dem Gedanken privacy by design Rechnung getragen, da es Studiomitglieder selbst in der Hand haben, ob Daten,

die für das reine Mitgliedsverhältnis zwischen Studio und Mitglied nicht erforderlich sind, mit dem Studio geteilt werden sollen oder nicht.

- Die Rechtsprechung erkennt ferner an, dass in den Pflichten- und Haftungskreis gemeinsamer Verantwortlichkeit nur einbezogen wird, wer auch tatsächlich Einfluss auf die Frage des „Ob“ einer Verarbeitung personenbezogener Daten nehmen kann.

    - Wie oben dargestellt, hat das Studio keine tatsächliche Einflussmöglichkeit auf das „Ob“ der Verarbeitung durch EGYM. Das „Ob“ (also ob eine Verarbeitung stattfindet durch EGYM im Zusammenhang mit den EGYM Produkten) beeinflusst ausschließlich das Mitglied selbst, in dem es sich aktiv für die Produkte von EGYM entscheidet.

    - Auch umgekehrt hat EGYM keine tatsächliche Einflussmöglichkeit im Zusammenhang mit den Mitgliedsdaten im Rahmen des Studio-Mitgliedschaftsvertrag. Über deren Verarbeitung entscheidet tatsächlich und nur das Studio über das „Ob“ der Datenverarbeitung, insoweit agiert EGYM aber als reiner Auftragsverarbeiter, weil EGYM keinen eigenen Bezugspunkt zum Mitgliedschaftsvertrag zwischen Studio und Mitglied hat (und auch kein dahingehendes eigenes Interesse an den Daten).

- Gelten aber für die Branded Member App Besonderheiten?

    Die App besteht im Wesentlichen aus studiobezogenen Funktionalitäten und erweiterten Möglichkeiten zur Erfassung von Trainings/Fitness-Aktivitäten außerhalb des Studios.

    Bzgl. der Erfassungsmöglichkeiten für Trainings- und Fitnessdaten des Nutzers wird immer ein eigenes Vertragsverhältnis zwischen EGYM und dem Nutzer erforderlich sein, da die Erfassungsmöglichkeiten für Training/Fitness für den Nutzer auch andere EGYM-Produkte, faktisch die gesamte EGYM-Produkt-Welt mit einbeziehen, um ein tatsächlich sinnvolles dem Nutzer dienliches Erfassen seiner Trainings-Aktivitäten auch außerhalb des Studios zu ermöglichen, seien es die eigene EGYM-Kraftgeräte, Kraftgeräte von Dritten, die mit EGYM verbunden sind, die EGYM-App, die Schnittstellen zu sonstigen Dritt-Anbietern (Waagen, Fitnesstracker etc.) sowie die Erfassung manuellen Trainings durch den Nutzer, insgesamt also aus diversen Quellen, für die EGYM datenschutzrechtlich verantwortlich ist für die Datenverarbeitung der Daten der Nutzer. Auf diese Erfassung und Verarbeitung hat das Studio keinerlei Einflussmöglichkeiten, daher ist es nicht sachgerecht hierfür dem Studio die Verantwortung auch nur als gemeinsam Verantwortlicher zu übertragen.

    Bzgl. der Studiodaten hingegen, also den Daten, die im Zusammenhang konkret mit der Mitgliedschaft des Nutzers stehen, erfolgt die Verarbeitung durch EGYM nur als Auftragsverarbeiter, da EGYM keine Einflussmöglichkeiten auf diese Daten hat und auch kein Interesse an diesen Studiodaten hat. Diese werden im

Zusammenhang mit der App daher von EYGM nur strikt weisungsgebunden verarbeitet, nämlich insoweit, als das Mitglied für die Nutzung der App als Studiomitglied verifiziert wird, Kurse bucht oder Mitgliedschaftsdaten abruft/einsieht oder ändert.

Die Parteien können wechselseitig keinen tatsächlichen Einfluss auf die Frage des „Ob“ einer Verarbeitung personenbezogener Daten der anderen Partei nehmen, was eine gemeinsame u.E. Verantwortlichkeit ausschließt.

- Wir evaluieren aber regelmäßig im Interesse von EGYM und den Kunden von EGYM die weitere Entwicklung und insbesondere Judikatur und etwaige Einlassungen der Aufsichtsbehörden zum Thema gemeinsame Verantwortlichkeit.

Sollte sich daraus ein Anpassungsbedarf der aktuellen Ausgestaltung ergeben, werden wir den derzeit verfolgten Ansatz erneut prüfen und ggf. die hieraus erforderlichen Konsequenzen ziehen.

6. Was muss ich als Studiobetreiber tun / Wie informiere ich meine Mitglieder über den Einsatz von EGYM als Auftragsverarbeiter?

