DATA PROCESSING AGREEMENT (DPA)

PRO Everything on Time B.V. – Map My Plant

1. Partijen

Deze verwerkersovereenkomst (“DPA”) wordt gesloten tussen:

PRO Everything on Time B.V., gevestigd te Purmerend, Nederland, ingeschreven bij de Kamer van Koophandel onder nummer 84440252,
hierna: **“Verwerker”**

en

Klant,
hierna: **“Verwerkingsverantwoordelijke”**

Gezamenlijk te noemen: **“Partijen”**.

2. Doel en reikwijdte

2.1 Deze DPA regelt de verwerking van persoonsgegevens door Verwerker in het kader van de levering van de softwaredienst **Map My Plant** en eventuele daarmee samenhangende ondersteuning, hosting, onderhoud en consultancy.

2.2 Deze DPA maakt integraal onderdeel uit van de tussen Partijen gesloten hoofdovereenkomst, offerte, abonnementsrelatie of andere overeenkomst (“Hoofdovereenkomst”).

2.3 Indien bepalingen uit deze DPA strijdig zijn met bepalingen uit de Hoofdovereenkomst, prevaleert deze DPA voor zover het de verwerking en bescherming van persoonsgegevens betreft.

2.4 Deze DPA is van toepassing op alle verwerkingen van persoonsgegevens die Verwerker namens Verwerkingsverantwoordelijke uitvoert in het kader van Map My Plant.

3. Rollen van Partijen

3.1 Verwerkingsverantwoordelijke bepaalt de doeleinden en middelen van de verwerking van persoonsgegevens.

3.2 Verwerker verwerkt persoonsgegevens uitsluitend namens Verwerkingsverantwoordelijke en uitsluitend in overeenstemming met diens gedocumenteerde instructies, tenzij een op Verwerker rustende wettelijke verplichting anders voorschrijft.

3.3 Indien Verwerker op grond van wet- of regelgeving verplicht is persoonsgegevens te verwerken buiten instructie van Verwerkingsverantwoordelijke, zal Verwerker Verwerkingsverantwoordelijke daarvan voorafgaand informeren, tenzij die wetgeving deze kennisgeving verbiedt.

4. Onderwerp, aard en doel van de verwerking

4.1 Verwerker verwerkt persoonsgegevens uitsluitend voor zover dat noodzakelijk is voor de uitvoering van de Hoofdovereenkomst.

4.2 De verwerking kan onder meer betrekking hebben op:

- het aanmaken en beheren van gebruikersaccounts;
- authenticatie en autorisatie van gebruikers;
- het beschikbaar stellen van de webapplicatie;
- opslag van account- en gebruiksgegevens;
- technische ondersteuning;
- onderhoud, beveiliging, logging en monitoring;
- foutanalyse en incidentafhandeling;
- back-up en herstel;
- communicatie met gebruikers over het gebruik van de dienst.

4.3 De verwerking geschiedt via de door Verwerker beheerde SaaS-omgeving en, waar relevant, via ondersteunende systemen voor hosting, e-mail en infrastructuurbeheer.

4.4 Voor zover Map My Plant in bepaalde configuraties of gebruiksvormen offline of lokaal kan functioneren, vallen gegevens die uitsluitend lokaal op systemen van Verwerkingsverantwoordelijke of diens gebruikers worden opgeslagen, niet onder de verantwoordelijkheid van Verwerker zolang Verwerker daar feitelijk geen toegang toe heeft.

5. Categorieën persoonsgegevens

5.1 Verwerker kan, afhankelijk van het gebruik door Verwerkingsverantwoordelijke, de volgende categorieën persoonsgegevens verwerken:

- naam of weergavenaam van gebruiker;
- e-mailadres;
- functietitel of rol;
- IP-adres;
- browsergegevens;
- apparaatgegevens;
- login- en sessiegegevens;
- gebruikersinstellingen;
- log- en auditgegevens;
- metadata over gebruik van de software;
- eventueel overige persoonsgegevens die Verwerkingsverantwoordelijke zelf in de software invoert.

5.2 Partijen erkennen dat Map My Plant primair is bedoeld voor technische, procesmatige en milieugerelateerde data en niet voor het structureel verwerken van bijzondere persoonsgegevens of andere gevoelige categorieën persoonsgegevens.

5.3 Verwerkingsverantwoordelijke zal geen bijzondere persoonsgegevens of strafrechtelijke persoonsgegevens in Map My Plant invoeren, tenzij dit uitdrukkelijk is overeengekomen en passende aanvullende maatregelen zijn genomen.

