



Datenschutz im Fitnessstudio

Was bedeutet die neue EU-Datenschutz-Grundverordnung für Ihre Fitness- und Gesundheitseinrichtung?

Den 25. Mai 2018 sollten Sie sich merken. An diesem Tag wird die neue EU-Datenschutz-Grundverordnung (DS-GVO) in Deutschland in Kraft treten. Es gilt der Grundsatz: Wer personenbezogene Daten von EU-Bürgern verarbeitet, muss die DS-GVO einhalten. Jeder Verstoß gegen diese Verordnung wird bestraft, was zu einem echten Risiko für ein Fitnessstudio werden kann.

Als Betreiber eines Fitnessunternehmens verarbeiten Sie Daten z.B. in der Mitgliederverwaltung, im Marketing und Vertrieb, bei der Erstellung von Trainingsplänen sowie Checks. Für die Verarbeitung von Gesundheitsdaten, biometrischen Daten oder Daten von Kindern gelten strenge Vorgaben. Für Physiotherapeuten ist die Verarbeitung von gesundheitsbezogenen Daten überdies eine Kernaufgabe, daher muss zum Beispiel eine Physiotherapiepraxis auf alle Fälle einen Da-

tenschutzbeauftragten bestellen. Dasselbe gilt für Anbieter von Rehasport, also Rehasportvereine und Fitnessrichtungen, die Rehasport anbieten.

Datenverarbeitung nur mit Einwilligung

Eine Datenverarbeitung ist unter anderem nur rechtmäßig, wenn der Betroffene eingewilligt hat oder die Datenverarbeitung erforderlich ist, beispielsweise zur Durchführung eines Vertrages. Wie bereits nach derzeitigem deutschen

Recht, muss die Einwilligung freiwillig und ausdrücklich erteilt werden. Dies gilt insbesondere für den ehernen Grundsatz des „Verbots mit Erlaubnisvorbehalt“. Danach sind alle Arten des Umgangs mit persönlichen Informationen so lange verboten, bis der Gesetzgeber die Handlung explizit erlaubt oder der Betroffene ausdrücklich einwilligt.

Auch das Gebot der Zweckbindung. Danach dürfen personenbezogene Daten nur für „festgelegte, eindeutige und rechtmäßige Zwecke erhoben werden“.

Wenn ein Studio beispielsweise zum Zweck der Abwicklung eines Mitgliedsvertrages personenbezogene Daten von Kunden erhebt, ergibt sich daraus künftig nicht automatisch die Erlaubnis, diese Daten zu anderen Zwecken zu nutzen.

Verbraucherrechte werden gestärkt

Gewinner des neuen europäischen Rechts sind in vielen Punkten die Verbraucher; mehr als zuvor hängt von ihrer persönlichen Erlaubnis ab. Die Artikel 7 und 8 der DS-GVO regeln explizit die Voraussetzungen, die für eine Einwilligung zur Datenverarbeitung zu beachten sind. Diese muss wie bisher freiwillig und in Kenntnis der beabsichtigten Nutzung erfolgen. Der Verbraucher darf die Zustimmung jederzeit widerrufen. Sie unterfällt einem Kopplungsverbot, wonach „die Erbringung einer Dienstleistung nicht von der Einwilligung zur Verarbeitung von Daten abhängig gemacht“ werden darf, die für die Erfüllung des Vertrags nicht erforderlich ist. Gemeint sind hier beispielsweise die bekannten „Gewinnspiel-Kopplungen“, bei denen man durch die Teilnahme an einer Verlosung einer Verwendung der persönlichen Daten zu Marketingzwecken ebenfalls zustimmen muss.

Artikel 12 der neuen Verordnung legt strengere Informationspflichten fest. Unternehmen müssen den Nutzern die Rechtsgrundlage zur Verarbeitung der Daten ebenso mitteilen wie die Dauer der Speicherung, die Kriterien für die Dauer der Speicherung oder die Weitergabe an Auftragsdatenverarbeiter.

