

Overwegende dat

- Verwerker levert een op web- en mobiele applicatie gebaseerde software oplossing die een breed scala aan functionaliteiten biedt op het gebied van onder andere activiteiten- en voortgangsregistratie, voeding, coaching, boekingen, ledenbeheer en facturering (De Service). In deze rol zal Verwerker i) gegevens verwerken, ii) gegevens opslaan en iii) gegevens analyseren;
- Verwerkeringsverantwoordelijke kan aanvullende oplossingen bieden voor onder andere activiteiten- en voortgangsregistratie, voeding, coaching, boekingen, lidmaatschappen, facturering en andere informatie die ten behoeve van Verwerkingsverantwoordelijke kan worden gekoppeld aan De Service van Verwerker;
- Verwerker en Verwerkingsverantwoordelijke hebben eerder een licentieovereenkomst voor De Service gesloten, waarvan deze Verwerkersovereenkomst deel uitmaakt;
- Wat de verwerking van persoonsgegevens betreft, kan Verwerker volgens het recht van de Europese Unie worden aangemerkt als een Verwerker in de zin van artikel 4, lid 8, van de Algemene Verordening Gegevensbescherming (AVG) en kan Verwerkingsverantwoordelijke worden aangemerkt als een Verwerkingsverantwoordelijke in de zin van artikel 4, lid 7, van de AVG;
- Partijen wensen - mede ter uitvoering van het bepaalde in artikel 28, lid 3, van de AVG - en ten behoeve van de Verwerkingsverantwoordelijke in deze Verwerkersovereenkomst een aantal voorwaarden vast te leggen die van toepassing zijn op hun relatie in het kader van voornoemde taken.

1. Definities

1.1 In deze Verwerkersovereenkomst hebben de volgende begrippen de hieronder omschreven betekenis en worden verwante termen overeenkomstig geïnterpreteerd:

1.1.1 **"Vertrouwelijke informatie"**: alle informatie van vertrouwelijke, bedrijfseigen of geheime aard die van toepassing is of kan zijn op of op enige wijze verband houdt met: i) de huidige of toekomstige activiteiten van Verwerker; of (ii) het onderzoek naar en de ontwikkeling van bedrijfseigen informatie en andere informatie waarop eigendomsrechten berusten van Verwerker, waaronder onder andere zonder enige beperking, de identiteit van een klant, leverancier of klant van Verwerker, handelsgeheimen, processen, formules, gebruikersdata, know-how, verbeteringen, uitvindingen, patenten, auteursrechten, technieken, marketingplannen, beleid, procedures, prijzen, technische software, met inbegrip van bron- en objectcode, besturingssystemen, bridgeware, firmware, middleware en hulpprogramma's, en strategieën, kosten, winst- en marge-informatie, financiën en financiële projecties en huidige of toekomstige businessplannen en -modellen;

1.1.2 **"De Service"**: Verwerker heeft een flexibele white-label-technologieoplossing ontwikkeld voor op web en mobiele apps gebaseerde lifestyle, fitness en wellness platformen die een breed scala aan

functionaliteiten biedt op het gebied van onder andere activiteiten- en voortgangsregistratie, voeding, mentale vitaliteit, coaching, boeking, ledenbeheer, en facturering;

1.1.3. **"Bijlage"**: elke toevoeging aan deze Verwerkersovereenkomst die daarvan een integraal onderdeel uitmaakt;

1.1.4. **"Overeenkomst"**: de eerder tussen Partijen gesloten licentieovereenkomst;

1.1.5. **"Persoonsgegevens"**: alle informatie betreffende een geïdentificeerde of identificeerbare natuurlijke persoon als bedoeld in sectie 4, punt 2, van de AVG;

1.1.6. **"Verwerking"**: betekent, alsmede vervoegingen van dit werkwoord: de verwerking van Persoonsgegevens als bedoeld in artikel 4 lid 2 AVG;

1.1.7. **"Verwerkersovereenkomst"** verwijst naar deze overeenkomst;

1.1.8. **"Subverwerkers"**: de door Verwerker ingeschakelde onderaannemer die namens de Verwerkingsverantwoordelijke in het kader van deze Verwerkersovereenkomst persoonsgegevens verwerkt, zoals bedoeld in artikel 28 lid 4 AVG.

