



Zwei Jahre DSGVO

Bedeutung des Datenschutzes für die Fitnessbranche

Zum einen gab es zahlreiche Akteure, die mit der DSGVO-Einführung ein Geschäft witterten. Und mit „Angstmachen“ und „Panikverbreiten“ funktionierte dieses Neugeschäft ganz gut. Zum anderen mussten sich die Aufsichtsbehörden innerhalb Deutschlands erst einmal orientieren und einheitliche Vorgehensweisen erarbeiten. Hinzu kam, dass es zu auslegungsfähigen Artikeln in der DSGVO noch keinerlei Rechtsprechung gab. Urteile zur DSGVO kommen erst nach und nach. Und selbst Urteile schaffen nicht immer Klarheit, z. B. haben die Urteile zu Facebook-Fanseiten, das Zeugen-Jehovas-Urteil oder das Urteil zum Thema „Tracking-Tools“ auf Webseiten viele noch zusätzlich verwirrt. Nur die wenigsten wissen, was sie nun konkret tun müssen, um bußgeldsicher diese Dienste nutzen zu können. Durch

das Zeugen-Jehovas-Urteil ist dieser Begriff nun sehr weit gefasst – selbst Notizzettel fallen unter die DSGVO.

Ein weiterer Punkt: Die Aufsichtsbehörden wurden schlicht von den Beratungsanfragen der Betroffenen und Verantwortlichen überrannt, sodass Kontrolltätigkeiten schlicht auf ein Minimum heruntergefahren wurden. Und wenn kontrolliert wurde, waren es meist nur öffentliche Stellen wie Behörden und datengetriebene Branchen. Die Fitness- und Gesundheitsbranche stand bisher noch nicht im Fokus der Aufsichtsbehörde. Eine Aussage, ob sich dies ändert, wäre reine Spekulation.

Prüfung bei konkreten Beschwerden

Wenn sich allerdings Betroffene konkret bei der Datenschutzaufsicht beschwe-

ren, wird diese im Einzelfall auch tätig. So durfte ich 2019 einen Kunden übernehmen, dessen Videoüberwachung im Studio hätte deinstalliert werden sollen. Mit guten Argumenten konnten wir die gesamte Videoüberwachung, etwas modifiziert, auch weiterhin betreiben. Bei einem anderen Kunden war der Erlass der Aufsichtsbehörde bereits erteilt und wir konnten hier zumindest die komplette Deinstallation noch vermeiden.

„Videoüberwachung im Fitnessclub“ war also bereits ein Thema und wird vermutlich auch 2020 und 2021 ein Dauerbrenner sein. Wenn Sie also bereits eine Videoüberwachung durchführen oder planen: Sprechen Sie das Vorgehen eng mit Ihrem Datenschutzbeauftragten oder einem Datenschutzberater ab. Der Betrieb einer Videoüberwachung muss gut begründet und dokumentiert sein,

Foto: Thomas - stock.adobe.com

Die Welt ging damals nicht unter. Auch nach dem 25. Mai 2018 drehte sie sich weiter. Es kam weder zu einer Abmahnwelle, noch wurden die Betreiber von Fitnessclubs zur Zahlung von horrenden Bußgeldern „verdonnert“. Woran liegt es, dass es rund um das Thema „Datenschutz“ doch ganz anders kam als befürchtet?

zügige Beantwortung ihrer Fragen innerhalb von 30 Tagen.

Gesetzesanpassung 2019

Im November 2019 kam es zu einer wichtigen Gesetzesanpassung, die auch für die Fitnessbranche bedeutend ist. Im Rahmen des Zweiten Datenschutz-Anpassungs- und Umsetzungsgesetzes EU (2. DSAnpUG-EU) wurde durch den Bundestag beschlossen, dass Verantwortliche zukünftig erst ab 20 Mitarbeitern, die ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, einen Datenschutzbeauftragten zu benennen haben. Die bisherige Grenze von 10 Personen ist damit seit dem 26. November 2019 passé. In der Praxis heißt das, dass die meisten Fitnessclubs nicht verpflichtet sind, einen Datenschutzbeauftragten (egal ob intern oder extern) zu benennen. Aber: keine voreiligen Schlüsse! Als Clubbetreiber können Sie jetzt auf der einen Seite ju-

hörde bei Ihnen im Club steht, ist verschwindend gering. Wahrscheinlicher ist es, dass Sie Post von Ihrer Behörde bekommen. Das BayLDA (Bayrisches Landesamt für Datenschutzaufsicht) hat in der Vergangenheit schon KMU angeschrieben und gezielt nach den Datenschutzmaßnahmen gefragt.