6. Categorieën betrokkenen

De categorieën betrokkenen kunnen onder meer omvatten:

- medewerkers van Verwerkingsverantwoordelijke;
- ingehuurde krachten en consultants van Verwerkingsverantwoordelijke;
- beheerders van Verwerkingsverantwoordelijke;
- contactpersonen van Verwerkingsverantwoordelijke;
- andere natuurlijke personen van wie persoonsgegevens door Verwerkingsverantwoordelijke in de Software worden ingevoerd.

7. Verplichtingen van Verwerker

7.1 Verwerker verwerkt persoonsgegevens uitsluitend op basis van gedocumenteerde instructies van Verwerkingsverantwoordelijke.

7.2 Verwerker zal persoonsgegevens niet voor eigen doeleinden gebruiken, verkopen, verhuren of anderszins exploiteren.

7.3 Verwerker beperkt de verwerking tot hetgeen noodzakelijk is voor de levering van de overeengekomen diensten.

7.4 Verwerker zorgt ervoor dat personen die onder zijn gezag handelen en toegang hebben tot persoonsgegevens:

- gebonden zijn aan een geheimhoudingsverplichting; of
- een passende wettelijke verplichting tot vertrouwelijkheid hebben.

7.5 Verwerker zal Verwerkingsverantwoordelijke, voor zover redelijk mogelijk, ondersteunen bij het nakomen van diens verplichtingen onder de AVG, waaronder verplichtingen ten aanzien van beveiliging, datalekken, gegevensbeschermingseffectbeoordelingen en verzoeken van betrokkenen.

7.6 Indien Verwerker van mening is dat een instructie van Verwerkingsverantwoordelijke in strijd is met de AVG of andere toepasselijke privacywetgeving, zal Verwerker Verwerkingsverantwoordelijke daarvan onverwijld op de hoogte stellen.

8. Verplichtingen van Verwerkingsverantwoordelijke

8.1 Verwerkingsverantwoordelijke garandeert dat hij gerechtigd is persoonsgegevens te laten verwerken door Verwerker.

8.2 Verwerkingsverantwoordelijke draagt er zorg voor dat de persoonsgegevens die hij aan Verwerker verstrekt:

- rechtmatig zijn verkregen;
- relevant en niet bovenmatig zijn;
- juist en actueel zijn voor zover redelijkerwijs vereist.

8.3 Verwerkingsverantwoordelijke is verantwoordelijk voor:

- de inhoud van de data die in Map My Plant wordt ingevoerd;
- het bepalen van bewaartermijnen;
- het voldoen aan informatieplichten richting betrokkenen;
- het beoordelen of een verwerkingsgrondslag aanwezig is.

8.4 Verwerkingsverantwoordelijke zal geen gegevens invoeren waarvan hij weet of redelijkerwijs moet vermoeden dat deze onrechtmatig zijn verwerkt of waarvoor Verwerker niet passend is ingericht.

9. Subverwerkers

9.1 Verwerker is gerechtigd om bij de verwerking gebruik te maken van subverwerkers.

9.2 Verwerker zal ervoor zorgen dat iedere subverwerker schriftelijk wordt gebonden aan verplichtingen die in materieel opzicht ten minste gelijkwaardig zijn aan de in deze DPA opgenomen verplichtingen, voor zover relevant voor de uitbestede verwerking.

9.3 Verwerker blijft verantwoordelijk voor het handelen en nalaten van door hem ingeschakelde subverwerkers alsof het zijn eigen handelen of nalaten betreft.

9.4 Verwerker zal Verwerkingsverantwoordelijke op diens verzoek informeren over de actuele categorieën of lijst van relevante subverwerkers.

9.5 Verwerkingsverantwoordelijke kan, op redelijke en objectief gemotiveerde gronden die verband houden met gegevensbescherming, bezwaar maken tegen de inzet van een nieuwe subverwerker. Partijen zullen in dat geval in redelijkheid overleggen over een passende oplossing.

10. Internationale doorgifte

10.1 Verwerker zal persoonsgegevens in beginsel verwerken binnen de Europese Economische Ruimte (EER).

10.2 Indien persoonsgegevens toch buiten de EER worden verwerkt of toegankelijk worden gemaakt, zal Verwerker zorg dragen voor een passende rechtsgrondslag en passende waarborgen, waaronder indien van toepassing:

- een adequaatheidsbesluit;
- Standard Contractual Clauses;
- aanvullende technische en organisatorische maatregelen.

10.3 Verwerker zal Verwerkingsverantwoordelijke op verzoek informeren over de gehanteerde waarborgen voor internationale doorgifte.

11. Beveiliging van de verwerking

11.1 Verwerker neemt passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen.

11.2 Bij het bepalen van het passende beveiligingsniveau houdt Verwerker rekening met:

- de stand van de techniek;
- de uitvoeringskosten;
- de aard, omvang, context en doeleinden van de verwerking;
- de waarschijnlijkheid en ernst van risico’s voor de rechten en vrijheden van betrokkenen.