1.2 De bepalingen van de Overeenkomst zijn van toepassing op deze Verwerkersovereenkomst. Indien bepalingen met betrekking tot de Verwerking van Persoonsgegevens in de Overeenkomst in strijd zijn met de bepalingen in deze Verwerkersovereenkomst, zijn de bepalingen van deze Verwerkersovereenkomst van toepassing.

2. Doel van de verwerking van persoonsgegevens

2.1 Partijen wensen deze Verwerkersovereenkomst aan te gaan om de voorwaarden van de Verwerking van Persoonsgegevens in het kader van de Overeenkomst vast te leggen. Een overzicht van de soorten Persoonsgegevens, de categorieën van betrokkenen en de doeleinden van Verwerking is opgenomen in Bijlage I.

2.2 Verwerker zal persoonsgegevens uitsluitend verwerken ten behoeve van de activiteiten waarnaar in deze Verwerkersovereenkomst wordt verwezen. Verwerker garandeert de Persoonsgegevens die hij in het kader van deze Verwerkersovereenkomst verwerkt niet zonder uitdrukkelijke schriftelijke toestemming van de Verwerkingsverantwoordelijke voor eigen of externe doeleinden te gebruiken, tenzij i) de doeleinden uitdrukkelijk anders zijn vermeld in deze Verwerkersovereenkomst of eerder ondertekende overeenkomsten ii) Verwerker daartoe wettelijk verplicht is. In dat geval zal Verwerker de Verwerkingsverantwoordelijke onmiddellijk op de hoogte stellen van deze wettelijke verplichting alvorens tot Verwerking over te gaan, tenzij wettelijk een dergelijke kennisgeving aan de Verwerkingsverantwoordelijke verboden wordt.

3. Technische en organisatorische bepalingen

3.1 Verwerker zal, rekening houdend met de aard van de Verwerking en voor zover dit redelijkerwijs mogelijk is, de Verwerkingsverantwoordelijke assisteren bij de nakoming van de

verplichtingen op grond van de AVG en bij het nemen van passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen. Deze maatregelen worden zodanig ontworpen dat, rekening houdend met de beste praktijken en de kosten van uitvoering, een passend beveiligingsniveau wordt vastgesteld in het licht van de aard van de te beschermen gegevens en de risico's die de Verwerking van Persoonsgegevens met zich meebrengt. Verwerker zal in ieder geval commercieel redelijke inspanningen leveren om Persoonsgegevens te beschermen tegen onbedoeld of onwettige vernietiging, onopzettelijk of opzettelijk verlies, vervalsing, niet-geautoriseerde distributie of toegang, of enige andere vorm van onwettige Verwerking.

3.2 Verwerker zal een document ter beschikking stellen waarin de door Verwerker te nemen technische en organisatorische maatregelen worden beschreven. Dit document zal als bijlage worden toegevoegd aan deze Verwerkersovereenkomst.

4. Vertrouwelijkheid

4.1 Verwerker zal de medewerkers die betrokken zijn bij de uitvoering van deze Verwerkersovereenkomst verplichten tot ondertekening van een geheimhoudingsverklaring, waarin in ieder geval is opgenomen dat deze medewerkers de Persoonsgegevens strikt vertrouwelijk dienen te behandelen.

5. Verwerking van persoonsgegevens buiten Europa

5.1 Het is Verwerker toegestaan om Persoonsgegevens buiten de Europese Unie door te geven met inachtneming van wettelijke verplichtingen die van toepassing zijn.

6. Subverwerkers

6.1 Verwerker is gerechtigd de uitvoering van de Verwerking in opdracht van Verwerkingsverantwoordelijke geheel of gedeeltelijk uit te besteden aan de in Bijlage III omschreven Subverwerkers. Indien Verwerker Subverwerkers wil inschakelen, zal Verwerker de Verwerkingsverantwoordelijke op de hoogte stellen van voorgenomen wijzigingen met betrekking tot het toevoegen of vervangen van Subverwerkers. Verwerkingsverantwoordelijke kan binnen 5 werkdagen na ontvangst van de schriftelijke bevestiging van de voorgenomen wijziging van Subverwerker door Verwerker, bezwaar maken tegen dergelijke wijzigingen. Een dergelijk bezwaar dient op redelijke gronden te berusten.

