FiTNEZZplaza
bewegen is medicijn!

Privacy Policy Beleid

(Wet Algemene verordening gegevensbescherming)

Wet in een notendop:
https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/avg_in_een_notendop.pdf

Register van verwerkingsactiviteiten
FP houdt een register van verwerkingsactiviteiten bij van medewerkers en klanten. Voor medewerkers zijn alle mutaties terug te vinden in het personeelsdossier. Dit dossier is strikt vertrouwelijk tussen de directie van FP en de medewerker en wordt beheerd door de directie van FP. Voor klanten worden gegevens digitaal verwerkt. Hiervoor wordt het ledenadministratie software DEWI gebruikt. De gegevens zijn beveiligd opgeslagen op de beveiligde externe servers van DEWI. Zie verklaring DEWI. Gezondheidsgegevens, zoals krachttesten en trainingsschema's worden opgeslagen in de eGym software. Zie verklaring eGym.

Aandachtsgebieden van de wet AVG
FiTNEZZplaza hanteert het beleid rondom de aandachtsgebieden van de wet AVG. FP is heeft meer dan één aandachtsgebied (verwerking) waarop zij een grondslag hebben. Deze aandachtgebieden zijn opgenomen in het MVO beleid. Medewerkers en directie zijn hierdoor op de hoogte van de wetgeving AVG en zullen naar eer en geweten handelen conform deze wet.

De grondslag

1. Toestemming van de gebruiker

   Bij het onderteken van de overeenkomst gaat de persoon die zich inschrijft akkoord met het registreren van zijn 'gewone' persoonsgegevens en 'Bijzondere' persoonsgegevens. FP houdt geen registratie van 'strafrechtelijke' persoonsgegevens bij.

   'Gewone' persoonsgegevens,
   zijn gegevens zoals, naam, adres, woonplaats en telefoonnummer. Geboortedatum, bankrekeningnummer en e-mailadres. En worden gebruikt om met de persoon te kunnen communiceren als ook betalingen automatisch te kunnen verwerken.

   'Bijzondere' persoonsgegevens,
   zijn gegevens van de persoon welke gaan over de gezondheid van de persoon, de trainingsactiviteiten, de voortgang en het sportritme van de persoon. Deze gegevens zijn nodig om de persoon op een verantwoordelijke en professionele wijze te kunnen begeleiden. FP gebruikt hiervoor data-software DEWI en eGym.

   'Strafrechtelijke' persoonsgegevens,
   Zijn gegevens die FP niet registreert.

2. Vitale belangen
   Gegevens die FP nodig heeft rondom de gezondheid en het sportritme van de persoon worden opgeslagen in de genoemde data-software. Deze gegevens zijn nodig om de persoon voldoende te kunnen helpen bij in ieder geval verantwoord sporten. Bij calamiteiten worden waar nodig en indien de gegevens noodzakelijk zijn te hebben, ook naar extra gezondheid gegevens gevraagd. Het kan dan zijn dat we geen toestemming hebben gekregen van de persoon om deze gegevens te vragen/registeren, omdat de persoon in kwestie op dat moment niet in staat is toestemming te geven.

3. Wettelijke verplichting
   FP voldoet aan de wettelijke verplichting persoonsgegevens te mogen registreren. Zij voldoen aan vijf van zes AVG-grondslagen, terwijl minimaal één noodzakelijk is.

4. Overeenkomst
   Met de persoon wordt een overeenkomst afgesloten. De overeenkomsten worden digitaal verwerkt in de genoemde data-software.

5. Algemeen belang
   Hoewel FP geen direct algemeen belang vertegenwoordigd – indirect wel vanwege de verbetering van de algemene gezondheid van de bevolking – registreert FP gegevens om de gezondheid van de persoon en daarmee de bevolking te kunnen verbeteren.

6. Gerechtvaardigd belang
   a. Zonder de opgeslagen gegevens kan FP haar werk niet uitvoeren. Personeelsdossier en voor de begeleiding en administratieve verwerking van betalingen bij klanten.
   b. Proportionaliteit. Voor zover FP kan beoordelen verwerken wij enkel gegevens die nodig zijn om een goede begeleiding van de sportactiviteiten te kunnen waarborgen. Zoals:
      - Lichaamsmetingen
      - Gezondheidshistorie
      - Beperkingen
      - Sportritme
      - Voortgang sportdoelen

      Als ook gegevens die nodig zijn om betalingen te kunnen realiseren en of te kunnen communiceren met de persoon.

   c. Subsidiariteit. Behoudens de ‘gewone’ ‘persoonsgegevens, kan de persoon zelf weinig met de verzamelde ‘bijzondere’ persoonsgegevens. Het gaat om de analyse en de vakkundige en professionele interpretatie van de gegevens door de Personal Coach (PC), zodat de PC op basis van de analyse en interpretatie de persoon op de juiste wijze kan begeleiden.

   d. FP heeft een belang om analyses te maken van persoonsgebonden gegevens voor een goede begeleiding van de persoon.