11.3 De beveiligingsmaatregelen van Verwerker zijn nader uitgewerkt in **Annex II – Technische en Organisatorische Beveiligingsmaatregelen (ISO 27001-stijl)**.

12. Persoonsgegevenslekken

12.1 Verwerker meldt een inbreuk in verband met persoonsgegevens aan Verwerkingsverantwoordelijke zonder onredelijke vertraging nadat Verwerker kennis heeft genomen van de inbreuk.

12.2 Voor zover beschikbaar bevat de melding in ieder geval:

- de aard van de inbreuk;
- de vermoedelijke oorzaak;
- de categorieën betrokken gegevens;
- de categorieën betrokkenen;
- de waarschijnlijke gevolgen van de inbreuk;
- de reeds genomen of voorgestelde corrigerende maatregelen;
- een contactpunt voor vervolgvragen.

12.3 Verwerker zal redelijke medewerking verlenen aan Verwerkingsverantwoordelijke bij het:

- onderzoeken van de inbreuk;
- treffen van mitigerende maatregelen;
- voldoen aan meldplichten richting toezichthouders;
- informeren van betrokkenen, voor zover wettelijk vereist.

12.4 Verwerker doet geen meldingen aan betrokkenen of toezichthouders namens Verwerkingsverantwoordelijke, tenzij Partijen dat uitdrukkelijk overeenkomen of Verwerker daartoe wettelijk verplicht is.

13. Bijstand bij verzoeken van betrokkenen

13.1 Verwerker zal Verwerkingsverantwoordelijke, voor zover redelijk mogelijk en rekening houdend met de aard van de verwerking, ondersteunen bij het vervullen van diens verplichtingen ten aanzien van verzoeken van betrokkenen.

13.2 Indien een betrokkene zich rechtstreeks tot Verwerker wendt met een verzoek inzake inzage, rectificatie, wissing, beperking, overdraagbaarheid of bezwaar, zal Verwerker dat verzoek zo spoedig mogelijk doorgeleiden aan Verwerkingsverantwoordelijke, tenzij Verwerker wettelijk verplicht is zelf op het verzoek te reageren.

13.3 Verwerker zal zonder instructie van Verwerkingsverantwoordelijke geen inhoudelijke reactie geven op een dergelijk verzoek, behoudens wettelijke verplichtingen.

14. DPIA en voorafgaande raadpleging

14.1 Verwerker zal Verwerkingsverantwoordelijke, voor zover redelijkerwijs mogelijk en passend gezien de aard van de verwerking en de beschikbare informatie, ondersteunen bij het uitvoeren van:

- een gegevensbeschermingseffectbeoordeling (DPIA);
- een voorafgaande raadpleging van de toezichthouder.

14.2 Verwerker is gerechtigd om redelijke kosten in rekening te brengen voor substantiële ondersteuning buiten de normale dienstverlening.

15. Audit en controle

15.1 Verwerkingsverantwoordelijke heeft het recht om naleving van deze DPA in redelijke mate te verifiëren.

15.2 Verwerker zal op redelijk verzoek informatie verstrekken die nodig is om aan te tonen dat Verwerker zijn verplichtingen uit deze DPA nakomt.

15.3 Indien Verwerkingsverantwoordelijke een audit wenst uit te voeren, gelden de volgende voorwaarden:

- maximaal eenmaal per kalenderjaar, tenzij sprake is van een redelijk vermoeden van een materiële tekortkoming of een ernstig incident;
- met een redelijke aankondigingstermijn van ten minste 30 dagen;
- tijdens reguliere kantooruren;
- zonder onnodige verstoring van de bedrijfsvoering van Verwerker;
- onder strikte geheimhouding;
- voor rekening van Verwerkingsverantwoordelijke.

15.4 Verwerker mag verlangen dat een auditor:

- onafhankelijk is;
- geen concurrent van Verwerker is;
- gebonden is aan passende geheimhoudingsverplichtingen.

15.5 Verwerker mag auditverzoeken beperken of alternatieve bewijsvoering aanbieden indien dit redelijkerwijs nodig is ter bescherming van:

- de beveiliging van systemen;
- vertrouwelijke informatie van andere klanten;
- de integriteit van de dienstverlening.

16. Bewaartermijnen, teruggave en verwijdering

16.1 Verwerker bewaart persoonsgegevens niet langer dan noodzakelijk voor de uitvoering van de Hoofdovereenkomst, tenzij een langere wettelijke bewaarplicht geldt.

16.2 Na beëindiging van de Hoofdovereenkomst zal Verwerker, naar keuze van Verwerkingsverantwoordelijke en voor zover technisch mogelijk en contractueel voorzien:

- persoonsgegevens teruggeven; of
- persoonsgegevens verwijderen.