6.2 Verwerker streeft ernaar elke Subverwerker te verplichten tot naleving van de vertrouwelijkheidsverplichtingen, kennisgevingsverplichtingen en beveiligingsmaatregelen met betrekking tot de Verwerking van Persoonsgegevens, welke verplichtingen en maatregelen ten minste moeten voldoen aan de bepalingen van deze Verwerkersovereenkomst.

7. Aansprakelijkheid

7.1 Ten aanzien van de aansprakelijkheids- en vrijwaringsverplichtingen van Verwerker op grond van deze Verwerkersovereenkomst is het in de Overeenkomst bepaalde, of hetgeen middels verwijzing in de Overeenkomst is opgenomen, met betrekking tot de beperking van aansprakelijkheid van toepassing.

7.2 Partijen zijn jegens elkaar aansprakelijk voor alle directe schade die voortvloeit uit of verband houdt met het uitvoeren van of het niet uitvoeren van deze Verwerkersovereenkomst. Echter, elke aansprakelijkheid die voortvloeit uit deze Verwerkersovereenkomst, hetzij op basis van een actie of claim in nalatigheid, onrechtmatige daad of anderszins, voor alle gebeurtenissen, handelingen of omissies in het kader van deze overeenkomst, zal in totaal niet meer bedragen dan de vergoedingen betaald of te betalen in het kader van de Overeenkomst over een periode van maximaal zes maanden.

8. Schending van persoonsgegevens

8.1 In het geval dat Verwerker zich bewust wordt van een incident dat een wezenlijke impact kan hebben op de bescherming van Persoonsgegevens, zal Verwerker i) Verwerkingsverantwoordelijke daarvan op de hoogte stellen binnen 24 uur nadat Verwerker zich bewust werd van het incident en ii) alle redelijke maatregelen nemen om de impact van het incident te voorkomen of te beperken en toekomstige incidenten te voorkomen.

8.2 Verwerker zal, voor zover redelijk, medewerking verlenen gevraagd door Verwerkingsverantwoordelijke om ervoor te zorgen dat de Verwerkingsverantwoordelijke zijn wettelijke verplichtingen in verband met een dergelijk incident nakomt.

8.3 Verwerker assisteert de Verwerkingsverantwoordelijke, voor zover redelijk, bij de meldingsplicht van de Verwerkingsverantwoordelijke met betrekking tot de Persoonsgegevens aan de gegevensbeschermingsautoriteit en/of de betrokkene, als bedoeld in artikel 33, lid 3, en artikel 34, lid 1, van de AVG. Verwerker is op grond van deze Verwerkersovereenkomst nimmer gehouden een inbreuk in verband met persoonsgegevens te melden bij de gegevensbeschermingsautoriteit en/of de betrokkene.

8.4 Verwerker is niet verantwoordelijk en/of aansprakelijk voor de (tijdige en juiste) meldingsplicht aan de betrokken toezichthouder en/of betrokkene als bedoeld in de artikelen 33 en 34 van de AVG.

9. Samenwerking

9.1 Verwerker zal, voor zover redelijkerwijs mogelijk, medewerking verlenen aan de Verwerkingsverantwoordelijke bij de naleving van zijn verplichting op grond van de AVG om te

antwoorden op verzoeken die betrekking hebben op uitoefening van de rechten van betrokkenen, met name het recht van inzage (artikel 15 AVG), rectificatie (artikel 16 AVG), gegevenswissing (artikel 17 AVG), beperking van verwerking (artikel 18 AVG), overdraagbaarheid van gegevens (artikel 20 AVG) en het recht van bezwaar (artikelen 21 en 22 AVG). Verwerker stuurt een klacht of verzoek van een betrokkene met betrekking tot de verwerking van persoonsgegevens door aan de Verwerkingsverantwoordelijke indien redelijkerwijs mogelijk na ontvangst daarvan, aangezien de Verwerkingsverantwoordelijke (mede) verantwoordelijk kan zijn voor de behandeling van het verzoek. Verwerker is gerechtigd alle kosten die verband houden met de samenwerking met de Verwerkingsverantwoordelijke met betrekking tot de voorwaarden van deze Verwerkersovereenkomst in rekening te brengen. Verwerkingsverantwoordelijke is als enige verantwoordelijk voor de toepasselijke kosten onder dit artikel, met inbegrip van - maar niet beperkt tot - aanvullend werk met een uurtarief van 69,- per uur te betalen aan Verwerker voor tijd besteed aan verzoeken onder dit artikel.