Zorgvuldigheid

1. Functionaris gegevensbescherming
   Hoewel FP geen grote organisatie is, geen grote groepen volgt en dataverzameling bij FP geen kernactiviteit is, hebben we wel te maken de drie situaties op grond van artikel 37 van de AVG. Een Functionaris voor de gegevensbescherming (FG) is dan verplicht.
   - Publieke organisatie. FP is een locatie waar een grote groep individuen komen (jaarlijks 3 – 5% van de Oss gemeenschap.
   - FP volgt (niet op grote schaal en alleen voor individueel begeleiding) klanten (individuen)
   - FP houdt gezondheidsgegevens van klanten bij voor individuele begeleiding

   Functionaris voor de gegevensbescherming:

   Milton van Haren / 06 53 147 357 / milton@fitnezzplaza.nl

2. Privacy by design
   Bij het ontwerpen van producten en diensten is de functionaris gegevensbescherming van FP (zie punt 1) vanaf het begin betrokken om te voorkomen dat persoonsgegevens onvoldoende worden beschermd.

3. Impact assessment
   De organisatie FP verwerkt persoonlijke gegevens voor het goed kunnen begeleiden van klanten, maar er is geen sprake van een groot privacy risico. FP is daarom niet verplicht een DPIA (Data Protection Impact Assessment) uit te voeren.

Verplichtingen

1. Registreer met alle verwerkingen
   FP heeft minder dan 250 medewerkers en verwerkt persoonlijke gegevens niet incidenteel. FP is verplicht een register van verwerkingsactiviteiten op te stellen. FP heeft twee registers digitaal vormgegeven.
   - Ledenadministratie in DEWI (Zie bijlage 5a)
   - Gezondheidsregistratie in eGym (Zie bijlage 5b)

2. Gegevens beschermingsbeleid
   FP voldoet aan de verantwoordingsplicht door de opstelling van Beleid AVG document.

3. (Digitale) beveiliging
   FP heeft persoonsgegevens als volgt beschermd.

   Technische beveiligingsmaatregelen
   - Pand waar de persoonsgegevens zijn opgeslagen is op sluitingstijden fysiek gesloten met sloten voorzien van certificaat. Er wordt een sleutelregister bijgehouden.
   - Pand waar de persoonsgegevens zijn opgeslagen is op sluitingstijden fysiek beschermd door middel van een elektronisch alarminstallatie en is verbonden aan de meldkamer EUROPAC.
   - De software DEWI en eGym draaien op een computer (NAS). Deze computer is achter gesloten deur opgesteld (serverruimte) en is enkel met dubbele wachtwoorden toegankelijk. Een wachtwoord om toegang te krijgen tot de computer en een wachtwoord om toegang te krijgen tot de software. Wachtwoorden worden selectief afgegeven aan bevoegde medewerkers. Hiervan wordt een wachtwoordregister bijgehouden.
   - Medewerkers zijn geïnstrueerd dat beeldschermen op Windows-L (Lock) gezet worden wanneer een beeldscherm onbeheerd wordt achter gelaten.
   - Data wordt tevens opgeslagen bij de organisatie eGym. EGym heeft een verklaring opgesteld dat de dataopslag volledig voldoet aan de wet AVG. Zie verklaring eGym AVG.
   - Individuele correspondentie met klanten wordt opgeslagen op de NAS en gesynchroniseerd met one-drive (cloud). One-Drive (office 365) voldoet aan de eisen wet AVG.
   - De nog fysieke, niet gedigitaliseerde, contracten zijn op alfabetische volgorde gedocumenteerd in ordners. Deze ordners staan in een afgesloten kast. (Deze documenten wordt in de tijd gedigitaliseerd en verdwijnen uit de registratie)

   Organisatorische beveiligingsmaatregelen
   - Het beleid AVG is opgenomen in het beleid MVO (Maatschappelijk Verantwoord Ondernemen). (Nieuwe) medewerkers worden geacht en aangespoord het MVO beleid te kennen, zodat hiermee de beveiligingsbewustzijn bij bestaande en nieuwe medewerkers geborgd is.
   - FP heeft een functionaris voor de gegevensbescherming. Zie punt 1 zorgvuldigheid
   - Eens per jaar worden wachtwoorden, codes en sleutels update gemaakt, waar nodig gewijzigd.
   - In de tijd wordt de procedure AVG verscherpt en uitgebreid met de registratie van bevoegdheden en verantwoordelijkheden.