Zudem sind Sie verantwortlich für die Umsetzung der Informationspflicht gem. Art. 13 DSGVO. Ein Hinweis in den Datenschutzhinweisen Ihrer Fitnesseinrichtung ist erforderlich, um Ihre Mitglieder über die Übermittlung Ihrer personenbezogenen Daten an die EGYM GmbH zu informieren.
Folgenden Musterpassus können Sie in Ihren Datenschutzhinweisen zur Information an Ihre Mitglieder hinzufügen:

Einsatz von EGYM Produkten/Dienstleistungen

*Wir setzen in unserer Einrichtung Produkte und Dienstleistungen der EGYM GmbH, Einsteinstraße 172, 81677 München ein. Das bezieht sich auf [**VOM STUDIO EINZUSETZEN: EGYM Kraftgeräte in unserem Studio, EGYM Cloud, EGYM Trainer App, EGYM Fitness Hub, EGYM Branded Member App**]. In diesem Zusammenhang agiert EGYM als sog. Auftragsverarbeiter und verarbeitet personenbezogene Daten von Mitgliedern auf Basis einer Auftragsverarbeitungs-Vereinbarung gemäß Art. 28 DSGVO in unserem Auftrag und nach unseren Weisungen, um Dienstleistungen im Zusammenhang mit der effektiven Betreuung unserer Mitglieder im Studio zu erbringen. Dies dient z.B. dem Zweck, das Training der Mitglieder über die EGYM Trainer App zu optimieren, indem wir Ihnen beispielsweise Trainingspläne und -analysen in unserer Einrichtung bereitstellen. Hierzu übermitteln wir im Rahmen der Auftragsverarbeitung personenbezogene Daten der Mitglieder an EGYM, die EGYM in unserem Auftrag zu den vorgenannten Zwecken verarbeitet; dies bezieht sich auf*

Mitgliederstammdaten (wie Name, E-Mail, Geburtsdatum etc.) und sonstigen Daten zu Ihrer Mitgliedschaft in unserer Einrichtung (z.B. Beginn der Mitgliedschaft).

Bitte beachten Sie, dass soweit Sie sich im Rahmen der optionalen Nutzung der EGYM Kraftgeräte in unserer Einrichtung und/oder für sonstige von EGYM selbst angebotene EGYM Dienste/Anwendungen (wie z.B. an EGYM Geräten, Branded Member App, Fitness Hub oder Fitness App) separat bei EGYM registrieren und einen EGYM-Nutzeraccount anlegen und damit ein eigenständiges Vertragsverhältnis über die Nutzung der EGYM Produkte/Anwendung mit EGYM abschließen, diese Datenschutzerklärung keine Anwendung findet und in diesem Zusammenhang EGYM selbst datenschutzrechtlich Verantwortlicher für die Verarbeitung Ihrer personenbezogenen Daten ist. Über die Verarbeitung Ihrer personenbezogenen Daten durch EGYM werden Sie in diesem Fall bei der Registrierung für EGYM Produkte/Anwendungen informiert.

Soweit Sie sich separat bei EGYM gemäß dem Vorstehenden registriert haben, können Sie optional und freiwillig darin einwilligen, dass Studio-Daten aus unserer Einrichtung mit Ihrem EGYM-Nutzerprofil und umgekehrt auch Daten aus Ihrem EGYM-Nutzerprofil mit Ihren Studio-Daten fortlaufend synchronisiert und aktualisiert werden, damit Sie die jeweiligen weitergehenden Funktionen der EGYM Dienste nutzen können (z.B. Abruf eines von ihrem Trainer erstellten Trainingsplans in der EGYM Fitness App). Zu den Studio-Daten, die wir im Falle Ihrer Einwilligung an EGYM übermitteln zählen dabei: Mitgliedschaftsbeginn/-ende, Foto, Geburtsdatum, Geschlecht, Trainingserfahrung, -pläne und -vorlagen. Mit der umgekehrten Bereitstellung von EGYM-Daten (die im Rahmen des Vertragsverhältnisses mit EGYM von EGYM verarbeitet werden) an uns, wird die Anzeige und Analyse Ihrer Trainingsdaten aus EGYM Produkten/Anwendungen durch Ihren Trainer der Fitnesseinrichtung sowie die Anzeige von Ergebnissen von Gesundheits- und Krafttests und Ihr BioAge für Ihren Trainer in der von uns genutzten EGYM Trainer App zum Zwecke der optimalen Betreuung in unserer Einrichtung ermöglicht. Für die Übermittlung Ihrer Daten einschließlich Ihrer Gesundheitsdaten wird hierfür von EGYM Ihre vorherige, ausdrückliche Einwilligung vor der Übermittlung eingeholt (Rechtsgrundlage ist Art. 6 Abs. 1 Satz 1 lit. a / Art. 9 Abs. 2 lit a DSGVO). Ihre Einwilligung können Sie natürlich jederzeit gegenüber EGYM widerrufen."

III. Datensicherheit bei EGYM

1. Was sind technische und organisatorische Maßnahmen?

Zur Einhaltung der datenschutzrechtlichen Vorschriften müssen Unternehmen Vorkehrungen zum Schutz der gespeicherten personenbezogenen Daten treffen. Nach den gesetzlichen Vorgaben in Art. 32 DSGVO ist es erforderlich, geeignete technische und organisatorische Maßnahmen (kurz: TOM) zu treffen, die die Sicherheit der Datenverarbeitung gewährleisten.

Im Wesentlichen geht es darum, die personenbezogenen Daten vor einem Zugriff durch unberechtigte Dritte oder vor versehentlicher Löschung zu schützen.
Dies gilt gleichermaßen für die EGYM GmbH als auch für Fitnessstudios.

Welche konkreten TOM ein Unternehmen ergreift, um die Sicherheit der Verarbeitung zu gewährleisten, steht im Ermessen des Unternehmens.
Entscheidend ist aber in jedem Fall , dass die getroffenen Maßnahmen einem der Verarbeitung angemessenen Datenschutzniveau entspricht.