9.2 Verwerker zal, voor zover redelijkerwijs mogelijk, medewerking verlenen aan Verwerkingsverantwoordelijke om te voldoen aan zijn verplichting op grond van de AVG om een gegevensbeschermingseffectbeoordeling uit te voeren (art. 35 en 36 AVG). Verwerkingsverantwoordelijke is als enige verantwoordelijk voor de toepasselijke kosten onder dit artikel, met inbegrip van - maar niet beperkt tot - aanvullend werk met een uurtarief van 69,- per uur te betalen aan Verwerker voor tijd besteed aan verzoeken onder dit artikel.

9.3 Verwerker zal aan Verwerkingsverantwoordelijke alle informatie verstrekken die redelijkerwijs nodig is om aan te tonen dat Verwerker aan zijn verplichtingen op grond van de AVG voldoet. Voorts zal Verwerker - op verzoek van Verwerkingsverantwoordelijke - audits mogelijk maken en daaraan bijdragen, waaronder inspecties door een Verwerkingsverantwoordelijke gemachtigde auditor. Indien Verwerker van mening is dat een opdracht met betrekking tot de bepalingen van dit artikel in strijd zijn met de AVG of andere toepasselijke wetgeving inzake gegevensbescherming, stelt Verwerker Verwerkingsverantwoordelijke daarvan onmiddellijk in kennis. Verwerkingsverantwoordelijke is als enige verantwoordelijk voor de toepasselijke kosten onder dit artikel, met inbegrip van maar niet beperkt tot een uurtarief van 150,- per uur voor Verwerker voor tijd besteed aan voorbereiding en assistentie tijdens inspectie of de gevraagde audit.

10. Beëindiging en overige bepalingen

10.1 Ten aanzien van de beëindiging op grond van deze Verwerkersovereenkomst zijn de specifieke bepalingen van de Overeenkomst van toepassing. Onverminderd de specifieke bepalingen van de Overeenkomst zal Verwerker bij het eerste verzoek van Verwerkingsverantwoordelijke alle door Verwerkingsverantwoordelijke beheerde Persoonsgegevens verwijderen of retourneren, en alle

bestaande kopieën verwijderen, tenzij Verwerker wettelijk verplicht is sommige of alle daarvan op te slaan.

10.2 Verwerker is, binnen de grenzen van het toepasselijke recht, vrij in de keuze van de bewaartermijn die geldt voor verwerking van persoonsgegevens door Verwerker.

10.3 De in deze Verwerkersovereenkomst opgenomen verplichtingen die naar hun aard bedoeld zijn om ook na beëindiging voort te duren, blijven ook na beëindiging van deze Verwerkersovereenkomst van kracht.

10.4 De keuze van het recht en de bevoegde rechter geschiedt met inachtneming van de toepasselijke bepalingen van de Overeenkomst.

Alle getoonde bedragen zijn in de valuta van de Overeenkomst.

Naam: Hugo Braam

Bedrijf: DIGIFIT B.V.

Titel: CEO & Mede-oprichter

Handtekening: *Hugo Braam*

BIJLAGE I - OVERZICHT PERSOONSgegevens

SOORTEN PERSOONSgegevens

- Basis persoonsgegevens (bijv. naam)
- Contactgegevens
- Bankgegevens - beperkt
- Productinformatie (bijv. lidmaatschapsinformatie)
- Account status informatie
- Persoonlijke accountinstellingen (bijv. taalvoorkeur)
- Profielinformatie (bijv. profielfoto's)
- Inloggegevens (bijv. wachtwoord)
- Trainingsinformatie
- Voortgangsinformatie - anders dan "trainingsinformatie" (bijv. gewicht)
- Coachingsinformatie (bijv. doel van cliënt)
- Communicatie-informatie (bijv. community posts)
- Aankoopinformatie (bijv. aankopen van lidmaatschappen)
- Bezoek- en toegangsinformatie

- Reserveringsinformatie (bijv. geplande lessen)
- Vragenlijst informatie
- Marketing informatie (bijv. nieuwsbrief)
- Informatie niet gegenereerd met behulp van de applicatie (bijv. geüploade bestanden)

CATEGORIEËN BETROKKENEN

- Personeel, met inbegrip van vrijwilligers, tijdelijke en uitzendkrachten; en
- Klanten en patiënten, inclusief maar niet beperkt tot sporters en medewerkers.