Diesen Informationspflichten stehen Regeln zu Auskunft, Widerruf sowie Löschung zur Seite. In der Praxis dürfte dies zu neuen, seitenlangen Belehrungsschriften führen, die von den Betroffenen abzunicken sind, ohne jemals gelesen worden zu sein. Überdies dürften solche Informationspflichten immer neuen Stoff für Massenabmahner bieten, die jeden Fehler mit teuren Anwaltschreibern bestrafen.

Hohe Bußgelder bei Datenschutzverstößen

Ab Mai können Datenschutzverstöße mit bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes eines Unternehmens sanktioniert werden. Laut Aussage der Landesdaten-

schutzbehörde Baden-Württemberg betragen aktuell (Stand: November 2017) die durchschnittlichen Bußgelder 1.600 Euro. Ab Mai kann man laut LDSB (Landesbeauftragter für den Datenschutz) hier bei kleinen Unternehmen eine Null, bei größeren Unternehmen sogar zwei Nullen hinzufügen.

Für einen Fitnessstudioinhaber oder einen Physiotherapeuten sind dann Bußgelder bei gemeldeten Datenschutzvergehen zwischen 10.000 und 20.000 Euro zu erwarten, zum Beispiel wenn kein Datenschutzbeauftragter bestellt ist, obwohl mit gesundheitsbezogenen Daten agiert wird. Damit dürfte der Datenschutz nun auch in der Fitnessbranche zum Thema werden. Denn ab dem Stichtag, dem 25.5.2018, werden Datenschutzverstöße zu einem echten Risiko für ein Studio, einen Verein oder eine Therapieeinrichtung.

Keine „gelbe Karte“ mehr

Bei Verstößen im Arbeitsschutz oder im Brandschutz bekommt man aktuell als Unternehmer immer die Möglichkeit des Nachbesserns. Beim Datenschutz ist es ab Mai so, dass jedes Vergehen automatisch zu einer Bestrafung führt. Und diese muss laut DS-GVO wirksam, verhältnismäßig und abschreckend sein.

Die Aufsichtsbehörden, sprich die Landesdatenschützer, haben ebenfalls Auflagen von der EU erhalten. Diese müssen allen gemeldeten Verstößen nachgehen und diese auch sanktionieren – ohne Ausnahmen. Daher rüsten die Aufsichtsbehörden aktuell massiv Personal auf, um diese Anforderungen zu erfüllen.

Sind Sie auf die neue Herausforderung vorbereitet?

- Verschaffen Sie sich einen umfassenden Überblick über alle Datenverarbeitungsvorgänge in Ihrer Einrichtung, die personenbezogene Daten betreffen.
- Erstellen Sie eine Dokumentation über diese Vorgänge.
- Prüfen Sie unter dem Gesichtspunkt der Datenminimierung, ob diese Datenverarbeitungen tatsächlich erforderlich sind.
- Erstellen Sie ein möglichst praktikables Konzept bezüglich der Umsetzung der Informationssicherheit in der eigenen Datenverarbeitung.