Aufgrund der mit der DSGVO eingeführten Rechenschaftspflicht müssen Sie als Clubbetreiber liefern können. Das heißt, Sie müssen der Aufsichtsbehörde nachweisen können, dass Sie zum Beispiel die Grundsätze der Datenverarbeitung erfüllen oder geeignete Prozesse für Betroffenenanfragen oder den Umgang bei einer Datenschutzpanne eingeführt haben.

Ihre digitale Visitenkarte

Ihr Internetauftritt ist Ihre digitale Visitenkarte. Kunden, Wettbewerber und Aufsichtsbehörden können mit einfachen Mitteln feststellen, wie ernst Sie es

– eine Bilanz

sonst ist sie ganz schnell unrechtmäßig und muss womöglich außer Betrieb genommen werden.

Datenschutzrechte als „Waffe“

Die Verbraucher, also Ihre Mitglieder, haben ihre Betroffenenrechte, vor allem das Recht auf Auskunft und Löschung, als Druckmittel entdeckt, um ihre Forderungen durchzusetzen. Wenn Sie als Verantwortlicher einen guten Prozess für Betroffenenanfragen implementiert haben, sind Betroffenenanfragen zwar Arbeitsaufwand, aber ansonsten kein Risiko. Sollten Sie hier allerdings nicht gut aufgestellt sein, kommen Sie schnell in die Gefahr eines Rechtsverstoßes. Denn wenn Sie nicht innerhalb von 30 Tagen auf eine Auskunftsanfrage reagieren, kann es sehr unangenehm und im schlechtesten Fall auch teuer werden. Nehmen Sie die Anfragen Ihrer Mitglieder, vor allem Ihrer Ex-Mitglieder, ernst und sorgen Sie für eine vollständige und

behn, auf der anderen Seite müssen Sie sich aber bewusst sein, dass die Vorgaben der DSGVO trotzdem vollumfänglich gelten. Sie müssen sich das Wissen nun eben selbst erarbeiten und können nicht mehr auf die Beratung und Unterstützung eines fachkundigen Datenschutzbeauftragten zurückgreifen.

Lösungen speziell für Fitnessclubs und Gesundheitseinrichtungen, die keinen Datenschutzbeauftragten benötigen, gibt es. Wenn Sie als Clubbetreiber das Thema „Datenschutz und Datenschutzmanagement“ kostengünstig und ressourcenschonend umsetzen wollen, informieren Sie sich z. B. bei „Datenschutz365 Fitness&Gesundheit“. Informationen dazu finden Sie auf der Webseite oder durch Scannen des QR-Codes unter diesem Artikel.

Was erwartet eine Aufsichtsbehörde von Ihnen?

Die Wahrscheinlichkeit, dass unangemeldet die Datenschutz-Aufsichtsbe-

mit Datenschutz und IT-Sicherheit meinen. Dabei geht es nicht nur um Ihre Datenschutzerklärung und ein Cookie-Banner, sondern auch um grundlegende Einstellungen, damit Ihre Website nicht zur Spam-Schleuder wird. Zum Safer-Internet-Day 2019 wurden durch das BayLDA insgesamt 40 Websites von Unternehmen überprüft. Alle 40 Seiten wurden beanstandet.

Checkliste für Clubbetreiber

Technische und organisatorische Maßnahmen, die Sie als Clubbetreiber auf jeden Fall umsetzen sollen, können Sie mithilfe der Checkliste für Fitnessstudios & Vereine auf der Seite <https://qrco.de/checkfitness> überprüfen. Schauen Sie, welche Themen auch bei Ihnen im Studio umgesetzt werden müssen.

Die folgenden Maßnahmen sollten Sie idealerweise schon vor zwei Jahren umgesetzt haben – wenn nicht, dann sollten Sie diese schnellstmöglich angehen. Wenn Sie Unterstützung benötigen, ▶



Betreiber sollten überlegen, wie sie in ihrem Studio die DSGVO-Richtlinien am praktikabelsten umsetzen können

suchen Sie sich einen Datenschutzberater, der nicht nur die Branche kennt, sondern auch einen lösungsorientierten Beratungsansatz verfolgt. Mit einer falschen Beratung können Datenschutz und IT-Sicherheit sehr teuer werden und etablierte Prozesse werden plötzlich praxisfern und umständlich.