DOELEINDEN VAN VERWERKING

Verwerker, met inbegrip van zijn werknemers, agenten, onderaannemers en vertegenwoordigers zal Persoonsgegevens alleen gebruiken voor het uitvoeren van zijn diensten. Specifieke doeleinden zijn:

- Verwerkingsverantwoordelijke in staat stellen zijn diensten aan te bieden, zoals coaching, personal training, educatie, bedrijfsgezondheids en wellness services;
- Verbetering van kwaliteit van De Service;
- Passende maatregelen uitvoeren om de veiligheid en vertrouwelijkheid van persoonsgegevens te waarborgen;
- Persoonsgegevens beschermen tegen bekende of te verwachten bedreigingen die een gevaar vormen voor de veiligheid of integriteit van dergelijke informatie; en
- Beschermen tegen ongeautoriseerde toegang tot of gebruik van Persoonsgegevens dat kan resulteren in schade of ongemak voor een individu.

BIJLAGE II - SPECIFICATIE VAN DE BEVEILIGINGSMATREGELEN

Verwerker streeft ernaar klantgegevens en De Service te beschermen door het implementeren van beveiligingsmaatregelen op basis van industriestandaarden. Deze bijlage geeft een overzicht van de door Verwerker genomen maatregelen en na te leven normen.

NALEVING VAN REGELGEVING

Verwerker voldoet aan de volgende algemene eisen:

- Zorgdragen dat er een beveiligingsteam is dat zich richt op het beheren en onderhouden van het informatiebeveiligingsprogramma van Verwerker;
- Het bijhouden van een organisatieschema met een overzicht van rollen en verantwoordelijkheden van alle personen die beveiligingsfuncties uitvoeren; en
- Het verkrijgen en onderhouden van een uitgebreid industriestandaard informatiebeveiligingsprogramma.

OPERATIONELE VEILIGHEID

Verwerker documenteert en onderhoudt een uitgebreid informatiebeveiligingsbeleid dat wordt gecommuniceerd aan al het personeel en alle andere partijen die toegestaan zijn toegang te hebben tot Persoonsgegevens. Daarnaast zal Verwerker:

- Zorgdragen dat personeel, en alle relevante andere partijen, Verwerkers beveiligingsbeleid en beveiligingspraktijk erkent en naleeft wanneer zij toegang krijgen tot en omgaan met Persoonsgegevens; en
- Het beveiligingsbeleid formeel toetst (en actualiseren indien van toepassing), op een in ieder geval jaarlijkse basis.

VEILIGHEIDSBEWUSTWORDINGSTRAINING

Verwerker onderhoudt een beveiligingsbewustwordingsprogramma voor al het personeel dat ten minste i) de aard van Persoonsgegevens zal bevatten, ii) de juiste methoden voor het verwerken, beschermen, overdragen en opslaan van Persoonsgegevens, iii) procedures voor het melden van beveiligingsincidenten en iv) de gevolgen van het niet naleven van het Informatiebeveiligingsbeleid.

Verwerker zorgt ervoor dat elk personeelslid de beveiligingsbewustmakingstraining minstens jaarlijks en op het moment van tewerkstelling volgt.

Als er fouten of onvolkomenheden in de beveiligingsbewustmakingstraining worden gedetecteerd, zal Verwerker de beveiligingsbewustmakingstraining tijdig bijwerken.

PERSONEELSAFDELING

Verwerker is verantwoordelijk voor het uitvoeren van achtergrondcontroles bij personeel.

Achtergrondcontroles kunnen bestaan uit: verificatie van arbeidsverleden, verificatie van genoten opleiding, referentiescreening en screening van sociale media.