In der Auftragsverarbeitungsvereinbarung mit EGYM finden Sie in der Anlage 1 eine abschließende Aufzählung der TOM, die EGYM zur Datensicherheit im Unternehmen trifft.

2. Wie schützt sich EGYM vor Verlust der Daten oder Datenpannen im Unternehmen?

EGYM verarbeitet (erhebt, speichert und verwendet) an seinem Hauptsitz in München lediglich Bewerber- und Mitarbeiterdaten.

Stammdaten, die an den Kraftgeräten und über die Fitness App erhoben werden sowie alle Trainingsdaten, die über die Studioverwaltungssoftware erhoben und im Auftrag der Studios durch EGYM verarbeitet werden, werden in externen und sicheren Rechenzentren gespeichert und verarbeitet.

Dazu hat EGYM Vereinbarungen zur Auftragsverarbeitung mit den externen Dienstleistern **Amazon Webservices** und **Google Ireland.** geschlossen.

Alle genannten Unternehmen sichern die Daten durch geeignete TOM vor Verlust, Cyberangriffen und Hackern ab und verfügen über zahlreiche und aktuelle Zertifizierungen im Zusammenhang mit der Informationssicherheit.

Einen Überblick über die Zertifizierungen von Amazon Webservices finden sie unter https://aws.amazon.com/de/compliance/ und https://aws.amazon.com/de/compliance/iso-certified/, für Google unter https://cloud.google.com/security/compliance/iso-27001 und https://cloud.google.com/security/compliance/iso-27001.

3. Werden Mitgliederdaten in Länder außerhalb der EU übermittelt?

Wie oben beschrieben, setzt EGYM als externe Dienstleister die Cloud-Computing Dienstleister **Amazon Webservices** und **Google Cloud Platform** (Google Ireland) ein.

Amazon Webservices und Google werden insoweit als sog. Subunternehmer für uns ebenfalls auf Basis von Auftragsverarbeitungs-Vereinbarungen eingesetzt und verarbeiten demnach in unserem Auftrag und streng weisungsgebunden personenbezogene Daten in unserem Auftrag, nämlich zur Speicherung der Daten in der Cloud.

Wir haben dabei sowohl mit Google als auch mit Amazon Webservices die sog. EU-Option vereinbart, d.h. die in unserem Auftrag gespeicherten personenbezogenen Daten werden von Amazon Webservices und Google ausschließlich in Rechenzentren innerhalb der EU/ dem EWR gespeichert

Prüfung der Auswirkungen des EuGH-Urteils Schrems II vom 16.07.2020

Selbstverständlich haben wir im Zuge des EuGH-Urteils vom 16.07.2020 (Schrems II), mit dem das bisher als zulässiges Transferinstrument für Datenübermittlungen in die USA, das sog. “Privacy Shield” für ungültig erklärt wurde und trotz der mit AWS und Google vereinbarten EU-Option und dem Abschluss der sog. EU-Standardvertragsklauseln evaluiert, inwieweit dennoch ein Risiko eines Datenzugriffs z.B. durch US-Behörden auf diese in der EU gespeicherten Daten besteht und wie dieses im Hinblick auf die Rechte und Freiheiten betroffener Personen zu bewerten ist.

Wir sind im Rahmen dieser Prüfung zu dem Ergebnis gekommen, dass auf Basis der vertraglichen Abreden und ergänzender, effektiver technischer Maßnahmen im Hinblick auf die Möglichkeit einer behördlichen Zugriffsanfrage (im Wesentlichen nur im Zusammenhang mit Supportleistungen z.B. von Konzerngesellschaften von Google und AWS, da die Daten zu jedem Zeitpunkt in der EU gespeichert bleiben) derzeit ein im Wesentlichen gleichwertiges Datenschutzniveau besteht. Wir haben Ihnen die wesentlichen Ergebnisse unserer Prüfung wie folgt für Ihre Dokumentation zusammengefasst.

- Wir haben im nächsten Schritt die derzeitigen Subunternehmer von AWS und Google in Drittländern auf die von diesen zu erbringenden Leistungen hin geprüft. Dabei handelt es sich im Wesentlichen um Service Maintenance und Support-Leistungen, die keinen zwingenden Transfer der in der EU gespeicherten Daten in Drittländer erforderlich machen.

- In Bezug auf die Anwendbarkeit des US Patriot Acts/ FISA und Cloud Act etc. haben wir des Weiteren geprüft, ob diese auf Google und AWS als Subunternehmer von EGYM Anwendung finden:

    - In Bezug auf Google haben wir hierfür die von Google zur Verfügung gestellten Informationen zur Anwendbarkeit in deren Whitepaper zum Schrems II Urteil

geprüft (https://services.google.com/fh/files/misc/gsuite_foredu_whitepaper_gdpr_schremsii.pdf). Wir haben dabei auch berücksichtigt, dass Google am 10.08.2020 als Reaktion auf das EuGH-Urteil die eigenen Model Contract Clauses in Ergänzung zu den Standardvertragsklauseln angepasst hat. Ferner haben wir die aktuelle Praxis und die Prozesse von Google in Bezug auf den Umgang mit Auskunfts- und Herausgabeansprüchen auf Basis der Selbstauskunft von Google geprüft, insbesondere dahingehend, ob Google angemessene Prozesse implementiert hat, die u.a. die gerichtliche Prüfung oder Anfechtung von Beschlüssen auf Auskunft/Herausgabe beinhalten und ob sonstige Maßnahmen zur Information der Kunden/Betroffenen ergriffen werden, was u.E. der Fall ist. (https://services.google.com/fh/files/misc/google_cloud_governmentrequestsfor_cloud_customer_data_v2_1018.pdf?hl=de).