excio

TRAININGS GERÄTE

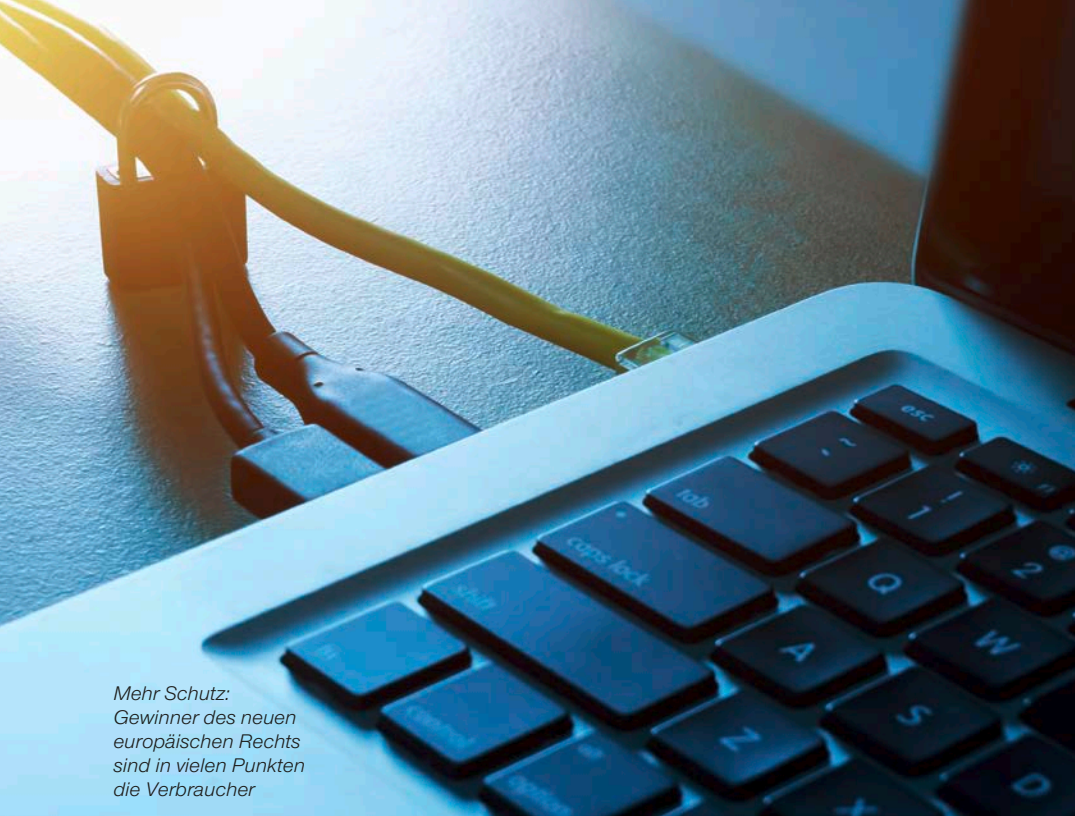
QUALITÄT MADE IN GERMANY!

hochwertig
innovativ
vielseitig



excio GmbH
Neustädter Str. 26
64747 Breuberg
Germany

Fon: 0 61 63 - 81 75 00
Fax: 0 61 63 - 81 75 27
Mail: info@excio.de
Web: www.excio.de



Mehr Schutz:
Gewinner des neuen
europäischen Rechts
sind in vielen Punkten
die Verbraucher

- Konzipieren Sie Richtlinien und neue Prozesse für die Einführung künftiger Verarbeitung von personenbezogenen Daten, die darauf ausgerichtet sind, Datenschutz-Folgeabschätzungen zu ermöglichen.
- Unterweisen Sie Ihre Mitarbeiter.

Was sind Ihre To-dos? Informationspflicht gegenüber Ihren Kunden

Die Information muss insbesondere Folgendes enthalten:

- Wer ist der Verantwortliche?
- Zu welchem Zweck sollen die Daten verarbeitet werden?
- Wer sind die Empfänger? Beispielsweise die Mitgliederverwaltung.
- Welche Kategorien von Daten sollen erhoben werden? Hier sollte beachtet werden, dass zum Beispiel auch eine E-Mail ein personenbezogenes Datum ist.
- Darüber hinaus muss immer angegeben werden, wenn Daten in Drittländer (außerhalb der EU) übermittelt werden.
- Die Aufbewahrungsfrist der Daten muss genannt werden.
- Welche Rechte hat der Betroffene? Er muss über die Möglichkeit, Auskunft, Sperrung und Löschung zu verlangen, informiert werden. Er kann der Datenverarbeitung widersprechen und seine einmal erteilte Einwilligung jederzeit widerrufen.
- Neu sind die Hinweispflichten auf das Recht zur Beschwerde bei einer Datenschutzbehörde.