VERANDERMANAGEMENT

Verwerker heeft tot doel een door de industrie aanvaard veranderingscontroleproces te gebruiken voor alle infrastructuren en middelen die ondersteunen bij het verwerken van Persoonsgegevens. Het proces voor wijzigingsbeheer omvat activiteitenlogs en processen voor herstel naar een eerdere staat.

OMGEVINGSVEILIGHEID

Dit gedeelte beschrijft maatregelen met betrekking tot Verwerkers omgevingsveiligheidsbeleid.

Verwerker onderhoudt en handhaaft fysieke beveiligingsprocedures en beveiligingsprocedures voor computersystemen op alle locaties waar diensten worden verleend die direct of indirect met De Service verband houden. Deze servicelocaties zijn:

- Gelijkwaardig aan industriestandaarden voor dergelijke typen servicelocaties; en

- In overeenstemming met de toepasselijke wetgeving, met name de toepasselijke veiligheidsvereisten uit de AVG in alle gevallen waarin persoonsgegevens worden opgeslagen.

Op locaties waar gegevens zijn opgeslagen streeft Verwerker ernaar dat alle serverruimtes zijn uitgerust met branddetectie en brand onderdrukkende systemen, een afdoende luchtkoelingsstelsel, dat er controles zijn om te zorgen dat telecommunicatiekabels worden beschermd tegen onderschepping of beschadiging en dat de faciliteiten zijn uitgerust met adequate apparatuur om de stroomvoorziening in stand te houden in het geval van een stroomonderbreking.

Verwerker richt zich op industrie aanvaarde beveiliging voor locaties waar gegevens worden opgeslagen. Dat kan zijn: het onderhouden van gekwalificeerde beveiligers bij faciliteiten waar data gehost wordt die er zorg voor dragen dat alleen geautoriseerde personen toegang hebben tot locaties die gegevens verwerken of de klant ondersteunen.

Verwerker vraagt bezoekers, aannemers en onderhoudspersoneel (Bezoekers) om in te checken. Bezoekers worden altijd begeleid door een medewerker.

VEILIGHEIDSCONTROLE

Verwerker voert regelmatig tests uit op de software en het ondersteunende netwerk en de ondersteunende infrastructuur voor Verwerkingsverantwoordelijke persoonsgegevens verwerkt. Alle geïdentificeerde verbeteringen zullen worden verwerkt en gepaste maatregelen zullen binnen een redelijke termijn worden geïmplementeerd.

KENNISGEVING VAN BEVEILIGINGSINCIDENTEN

Verwerker heeft gedocumenteerde procedures ingesteld voor het melden en afhandelen van beveiligingsincidenten, waaronder netwerkincidenten, gegevensdiefstal, ongeoorloofde toegang tot gegevens, diefstal van apparatuur en externe bedreigingen van systemen (inclusief virussen), en zorgt ervoor dat een door de industrie aanvaard actieplan voor incidenten wordt opgezet, gehandhaafd, bijgewerkt en gecommuniceerd. Verwerker ondersteunt een dergelijk proces met een speciaal incidentteam en houdt een logboek bij van alle beveiligingsincidenten.

Verwerker streeft ernaar daadwerkelijke beveiligingsincidenten waarbij gegevens van Verwerkingsverantwoordelijke of een betrokkene betrokken zijn, binnen 24 uur na detectie te melden. Verwerker zal statusrapporten met betrekking tot het oplossen van het beveiligingsincident en het voorkomen van toekomstige dergelijke beveiligingsincidenten delen, totdat Verwerker redelijkerwijs tot de conclusie komt dat het beveiligingsincident is opgelost.

ENCRYPTIE

Verwerker versleuteld opgeslagen persoonsgegevens en persoonsgegevens in overdracht. Verwerker voldoet aan de van toepassing zijnde internationale en nationale normen, alsmede aan alle Nederlandse wet- en regelgeving.

Verwerker beheert alle cryptografische sleutels en certificaten veilig in overeenstemming met gedocumenteerde controlevereisten en -procedures die in overeenstemming zijn met industrie standaarden en het informatiebeveiligingsbeleid van Verwerker, en beschermt de gegevens van de Verwerkingsverantwoordelijke tegen ongeoorloofde toegang of vernietiging.