- In Bezug auf AWS haben wir hierfür die von AWS öffentlich zur Verfügung gestellten Informationen zur Anwendbarkeit der US-Gesetze geprüft. Ferner haben wir die aktuelle Praxis und die Prozesse von AWS in Bezug auf den Umgang mit Auskunfts- und Herausgabeansprüchen auf Basis der Selbstauskunft von AWS geprüft, insbesondere dahingehend, ob AWS angemessene Prozesse implementiert hat, die u.a. die gerichtliche Prüfung oder Anfechtung von Beschlüssen auf Auskunft/Herausgabe beinhalten und ob sonstige Maßnahmen zur Information der Kunden/Betroffenen ergriffen werden, was u.E. der Fall ist und erst kürzlich im Februar 2021 seitens AWS noch durch zusätzliche Maßnahmen flankiert wurde (https://aws.amazon.com/de/blogs/security/aws-and-eu-data-transfers-strengthened-commitments-to-protect-customer-data/)

- Da sich ein Auskunftsgesuch/Herausgabegesuch bei Google oder AWS spezifisch auf die von EGYM gespeicherten Daten beziehen muss, haben wir ebenfalls im Rahmen des Risk Assessment geprüft, wie hoch die Wahrscheinlichkeit ist, dass die von EGYM gespeicherten Daten Gegenstand eines solchen Auskunfts- bzw. Herausgabeersuchens sein könnten und festgestellt, dass die Wahrscheinlichkeit u.E. aktuell eher gering einzustufen ist, da EGYM keine Kommunikationsdaten und/oder Daten, die ein exaktes Bewegungsprofil der Nutzer erlauben würden, speichert und demnach keine Daten, die im Zusammenhang im Wesentlichen mit Maßnahmen zur Terrorismusbekämpfung oder Strafverfolgung für eine anfragende Behörde wirklich von Belang sein könnten. Für diese Prüfung haben wir ferner berücksichtigt, dass EGYM selbst im Zusammenhang z.B. mit Terrorismusbekämpfung in der Vergangenheit ebenfalls keine entsprechenden Auskunfts- oder Herausgabeersuchen (von nationalen/internationalen (Strafverfolgungs-)Behörden etc.) erhalten hat.

- Wir haben ferner die bei EGYM bereits implementierten, technischen Schutzmechanismen in Bezug auf die bei Google und AWS in der Cloud in Europa gespeicherten Daten nach Maßgabe der EDSA-Empfehlungen vom 10.11.2020 evaluiert, insbesondere in Bezug auf die aktuell bereits implementierte Verschlüsselung (derzeit sowohl in transit als auch in rest) und dem Umstand, dass zumindest unserem derzeitigen Kenntnisstand nach die Encryption-Keys nur im Besitz der europäischen Google und AWS Gesellschaften und nicht der US-Konzerngesellschaften von Google bzw. AWS sind. Daraus haben wir gefolgert, dass damit zumindest eine zusätzliche technische Hürde für US-Konzerngesellschaften von Google bzw. AWS besteht, die Gegenstand eines Auskunftsverlangens seitens einer US-Behörde sein könnten und sind auch hier zu dem Schluss gekommen, dass mit den bereits bestehenden technischen Schutzmaßnahmen ein Zugriff auf Daten zumindest wesentlich erschwert wird.

- Wir werden aber, sobald die derzeit noch im Konsultationsverfahren befindlichen neuen EU-Standardvertragsklauseln zum Einsatz kommen können, diese neuen EU-Standardvertragsklauseln mit Google bzw. AWS abschließen. Sollte Google bzw. AWS diese neuen EU-Standardvertragsklauseln nicht als Transfermechanismus akzeptieren, werden wir einen etwaigen von Google bzw. AWS stattdessen vorgeschlagenen alternativen Transfermechanismus prüfen oder sonstige EGYM zur Verfügung stehenden Optionen im Verhältnis zu Google bzw. AWS (wie Sonderkündigungsrechte) prüfen.

III. Spezifische Fragen der Einrichtungen

1. Informationen zum Umgang mit personenbezogenen Daten

a. Welche Daten gehören zu den personenbezogenen Daten?

Genutzte personenbezogene Daten beim Training an einem EGYM Kraftgerät	**Genutzte personenbezogene Daten beim Nutzen der EGYM Trainer App**
Initial benötigte Daten zum Training - E-Mail-Adresse (auch als Alias) - RFID-Code(s) (durch RFID-CHip vergeben) **Erhobene Daten für das Training (je Kraftgerät)** - Sitzhöhe	**Daten von der Studio-Verwaltungssoftware[1]** - Vorname und Name - E-Mail-Adresse - Kontaktadresse - Telefonnummer - Liste der Indentifizierungs-Chips (RFID)