   Hoe lang bewaren wij persoonsgegevens ná beëindigen lidmaatschap:

   - FP is verplicht de financiële administratie tot 7 jaar na einde lidmaatschap te bewaren. Daarna zullen wij het lidaccount verwijderen uit onze ledenadministratie DEWI.
   - Na beëindiging lidmaatschap verwijderen wij binnen 6 maanden het eGym account met de bijzondere persoonsgegevens in onze trainersapp van eGym. Gegevens blijven dan wel bij eGym bewaard, maar zijn dan niet meer bij FP inzichtelijk.

Rechten van de betrokkenen

1. Recht om in te zien
   Leden van FiTNEZZplaza kunnen ten alle tijde hun gegevens inzien in onze apps. (DEWI voor de naw en bankgegevens bij “profiel” en betreffende het abonnement bij “abonnement”. Test en trainingsgegevens kunnen worden ingezien in de eGym app en nog uitgebreider op de eGym website. Specifieke notities kunnen worden ingezien bij de balie of bij de Personal Coach.

2. Recht om te wijzigen
   Leden kunnen hun naw en bankgegevens wijzigen middels een mutatieformulier, indien de juiste gegevens zijn veranderd. Wijzigen van test, trainingsgegevens en specifieke notities kunnen worden aangevraagd middels een verzoek via een mail naar: corina@fitnezzplaza.nl

3. Recht om vergeten te worden
   Indien een lid zijn lidmaatschap heeft beëindigd is het mogelijk om de gegevens van het lid geheel of gedeeltelijk uit onze ledenadministratie DEWI en trainingsapp eGym te verwijderen. U kunt dit aanvragen via een mail naar: corina@fitnezzplaza.nl

4. Recht om gegevens over te dragen

   Het lid kan zelf zijn gegevens overdragen door deze van de app te kopiëren. Overdracht van specifieke notities kunnen worden aangevraagd via: corina@fitnezzplaza.nl

5. Recht op informatie

   Het lid kan ten alle tijden middels persoonlijk contact bij zijn of haar Personal Coach en bij de baliemedewerker informatie opvragen over zijn of haar gegevens die bij FiTNEZZplaza bekend zijn. Hierbij moet rekening gehouden worden dat op het moment van informatie verstrekken, de medewerker van FiTNEZZplaza inzage krijgt in de gevraagde gegevens. Het lid geeft hierbij toestemming hiervoor. De medewerker van FiTNEZZplaza is ten alle tijde bevoegd om een legitimatie te vragen aan de informatievrager, alvorens de informatie te verstrekken. Telefonisch verstrekken wij geen gegevens.

   Het lid mag ten alle tijde algemene informatie vragen over het AVG-beleid van FiTNEZZplaza. In deze gevallen wordt een kopie van dit document aan het lid verstrekt.

   De aanwezigheid van het AVG-beleid is op 25 mei 2018 per nieuwsbrief medegedeeld aan de leden van FiTNEZZplaza. Vanaf deze datum worden nieuwe leden via het inschrijfformulier op de hoogte gebracht van de aanwezigheid van het AVG-beleid.

Meldplicht datalekken

Op het moment dat onze verwerkingsverantwoordelijke (directie van FP) zich bewust wordt van een datalek wordt er binnen 72 uur na ontdekking een melding gedaan aan de Autoriteit Persoonsgegevens. Door middel van melden op het meldingsloket https://datalekken.autoriteitpersoonsgegevens.nl/actionpage?0

Wanneer het onwaarschijnlijk is dat de inbreuk een hoog risico inhoudt voor de rechten en vrijheden van natuurlijke personen , dan kan de directie besluiten geen melding te doen (artikel 33 AVG).

Betrokkene wordt geïnformeerd wanneer het waarschijnlijk is dat de inbreuk resulteert in een hoog risico voor zijn of haar rechten en vrijheden. Dat stelt hem in staat eventuele voorzorgsmaatregelen te treffen. Zowel de aard van de inbreuk als aanbevelingen over hoe hij of zij mogelijke negatieve gevolgen kan beperken, worden hem of haar gemeld. (artikel 34 AVG).

De directie kan besluiten om een melding achterwege gelaten, dien er achteraf maatregelen zijn genomen door de directie van FP om te zorgen dat de hoge risico's voor de rechten en vrijheden van betrokkene zich waarschijnlijk niet meer voor zullen doen. (artikel 34 AVG).

De directie zal alle inbreuken documenteren, met inbegrip van de feiten omtrent de inbreuk, de gevolgen en de genomen corrigerende maatregelen (artikel 33, vijfde lid AVG).

Tot slot. De directie zal, n.a.v. een inbreuk per geval besluiten de data lek te melden aan toeleveranciers DEWI, eGym, Matrix en systeembeheerder De Witjes, zodat zij eventueel maatregelen kunnen nemen, waar FP geen invloed op heeft.

Indien de datalek voortkomt uit een analoge situatie, denk aan diefstal, dan wordt, indien nodig, ook de politie door de directie op de hoogte gebracht.