TOEGANGSMANAGEMENT

Verwerker handhaaft beleid en voert adequate technische controles uit die leiden tot de volgende veiligheidsmaatregelen:

- Toegangscontroles ontworpen om toegang tot gegevens te beperken tot geautoriseerde gebruikers zijn geïmplementeerd;
- Processen worden gedocumenteerd en uitgevoerd om ervoor te zorgen dat alle Persoonsgegevens worden geanonimiseerd na een bepaalde periode nadat de eigenaar inactief werd;
- Gebruikersaccounts kunnen te allen tijde handmatig inactief worden gemaakt;
- Toewijzingen van systeemaccounts wordt ten minste jaarlijks herzien;
- Unieke gebruiker-IDs en wachtwoorden worden voor personeel van Verwerker gebruikt;
- Processen worden gedocumenteerd en uitgevoerd om gebruikersbevoegdheden te controleren en bij te houden wanneer een gebruiker van rol/verantwoordelijkheid verandert;
- Er wordt een lijst bijgehouden van personeel met administratierechten en andere rechten die leiden tot veel privileges;
- Het systeem handhaaft de vergrendeling van gebruikersaccounts na een maximaal aantal inlogpogingen om aanvallen waarbij het wachtwoord geraden probeert te worden te voorkomen;
- Geprivilegieerde toegang voor ontwikkelaars tot productieomgevingen wordt alleen gebruikt voor geplande ondersteuning of ondersteuning in geval van nood; en
- Serviceaccounts zijn bestemd voor een specifiek doel en mogen niet worden gebruikt door personen voor enig ander doel.

WACHTWOORDMANAGEMENT

Verwerker heeft managementprotocollen opgesteld ter ondersteuning die met betrekking tot systeemaccounts, gebruikersaccounts en alle ondersteunende serviceaccounts op adequate wijze voorzien in de volgende wachtwoordmanagementcontroles:

- Verificatiemechanismen die niet kunnen worden omzeild om onrechtmatige toegang tot systemen te verkrijgen; en
- Authenticatiegegevens zoals wachtwoorden worden versleuteld opgeslagen, zodat de authenticatiegegevens niet in leesbare vorm kunnen worden hersteld.

DATAVEILIGING

Verwerker slaat alle back-up- en media met gegevens op in veilige opslagruimtes.

NETWERK- EN SYSTEEMBEVEILIGING

Verwerker documenteert en tracht te waarborgen dat:

- Firewalls met adequate ACL's (toegangscontrolelijsten) worden toegepast;
- Firewalls specifiek worden ingesteld om de door Verwerker geleverde diensten te beschermen; en
- Firewall logs worden gebruikt om al het verkeer in en uit de firewalls te registreren en te bewaken.

CYBERINBRAAKPREVENTIE

Verwerker maakt gebruik van industrie standaard tools voor inbraakdetectie en -preventie om vermoedelijke of daadwerkelijke cyberaanvallen te identificeren en op deze cyberaanvallen te reageren.

CLOUD COMPUTING

Verwerker levert een cloud-gebaseerde Service aan Verwerkingsverantwoordelijke en de betrokkenen.

ENDPOINTBEVEILIGING

Systemen van Verwerker hebben ingeschakelde en geüpdatete realtime malwarebescherming.

PATCH MANAGEMENT

Verwerker onderhoudt en handhaaft patch management. Verwerker implementeert patches die betrekking hebben op beveiliging en andere relevante updates van beveiligingskwetsbaarheden wanneer deze beschikbaar en goedgekeurd zijn.

SYSTEEMBEWAKING & -OPSLAG

Verwerker houdt een log bij van alle belangrijke incidenten, zoals incidenten die van invloed kunnen zijn op de betrouwbaarheid, integriteit en beschikbaarheid van de diensten voor de Verwerkingsverantwoordelijke en die kunnen helpen bij het identificeren of onderzoeken van

wezenlijke incidenten en/of inbreuken op toegangsrechten die zich met betrekking tot de gegevens van de Verwerkingsverantwoordelijke voordoen.