- Start- und Endposition - Ergebnis der Maximalkraftmessung - Initiale Trainingsmethode (Vorschlagswert) **Gespeicherte Daten (je Trainingseinheit und Kraftgerät)** - Trainingsfortschritt (absolvierte Trainingseinheiten) - Anzahl der Wiederholungen und Sätze - Bewegtes Trainingsgewicht - Trainierte Trainingsmethode **Weitere erhobene Nutzerdaten** - Anmeldeart (über Kraftgerät) - Anmeldeort (Fitnesseinrichtung) - Zustimmung zu den AGB - Datum und Uhrzeit der Anmeldung - Datum und Uhrzeit der Trainingseinheiten	- Mitgliedschaftsbeginn und -ende - Foto - Geburtsdatum - Geschlecht **In der Trainer App erfasste Daten[2]** - Geschlecht - Gewicht - Größe - Beruf, Arbeitshaltung, Hobbies und Sportarten - Studiobesuchsinformationen (Check-in- und Check-out-Zeitpunkte, Dauer, Besuchshäufigkeit, Trainingsintensität) - Geräteeinstellungen (z.B. Gewichte) - Trainingserfahrung -pläne - Fragebogen-Antworten aus dem Fitness-Check - Gesundheitszustand (Anamnese) - Trainings- und Fitnesstest-Ergebnisse - vom Mitglied gestellte Wünsche/Aufgaben und gewünschte Alerts - Zuordnung Mitglied zu Trainer - EGYM Premium Status - Mitglied ansprechbar / nicht ansprechbar

1) Abhängig von der Art der Schnittstelle. Alternativ können diese Daten auch manuell eingegeben werden.
2) Ausgenommen Login-Informationen des Studiobetreibers und Trainers

b. Wo werden die Daten gespeichert?

Die Daten, die an den EGYM Kraftgeräten erhoben werden sowie alle Daten, die über die Studioverwaltungssoftware im Rahmen der Auftragsverarbeitung an EGYM übermittelt werden, werden in Rechenzentren innerhalb der EU/ der EWR verarbeitet und gespeichert. Mehr Information dazu finden Sie in Abschnitt II.

Der RFID-Chip, welcher der vereinfachten Anmeldung an den Kraftgeräten dient, **speichert keinerlei** personenbezogene Daten. Bei erstmaliger Registrierung wird die Kennnummer der Chips mit der E-Mail-Adresse des Nutzers in der EGYM Cloud verknüpft. Durch diese Verknüpfung ist eine Übermittlung der erforderlichen Daten an das Kraftgerät möglich, um das Training an den Geräten zu ermöglichen (Übermittlung der Geräteeinstellungen sowie Trainingsmethode etc.).

Die Kraftgeräte sowie die Trainer App und die Fitness App speichern Daten nur temporär lokal, wenn die Geräte offline sind. Sofern eine Verbindung zum Internet besteht, werden alle Daten an die EGYM Cloud übermittelt.

c. Wie wissen wir sicher, dass EGYM die Daten nicht weitergibt?

Weil EGYM als Auftragsverarbeiter der Einrichtung ebenfalls weitreichenden gesetzlichen Pflichten der DSGVO unterliegt und sich gemäß der Auftragsverarbeitungs-Vereinbarung mit Ihnen auch vertraglich dazu verpflichtet hat, in Ihrem Auftrag verarbeitete Studio-Daten nur im Rahmen ihrer Weisungen zu verarbeiten. Das schließt selbstverständlich die Pflicht ein, Daten nicht unberechtigterweise an Dritte zu übermitteln/weiterzugeben.

d. Wozu werden die erhobenen Daten von EGYM verwendet?

Während dem Training an einem EGYM Kraftgerät werden Trainingsdaten erhoben, die automatisch mit der EGYM Cloud synchronisiert werden. Durch Angabe der E-Mailadresse in Verbindung mit einem RFID-Chip wird ein passwortgeschütztes Profil erstellt. Das Passwort wird durch den Nutzer zu einem späteren Zeitpunkt in der Fitness App oder auf der EGYM Webseite vergeben.

Über die Webseite und in der Fitness App werden die erhobenen Daten den Mitgliedern kostenlos zur Verfügung gestellt. Zusätzlich stellt EGYM die Daten den Fitnessstudios in der EGYM Trainer App zur Verfügung, damit diese eine individuelle und zielgerichtete Betreuung ihrer Mitglieder durchführen können.