Datenschutzerklärung

Eine Pflicht zur Datenschutzerklärung besteht nach der DS-GVO nicht. Allerdings besteht die Pflicht nach deutschem Recht, das neben der Verordnung anwendbar bleibt. Bestehende Datenschutzerklärungen sollten allerdings angepasst werden.

Öffentliche und interne Verfahrensverzeichnisse

Die meisten Unternehmen sind verpflichtet, umfangreiche Verzeichnisse zur Datenverarbeitung zu führen. Dies gilt für Unternehmen ab 250 Mitarbeitern uneingeschränkt sowie für Unternehmen mit spezieller Datenverarbeitung, beispielsweise Gesundheitsdaten, unabhängig von der Größe.

Interner oder externer Datenschutzbeauftragter

Ein Datenschutzbeauftragter muss insbesondere ernannt werden, wenn die Verarbeitungsvorgänge eine umfangreiche und regelmäßige systematische Überwachung der Betroffenen erforderlich machen oder beispielsweise Gesundheitsdaten umfangreich verarbeitet werden. Der Datenschutzbeauftragte kann ein Mitarbeiter oder ein externer Berater sein. Mit einem externen Berater muss dann ein Dienstleistungsvertrag geschlossen werden. Der Datenschutzbeauftragte muss ausreichend Fachwissen im Datenschutzrecht besitzen und seine Aufgaben schließen die Beratung des Unternehmens im Datenschutz, die Überwachung der Einhaltung des Datenschutzes und die Zusammenarbeit mit der Aufsichtsbehörde ein.

Bei Verstößen drohen auch hier Geldbußen bis zu zehn Millionen Euro oder zwei Prozent des Jahresumsatzes. Physiotherapiepraxen und Rehasportvereine benötigen auf jeden Fall einen Datenschutzbeauftragten, Fitnessstudios mit mehr als neun Beschäftigten ebenfalls. Bei internen Datenschutzbeauftragten müssen die Unternehmer dann den besonderen Kündigungsschutz des Datenschutzbeauftragten beachten; dieser ist vergleichbar mit dem Kündigungsschutz eines Betriebsrates.

Fazit

Was ändert sich durch die Datenschutz-Grundverordnung?

- Bei Verstößen drohen erhebliche Geldbußen.
- Die Betroffenen einer Datenverarbeitung müssen umfassend informiert werden.
- Die Rechte des Betroffenen werden ausgeweitet.
- Bei der Verarbeitung von Daten von Kindern (unter 16 Jahren) ist zusätzlich zu der Einwilligung des Kindes die Zustimmung der Eltern nötig.
- Bei der Verarbeitung von Gesundheitsdaten (zum Beispiel in der Physiotherapie oder im Rehasport) ist ein Datenschutzbeauftragter zu bestellen.
- Im klassischen Fitnessstudio muss ein Datenschutzbeauftragter spätestens dann bestellt werden, wenn mehr als neun Beschäftigte personenbezogene Daten verarbeiten.
- Verstößen wird seitens der Aufsichtsbehörden rigoros nachgegangen und sie müssen sanktioniert werden. Ausgesprochene Strafen werden dem Unternehmen „wehtun“.

Achim Barth



Achim Barth, Dipl.-Betriebswirt (FH), Fachwirt für Prävention und Gesundheitsförderung. Gründer von BARTH Sportmanagement (www.barth-sport.de). Als externer Datenschutzbeauftragter und Betrieblicher Gesundheitsmanager berät er Unternehmen in den Themenfeldern Arbeitsschutz und BGM. Für Fitnessstudioinhaber bietet er spezielle BGM/BGF-Seminare an, um die Studios fit für Firmenkooperationen zu machen.