Verwerker bewaart dergelijke logs gedurende een periode van minimaal twaalf (12) maanden na creatie en zal dergelijke logs beschermen tegen ongeautoriseerde wijziging (waaronder het wijzigen of verwijderen van een log).

BACK-UP & HERSTEL NA EEN CALAMITEIT

Verwerker heeft een back-up strategie en proces met betrekking tot bedrijfscontinuïteit. Verwerker streeft er naar dat back-ups worden behandeld volgens industriestandaarden voor back-up en beveiliging; en verwerker zorgt ervoor dat frequent back-ups worden gemaakt en dat deze regelmatig worden getest om ervoor te zorgen dat systemen in afdoende een oude staat kunnen worden hersteld.

Verwerker heeft een formeel plan voor bedrijfscontinuïteit en calamiteitenherstel geïmplementeerd.

BIJLAGE III - OVERZICHT SUBVERWERKERS

De onderstaande lijst van Subverwerkers geeft een overzicht van alle Subverwerkers die Verwerker gebruikt om gegevens te verwerken. Subverwerkers die grote hoeveelheden Persoonsgegevens verwerken, worden geïntroduceerd, waarna wordt uitgelegd hoe de diensten van de subverwerker worden gebruikt. Ten slotte wordt aanvullende beveiligingsinformatie voor deze Subverwerkers gedeeld.

Portaalfunctionaliteiten, analyse en hosting - Subverwerkers

DOMO, Inc.

INLEIDING - Domo is een alles-in-één business intelligence platform voor het effectief bundelen en visualiseren van gegevens. Domo is een van de grootste spelers op de Business Intelligence markt en bedient allerlei bedrijven, waaronder multinationals. Als bedrijf dat altijd met data werkt is databeveiliging een van hun hoogste prioriteiten.

GEBRUIK - Verwerker gebruikt Domo-diensten i) om zijn klanten toegang te verlenen tot geavanceerde dashboarding voor analytische doeleinden, en ii) voor de analytische doeleinden van Verwerker.

AANVULLENDE BEVEILIGINGSINFORMATIE - Domo voldoet aan de hoogste industriestandaarden voor beveiliging, bijv. HIPAA, SOC-2 en het 'Privacyshield framework' dat bestaat tussen de VS en de EU. Domo is nooit eigenaar of gebruiker van ingevoerde gegevens en er wordt in geen geval toegang verleend tot de database van Verwerker zonder de uitdrukkelijke toestemming van Verwerker. In overeenstemming met de AVG zal Verwerker DOMO alleen toegang verlenen i) indien dit noodzakelijk is voor servicedoeleinden, en ii) ten behoeve van de bedrijfscontinuïteit.

Amazon Web Services

INTRODUCTIE - Amazon Web Services biedt betrouwbare en schaalbare cloudservices. Amazon Web Services is 's werelds grootste cloudserviceplatform, dat hosting biedt aan allerlei bedrijven.

GEBRUIK - Verwerker maakt gebruik van Amazon Web Services om gegevens veilig op te slaan en De Service te optimaliseren.

AANVULLENDE BEVEILIGINGSINFORMATIE - Amazon Web Services werkt volgens hoge beveiligingsstandaarden en stelt Verwerker in staat gegevens volgens dezelfde hoge standaarden op te slaan. Amazon Web Services is nooit eigenaar of gebruiker van ingevoerde gegevens en er wordt in geen geval zonder uitdrukkelijke toestemming van Verwerker toegang verleend tot de database van Verwerker. In overeenstemming met de GDPR zal verwerker Amazon Web Services alleen toegang verlenen i) indien nodig voor servicedoeleinden en ii) ten behoeve van de bedrijfscontinuïteit.

Marketing en Sales - Subverwerkers

- Salesforce
- Hubspot
- Hotjar
- Zoom
- LinkedIn Sales Navigator
- LinkedIn Ads
- Yesware
- Docusign
- Google Analytics
- MailChimp

Klantondersteuning - Subverwerkers

- Zendesk
- Intercom
- Jira
- FluentStream
- Voys
- Teamviewer
- GoToWebinar
- Typeform
- Receptive
- UserVoice

Administratie en interne communicatie - Subverwerkers

- Google (G Suite)
- Microsoft Office
- Exact