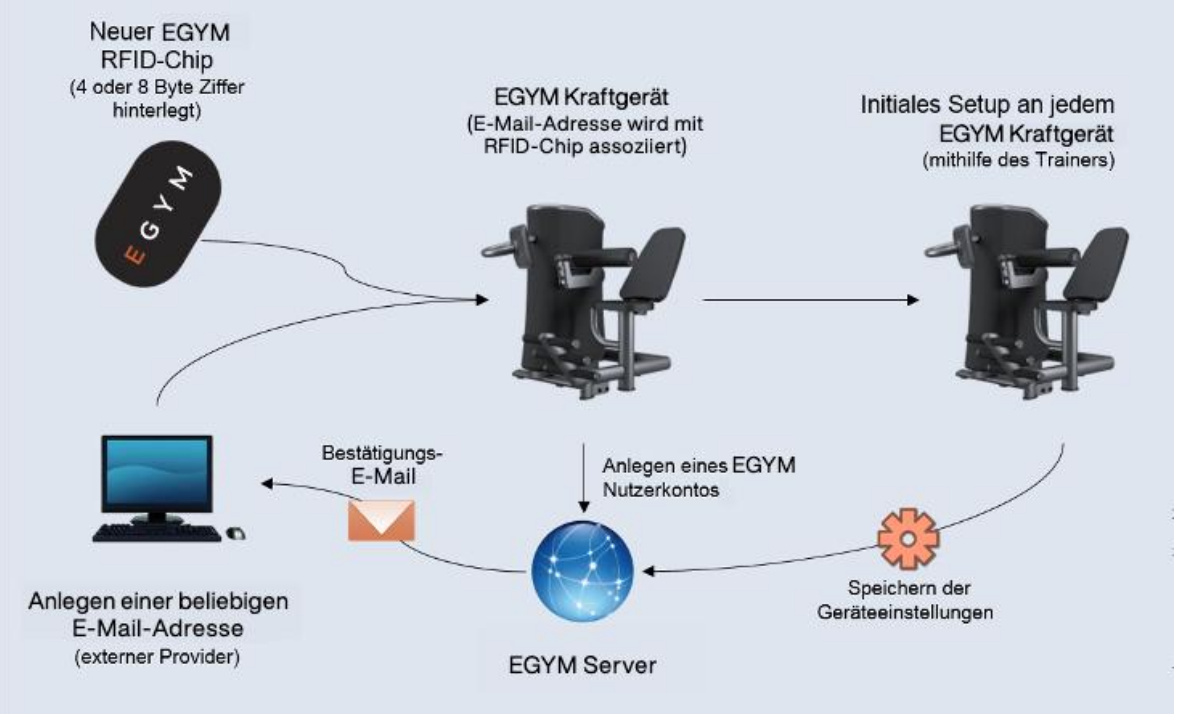


Abb.: Registrierung an einem EGYM Kraftgerät

Die Angabe der E-Mail-Adresse, die Maximalkraftmessung sowie die Größeneinstellung des Mitglieds an den Geräten ist erforderlich, um ein Training an den EGYM Geräten zu ermöglichen. Alle weiteren Informationen können optional angegeben und dadurch von EGYM erhoben werden, um weitere Funktionen nutzen zu können.

Im Rahmen der Auftragsdatenverarbeitung durch EGYM für die Studios können Trainings- und Stammdaten sowie Profilinformationen in der Trainer App verwendet werden, wie beispielsweise das Erstellen eines Trainingsplans für einen Nutzer durch einen Trainer oder das Analysieren des Trainings. Die Nutzer können sich außerdem über die „Ranking“ Funktion in Fitnessteams wiederfinden (studiobezogen) und werden somit zum Training motiviert.

E-Mail-Adresse, Maximalkraftmessung und Größeneinstellung des Mitglieds auf die Geräte ist für das Training an den Fitnessgeräten erforderlich. Alle weiteren Angaben sind optional.

2. Zugriffsberechtigte - Wer hat Zugriff auf die Daten bei EGYM?

Ausschließlich die zur Benutzung eines Datenverarbeitungssystems berechtigten Personen können im Rahmen ihrer Zugriffsberechtigung auf personenbezogene Daten zugreifen. Die Berechtigungen werden fachbereichsabhängig und nur für den

bestimmten Zweck vergeben.

Im konkreten Fall von EGYM sind das:

- Mitarbeiter des Kundendienstes bei Kundenanfragen
- IT-Administratoren bei Verstößen oder Pannen oder zur Wartung der Systeme
- Mitarbeiter der Personalabteilung bei Bewerber- und Mitgliederdaten

3. Speicherdauer - Wie lange werden die Daten gespeichert?

Studio-Daten werden nach Maßgabe der Auftragsverarbeitungs-Vereinbarung mit Ihrer Einrichtung nur für die Dauer des Auftrags, also so lange der zugrunde liegende Service-Vertrag mit Ihnen besteht, gespeichert und danach gelöscht.

IV. Mitgliederbezogene Fragen

Im Folgenden haben wir für Sie Antworten auf typische Fragen vorbereitet, die Ihre Mitglieder im Zusammenhang mit den EGYM-Produkten in Ihrer Einrichtung an Sie stellen könnten. Zögern Sie aber bitte nicht, Ihr Mitglied bei Fragen spezifisch zu den EGYM-Produkten auch direkt an uns zu verweisen, z.B. indem das Mitglied uns eine E-Mail an datenschutz@egym.com schickt.

1. Profilinformationen

a. Warum muss die E-Mail-Adresse angegeben werden?

EGYM richtet für jeden Nutzer, der sich für die Nutzung der EGYM Produkte entscheidet, ein Nutzerprofil ein. Erforderlich für die Erstellung eines Profils ist, dass sich der Nutzer an einem beliebigen Kraftgerät mit seiner E-Mail-Adresse registriert. Überdies ist die Registrierung auch auf der EGYM Webseite oder der EGYM App möglich. Nach erfolgreicher Registrierung erhalten die Nutzer eine entsprechende E-Mail-Bestätigung, mithilfe dieser sich die Nutzer ein Passwort setzen können, um auf die geschützten Bereiche wie Webseite oder Fitness App zugreifen zu können. Die Angabe der E-Mail-Adresse ist daher für das Training an EGYM Kraftgeräten unerlässlich.

b. Welche Daten sind auf dem RFID-Chip gespeichert?