Was Sie im Datenschutz auf jeden Fall umsetzen sollten:

1. Sensibilisieren Sie Ihre Mitarbeiter bezüglich des Datenschutzes und der Vertraulichkeit und lassen Sie sich das unterschreiben.
2. Überprüfen Sie Ihre Website auf DSGVO-Konformität. Ihre digitale Visitenkarte muss den gesetzlichen Anforderungen entsprechen.
3. Dokumentieren Sie alle Verfahren im Club, in denen personenbezogene Daten verarbeitet werden. Prüfen Sie, ob es für die Verarbeitung eine Notwendigkeit gibt und wie lange Sie die Daten speichern wollen, wo die Daten gespeichert sind und wer darauf zugreifen kann.
4. Erstellen Sie eine Übersicht, an welche externen Stellen Sie personenbezogene Daten weitergeben. Danach prüfen Sie, ob es für die Weitergabe eine Rechtsgrundlage gibt. Bei Auftragsverarbeitern, z. B. einem Cloud-Dienstleister, müssen Sie sicherstellen, dass die notwendigen

Verträge vorliegen. Das gilt auch für gemeinsame Verantwortliche, z. B. Facebook, wenn Sie eine Facebook-Fanseite betreiben.

5. Halten Sie Ihr IT-System aktuell und sicher. Prüfen Sie die Sicherheitseinstellungen Ihrer Betriebssysteme, die Einstellungen von Ihren Browsern und Routern. Stellen Sie sicher, dass Sie sensible Gesundheitsdaten von Mitgliedern ausschließlich mit verschlüsselter E-Mail verschicken.
6. Implementieren Sie Prozesse für die Beantwortung von Betroffenenanfragen und den Umgang mit Datenschutzpannen.



Schritt-für-Schritt-Umsetzung

Wenn Sie heute nach Begriffen wie „DSGVO“ oder „Datenschutzumsetzung“ googeln, finden Sie Unmengen an Informationen, die sich teilweise auch noch widersprechen. Ohne fachkundiges Wissen werden Sie sich in der Fülle der Informationen nicht zurechtfinden. Im günstigsten Fall vergeuden Sie nur Ihre Zeit – im ungünstigsten Fall verlieren Sie viel Geld bei der Umsetzung von Maßnahmen, die völlig am Ziel vorbeischießen oder grundsätzlich überhaupt nicht notwendig sind. Arbeiten Sie sich Schritt für Schritt vor. Versuchen Sie nicht, alles auf einmal umzusetzen.

Fazit

Als Clubbetreiber sind Sie für die Einhaltung des Datenschutzes verantwortlich. Wenn Sie weniger als 20 Mitarbeiter beschäftigen, besteht keine Pflicht für Sie, einen Datenschutzbeauftragten zu benennen. Überlegen Sie sich, wie Sie die Anforderungen, die Ihnen die DSGVO stellt, praktikabel umsetzen können. Es gibt Unterstützungsmöglichkeiten, die Ihnen dabei helfen, vor allem wenn Ihnen die fachkundige Beratung eines Datenschutzbeauftragten fehlt. Gehen Sie bei der Umsetzung Schritt für Schritt vor und vermeiden Sie teuren Aktionismus. Ihr Bauchgefühl und Ihr gesunder Menschenverstand sind gute Ratgeber.

Abschließend ein Tipp von mir: Wenn Sie eine Datenverarbeitung durchführen, versetzen Sie sich in die Lage Ihres Mitglieds. Wollten Sie, dass mit Ihren Daten so umgegangen würde? Wenn Sie das innerlich verneinen, führen Sie die Verarbeitung nicht durch! Achim Barth



Achim Barth ist Geschäftsführer der Barth Datenschutz GmbH, zertifizierter Datenschutzbeauftragter (GDDcert EU, UDISzert) und fachkundiger IT-Sicherheitsbeauftragter (UDIS). Er berät lösungs- und kundenorientiert Verantwortliche im Gesundheitswesen und in der Fitnessbranche zu Datenschutzthemen.