1. Verkauf

**2018**

Ihre Firma

[Geben Sie den Firmennamen ein]

10.04.2018



1. Verkauf
2. Verfahren

Bezeichnung: Beratung von Interessenten, Verkauf und Abrechnung von Leistungen des Fitnessstudios

Fachabteilung: Vertrieb

Kontakt: [Name des Abteilungsleiters]

1. Zweckbestimmung

Akquisition von Kunden, Beratung von Interessenten, Abschluss und Abrechnung von Verträgen.

1. Details zur Datenverarbeitung
   1. Betroffene Personen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |
| --- | --- | --- |
|  | Personengruppe | Anmerkung |
| 01 | Interessenten | keine Kinder unter 16 Jahren |
| 02 | Kunden | keine Kinder unter 16 Jahren |
| 03 | Vertrauensperson | zur Information bei Notfällen |

* 1. Datenverwendung & Weitergabe  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

Verwendung intern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 01 | Rechnungswesen | Gesetz |
| 02 | Marketing | Einwilligung |
|  |  |  |

Weitergabe extern

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
| 03 | Steuerberatung, Rechtsanwälte | Abwägung 1) |
| 04 | Gerichte, Behörden | Gesetz |
| 05 | Externe Beratungsunternehmen | Einwilligung (soweit nicht anonymisiert) |
|  |  | Vertrag |

1. Interesse des Verarbeiters an steuerlicher, rechtlicher und sonstiger Beratung überwiegt das Geheimhaltungsinteresse des Betroffenen, wenn die Empfänger zur Verschwiegenheit gegenüber Dritten gesetzlich oder vertraglich verpflichtet sind.

Weitergabe Drittstaaten

|  |  |  |
| --- | --- | --- |
|  | Empfängerkategorie | Rechtsgrundlage |
|  |  |  |

* 1. Auftragsverarbeiter

Firma [genauer Firmenname]

Adresse [Postanschrift]

Kontaktperson [Name, E-Mail, TelNr.]

Vertragsnummer

(Mehrere Auftragsverarbeiter gesondert anführen)

1. Datenkategorien
   1. Kunden  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger – siehe 3.2. | Anmerkung |
| 01 | Name | Person | 5J | 01-05 |  |
| 02 | Geburtsdatum | Person | 5J | 01-05 |  |
| 03 | Geschlecht | Person | 5J | 02,04,05 |  |
| 04 | Sprache, Nationalität | Person | 5J | 02,04,05 |  |
| 05 | Postadresse | Person | 5J | 01-05 |  |
| 06 | Kontaktdaten inkl. TelNr | Person | 5J | 02,04,05 |  |
| 07 | Vertrauensperson | Person | 5J | 04 |  |
| 08 | Trainingsplan | Person | 5J | 02,04,05 |  |
| 09 | Preise, Konditionen | intern | 5J | 01-05 |  |
| 10 | Zahlungsart | Person | 5J | 01,03,04 |  |
| 11 | Bankverbindung, Kreditkarten | Person | 5J | 01,03,04 |  |
| 12 | KFZ Kennzeichen, PKW-Modell | Person | 5J | 04 |  |
| 13 | persönliche Bedürfnisse, Sonderwünsche | Person | 5J | 02,04,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 14 | Allergien & Unverträglichkeiten | Person | 5J | 02,04,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 15 | Anamnesedaten zu Fitness und Gesundheit | Person | 5J | 04,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 16 | Körpermaße | Person | 5J | 04,05 |  |
| 17 | Kunden-Feedback | Person | 5J | 02,04,05 |  |
|  |  |  |  |  |  |

* 1. Interessenten  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger – siehe 3.2. | Anmerkung |
| 01 | Name | Person | 1J | 02,04,05 |  |
| 02 | Geburtsdatum | Person | 1J | 02,04,05 |  |
| 03 | Geschlecht | Person | 1J | 02,04,05 |  |
| 04 | Sprache, Nationalität | Person | 1J | 02,04,05 |  |
| 05 | Postadresse | Person | 1J | 02,04,05 |  |
| 06 | Kontaktdaten inkl. TelNr | Person | 1J | 02,04,05 |  |
| 13 | persönliche Bedürfnisse, Sonderwünsche | Person | 3M | 02,05 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 14 | Allergien & Unverträglichkeiten | Person | 3M | 04 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 15 | Anamnesedaten zu Fitness und Gesundheit | Person | 3M | 04 | sensibel, Zugriffsbeschrän-kung sofort nach Kündigung |
| 16 | Körpermaße | Person | 3M | 04 |  |