Auf dem RFID-Chip werden keine personenbezogenen Daten gespeichert.
Speziell geschulte Trainer weisen den Nutzer bei der erstmaligen Nutzung an den Geräten ein und verknüpfen den RFID-Chip mit der E-Mail-Adresse des Nutzers.

Geräteeinstellungen wie Startposition und Bewegungsradius sowie das gewählte Trainingsziel und die Methode werden im passwortgeschützten EGYM Profil gespeichert.
Mithilfe des Chips kann das Mitglied sich jederzeit am Gerät identifizieren. Die Daten werden nun aus der EGYM Cloud an die Kraftgeräte übermittelt.

c. Kann die Bereitstellung der Daten vom Mitglied selbst reguliert werden?

Die Einstellungen zu personenbezogenen Daten können im Profil jederzeit selbst verändert werden. Auskünfte zu Körpergewicht und -größe, E-Mail- und Newsletter-Einstellungen, Geburtsdatum und Gesundheitsdaten für die Anamnese können manuell eingegeben bzw. gelöscht werden. Natürlich können auch alle weiteren Angaben zu Trainingshäufigkeit, bevorzugte Trainingstage, Länger der Trainingseinheit sowie Beruf, typische Arbeitshaltung, Hobbies und praktizierte Sportarten eingegeben werden, um eine zielgerichtete Betreuung zu ermöglichen und ein auf Analysen basierenden Trainingsplan zu erstellen.
Bitte beachten Sie, dass der Wunsch auf Löschung der E-Mail-Adresse die Löschung des Profils nach sich zieht und somit kein Training an den EGYM Geräten mehr möglich ist.

2. Einwilligung und Widerruf

a. Wie und wo können Mitglieder den EGYM Service abbestellen?

Durch Erklärung gegenüber EGYM in Form eines Widerrufs der Einwilligung gem. Art. 7 Abs. 3 DSGVO kann das Erheben und weitere Verarbeiten mit Wirkung für die Zukunft unterbunden werden.
Bitte beachten Sie, dass in diesem Fall keine weitere Leistung an das Mitglied durch EGYM erbracht werden kann. Insbesondere die Löschung eines Profils führt dazu, dass das Mitglied nicht mehr an den EGYM Kraftgeräten trainieren kann.
Weitere Informationen zur Notwendigkeit der E-Mail-Adresse finden Sie hier (S. 32).

b. Kann man dann überhaupt noch trainieren?

Ein Training an den Kraftgeräten ist nach Widerruf der Einwilligung zur Verarbeitung der personenbezogenen Daten nicht mehr möglich. Sofern nur andere Einwilligungen (z.B. Ranking oder Newsletter widerrufen werden, ist das Training weiterhin möglich.)

c. Kann ein EGYM Profil gelöscht werden? Was passiert dann mit den gespeicherten Daten?

Die Löschung des EGYM Profils kann jederzeit unter support@egym.de oder auf der Webseite www.egym.com beantragt werden. Leider ist ohne Profil kein Training an den EGYM Geräten möglich.
Die gelöschten Daten können im Nachhinein nicht wiederhergestellt werden.

d. Was passiert mit Studiodaten, wenn ein Mitglied sein Profil löschen möchte beziehungsweise seine Einwilligung widerruft?

In diesem Fall bleiben die Studiodaten erhalten, da diese vom Studio erhoben werden und daher nicht von dem Widerruf gegenüber EGYM betroffen sind. Die Möglichkeit der Betreuung über die Trainer App bleibt daher bestehen, bis das Mitglied seine Einwilligung gegenüber der Einrichtung widerruft oder das Vertragsverhältnis aufhebt.

3. Auskunftsanfragen

a. Wie bekommt das Mitglied heraus, welche Daten EGYM von ihm/ ihr gespeichert hat?

Den Datenschutzhinweisen auf www.egym.de kann genau entnommen werden, welche Daten automatisch gespeichert und welche Daten optional im Profil hinterlegt werden. Außerdem kann das Mitglied Auskunft im Studio selbst (bzgl. Studiodaten) bzw. In Bezug auf EGYM-Daten auch direkt bei EGYM verlangen.

Ein Mitglied kann sein Auskunftsrecht in Bezug auf EGYM unter datenschutz@egym.de ausüben. Wir stehen ihm oder ihr gerne bei Fragen zur Verfügung.

C. Schluss

Gibt es Fragen, die bisher nicht geklärt wurden? Zögern Sie nicht und kontaktieren Sie uns unter datenschutz@egym.de. Wir sind gerne bereit, Ihre offenen Fragen zu beantworten.

D. Checkliste

Nachfolgend finden Sie eine Checkliste zum Datenschutz in Fitnessstudios. Anhand dieser können Sie überprüfen, ob in Ihrem Studio ein angemessenes Datenschutzniveau erreicht wurde.

Datenschutz in Fitnessstudios	Erfüllt	Nicht erfüllt
Wesentliche Bestimmungen		
Soweit gemäß Art. 37 DSGVO iVm § 38 BDSG vorgeschrieben: Wurde ein Datenschutzbeauftragter bestellt?	☐	☐
Existiert für Ihre Mitarbeiter eine Datenschutz-Schulung?	☐	☐
Haben Sie ein Verzeichnis von Verarbeitungstätigkeiten angelegt, um einen Nachweis über die Einhaltung der DSGVO in Ihrem Studio führen zu können?	☐	☐
Allgemeiner Datenschutz		
Halte ich mich an den Grundsatz der Rechtmäßigkeit der DSGVO, indem ich vor jeder Verarbeitung von Daten eine Einwilligung einhole oder sicherstelle, dass ein Vertragsverhältnis bzw. eine andere Rechtsgrundlage dazu besteht?	☐	☐
Komme ich der Informationspflicht von Betroffenen in Form von Datenschutzhinweisen nach?	☐	☐
Haben Sie den Passus zum Einsatz von EGYM als Auftragsverarbeiter in Ihren Datenschutzhinweisen für Studio-Mitglieder (siehe hier) integriert?	☐	☐
Besteht die Möglichkeit, einem Mitglied einen vollständigen Abzug der verarbeiteten Daten zur Verfügung stellen, um das Recht auf Datenportabilität zu wahren oder Auskunft zu erteilen?	☐	☐
Habe ich mit allen Stellen, die von mir erhobene Daten verarbeiten, eine Vereinbarung zur Auftragsverarbeitung geschlossen und damit eine Rechtsgrundlage zur Verarbeitung der genutzten Daten geschaffen?	☐	☐
Verwende ich erhobene Daten ausschließlich zu dem dafür	☐	☐

vorhergesehenen Zweck oder nutze ich beispielsweise auch Kontaktdaten, um Werbung zu versenden ohne dafür eine konkrete Einwilligung eingeholt zu haben?		
Im Falle einer Datenpanne liegt ein Notfallkonzept vor, um die Informationspflichten rechtzeitig erfüllen zu können?	☐	☐
Werden personenbezogene Daten in Papierform (Trainingspläne, Mitarbeiterdaten, Kundendaten) bei Nichtgebrauch weggesperrt und somit vor unberechtigtem Zugang geschützt?	☐	☐
Speichere ich die Daten länger als für die Verarbeitung notwendig?	☐	☐
TOM		
Im Studio wird der Zugang zu Anlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte verwehrt? (Zugangskontrolle)	☐	☐
Gibt es Kontrollen durch z.B. kontinuierlich besetztem Empfang zur Überwachung der Ein- und Ausgänge? (Zutrittskontrolle)	☐	☐
Existieren elektronische Zutrittskontrollen für Mitarbeiter (z.B. für unbewachte Ein- und Ausgänge)? (Zutrittskontrolle)	☐	☐
Wird das Verwaltungssystem bzw. der Computer am Tresen bei Verlassen gesperrt? (Zugangskontrolle)	☐	☐
Gibt es ein verbindliches Verfahren zur Rücksetzung „vergessener“ Passwörter? (Zugangskontrolle)	☐	☐
Wird die unbefugte Eingabe von personenbezogenen Daten sowie die unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten verhindert? (Speicherkontrolle)	☐	☐
Kann in Ihrem Studio gewährleistet werden, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind? (Eingabekontrolle)	☐	☐
Wird das unbefugte Lesen, Kopieren, Verändern oder Löschen von Datenträgern verhindert? (Datenträgerkontrolle)	☐	☐
Kann in Ihrem Studio gewährleistet werden, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können? (Wiederherstellbarkeit)	☐	☐

Kann in Ihrem Studio gewährleistet werden, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden? (Zuverlässigkeit)	☐	☐
Kann in Ihrem Studio gewährleistet werden, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können? (Datenintegrität)	☐	☐
Kann in Ihrem Studio gewährleistet werden, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können? (Auftragskontrolle)	☐	☐
Kann in Ihrem Studio gewährleistet werden, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind? (Verfügbarkeitskontrolle)	☐	☐
Kann in Ihrem Studio gewährleistet werden, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können? (logische oder physische Trennbarkeit)	☐	☐
Sicherheit im WLAN		
Wird der öffentliche WLAN-HotSpot in Ihrem Studio nur mit VPN-Verbindung verwendet (Virtual Private Network)?	☐	☐
Setzen Sie Malware-Scanner auf allen (mobilen) Endgeräten ein?	☐	☐
Existieren Verschlüsselungen auf allen (mobilen) Endgeräten?	☐	☐
Werden Warnungen der (mobilen) Browser bei SSL-Problemen beachtet?	☐	☐
Herrscht eine Zwei-Faktor-Authentifizierung auch bei mobilen Endgeräten in Ihrem Studio?	☐	☐
Wird das Thema Datensparsamkeit bei Registrierung für WLAN-Zugänge berücksichtigt?	☐	☐

Bitte beachten Sie, dass diese Checkliste nur der Orientierung gilt und als Anregung für mögliche Datenschutzvorkehrungen im Studio gedacht ist. Wichtig ist, dass in Ihrer Einrichtung ein Datenschutzbeauftragter bestellt wird, eine Schulung zum Datenschutz für Ihre Mitarbeiter und ein Verzeichnis über Verarbeitungstätigkeiten geführt wird, um auf ein angemessenes Datenschutzniveau in Ihrer Einrichtung hinzuwirken. Alles Weitere dient als Überblick, welche Maßnahmen durchgeführt und dokumentiert werden können, um die Datensicherheit zu erhöhen.

Stand: Juni 2021

EGYM GmbH
Einsteinstraße 172

81677 München

Geschäftsführer:
Philipp Rösch-Schlanderer, Florian Sauter, Patrick Meininger
Gerichtsstand München | Amtsgericht München HRB 186394 | USt-IdNr. DE275313632