* 1. Vertrauenspersonen 1)  
     (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Kategorie | Herkunft | Lösch-frist | Empfänger  siehe 3.2. | Anmerkung |
| 01 | Name | Person |  | 04 |  |
| 02 | Naheverhältnis | Person |  | 04 |  |
| 03 | Postadresse | Person |  | 04 |  |
| 04 | Kontaktdaten inkl. TelNr. | Person |  | 04 |  |

1. Die Vertrauensperson wird im Notfall (Unfall, Erkrankung) benachrichtig.
2. Technisch-organisatorische Maßnahmen (TOMs)
   1. Applikationen  
      (Unzutreffendes löschen, Fehlendes ergänzen.)

|  |  |  |  |
| --- | --- | --- | --- |
|  | Applikation | Auftrags-verarbeiter | Maßnahmen |
| 01 | Mitgliederverwaltung |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
| 02 | Abrechnungs-Software |  | siehe Richtlinie für die Vergabe von User-Berechtigungen |
| 03 | Web-Portal |  | Schutzmaßnahmen gegen Hacker laut IT-Handhandbuch vom [….] |
|  |  |  |  |

* 1. Datenschutz durch Technologiegestaltung („privacy by design“) ist gewährleistet durch:
* Restriktive Zugriffsberechtigungen
* Datenschutzfreundliche Applikationen (siehe User-Handbuch der Applikationen)
* Verschlüsselung und Pseudonymisierung von Kreditkartendaten
* Sonstiges: Zugriff auf sensible Daten nur für besonders geschulte Mitarbeiter, die die Daten für ihre Tätigkeit (zB Personal Trainer) benötigen.

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datenschutz durch datenminimierende Voreinstellungen („privacy by default“) ist gewährleistet durch:
* Grundeinstellungen in der Buchungssoftware
* Grundeinstellungen im Web-Portal
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität)

Elektronische Verarbeitungen

* Verschlüsselung sämtlicher Datenträger auf denen personenbezogene Daten gespeichert werden;
* Verschlüsselung bei Übermittlungen an Auftragsverarbeiter oder Behörden;
* Mehrstufige Systemsicherungen (B2D2T). Sämtliche Sicherungsdaten sind ebenfalls verschlüsselt und die Aufbewahrung der Archivbänder erfolgt georedundant,
* Hohe Sicherungsmechanismen im Bereich der Netzwerktechnologie. Physisch getrenntes WLAN für Kunden.
* Regelmäßige Überprüfung der Maßnahmen durch den Datenschutzverantwortlichen und den Auftragsverarbeiter.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

Analoge Verarbeitungen

* Papierakten (Handakten) werden lediglich nach Aktenzahl und/oder Namen des Betroffenen und/oder chronologisch nach dem Datum des Geschäftsfalles abgelegt. Es liegt daher kein Dateisystem im Sinne der DSGVO vor.
* Sensible Daten in Papierakten werden nur versperrt und in Räumen mit Zugangskontrollen aufbewahrt.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Methoden zur Datenlöschung

Elektronische Verarbeitungen

* Die eingesetzten Applikationen (allenfalls ergänzt durch spezielle Software-Tools wie zB Tealium) gewährleisten, dass sämtliche elektronisch erfasste Datenkategorien mit entsprechenden Tags versehen werden. Dadurch wird die automatische Löschung bzw. Anonymisierung einzelner Datenkategorien, nach Wegfall der Rechtsgrundlage zur Verarbeitung, ermöglicht.
* Im Falle einer Löschung nach Betroffenenbegehren wird diese protokolliert und in die operativen Backups nachgezogen.
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen)

Analoge Verarbeitungen

* Da kein strukturierter Zugriff auf Papierakten, zB in Form einer dezentralen Abfrage bestimmter personenbezogener Daten, möglich ist, ist eine langfristige Aufbewahrung zur Beweissicherung bis maximal 10 Jahre nach dem letzten Kontakt gerechtfertigt.
* Sonstige: Sensible Daten werden 3 Monate nach Ende der Vertragsbeziehung in ein gesichertes Archiv mit Zutrittskontrollen transferiert.

(Zutreffendes ankreuzen oder ergänzen.)

1. Profiling

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Entscheidungsautomatisierung

* Nein
* Ja, und zwar:

(Zutreffendes ankreuzen oder ergänzen.)

1. Betroffenenrechte
   1. Information Betroffener

* Standardformat: PDF
* Sonstiges

(Zutreffendes ankreuzen oder ergänzen.)

* 1. Art der Information des Betroffenen?
* E-Mail, wenn Anfrage per E-Mail, sonst per Post
* Sonstiges:

(Zutreffendes ankreuzen oder ergänzen.)