16.3 Verwerker mag kopieën bewaren voor zover dit noodzakelijk is:

- om te voldoen aan wettelijke verplichtingen;
- voor bewijsdoeleinden;
- in back-ups die volgens het reguliere back-up- en retentiebeleid worden overschreven.

16.4 Voor zover persoonsgegevens in back-ups zijn opgenomen, worden deze niet opnieuw actief verwerkt, anders dan voor back-up- en hersteldoeleinden, en worden zij binnen een redelijke termijn verwijderd of overschreven volgens de geldende back-upcyclus.

17. Vertrouwelijkheid

17.1 Verwerker behandelt alle persoonsgegevens en alle informatie die hij in het kader van deze DPA ontvangt als vertrouwelijk.

17.2 Deze vertrouwelijkheid geldt niet voor informatie die:

- rechtmatig openbaar beschikbaar is;
- reeds rechtmatig in bezit was van Verwerker zonder geheimhoudingsplicht;
- op grond van wet- of regelgeving openbaar moet worden gemaakt.

17.3 De verplichting tot vertrouwelijkheid blijft van kracht na beëindiging van deze DPA zolang de informatie niet rechtmatig openbaar is geworden.

18. Aansprakelijkheid

18.1 De aansprakelijkheid van Partijen in verband met deze DPA volgt de aansprakelijkheidsregeling uit de Hoofdovereenkomst, tenzij dwingend recht anders bepaalt.

18.2 Niets in deze DPA beperkt de aansprakelijkheid van Partijen voor zover een dergelijke beperking onder toepasselijk recht niet is toegestaan.

18.3 Verwerker is niet aansprakelijk voor schade die het gevolg is van:

- onrechtmatige instructies van Verwerkingsverantwoordelijke;
- onjuiste of onrechtmatige invoer van persoonsgegevens door Verwerkingsverantwoordelijke;
- gebruik van de Software in strijd met de documentatie of de Hoofdovereenkomst;
- lokale of offline opslag buiten de feitelijke macht van Verwerker.

19. Duur en einde

19.1 Deze DPA treedt in werking op de datum waarop de Hoofdovereenkomst ingaat of, indien eerder, op de datum waarop Verwerker voor het eerst persoonsgegevens namens Verwerkingsverantwoordelijke verwerkt.

19.2 Deze DPA blijft van kracht zolang Verwerker persoonsgegevens namens Verwerkingsverantwoordelijke verwerkt.

19.3 Bepalingen die naar hun aard zijn bedoeld om na beëindiging van kracht te blijven, waaronder bepalingen over vertrouwelijkheid, aansprakelijkheid en verwijdering, blijven ook na beëindiging van deze DPA van kracht.

20. Toepasselijk recht en geschillen

20.1 Op deze DPA is uitsluitend Nederlands recht van toepassing.

20.2 Geschillen voortvloeiend uit of samenhangend met deze DPA worden exclusief voorgelegd aan de bevoegde rechter te Amsterdam, tenzij dwingend recht anders voorschrijft.

21. Ondertekening

Aldus overeengekomen en ondertekend:

Verwerker
PRO Everything on Time B.V.

Naam:
Functie:
Datum:
Handtekening:

Verwerkingsverantwoordelijke

Naam:
Functie:
Datum:
Handtekening:

ANNEX I – VERWERKINGSOVERZICHT

1. Onderwerp van de verwerking

Het faciliteren van toegang tot en gebruik van het Map My Plant platform, inclusief accountbeheer, hosting, logging, ondersteuning, onderhoud en beveiliging.

2. Duur van de verwerking

Gedurende de looptijd van de Hoofdovereenkomst en voor zover nodig daarna voor verwijdering, back-upcycli, wettelijke bewaartermijnen en afwikkeling van verplichtingen.

3. Aard van de verwerking

De verwerking kan onder meer omvatten:

- verzamelen;
- vastleggen;
- organiseren;
- structureren;
- opslaan;
- bijwerken;
- opvragen;
- raadplegen;
- gebruiken;
- doorzenden binnen de infrastructuur;
- beveiligen;
- verwijderen;
- vernietigen.

4. Doeleinden van de verwerking

De verwerking dient uitsluitend de volgende doeleinden:

- levering van de Software;
- beschikbaar stellen van gebruikersaccounts;
- identificatie en authenticatie;
- autorisatie en toegangsbeheer;
- technische ondersteuning;
- serviceverbetering en foutanalyse;
- monitoring van beschikbaarheid en beveiliging;
- incidentafhandeling en herstel.

5. Categorieën betrokkenen

- werknemers;
- ingehuurde krachten;
- systeembeheerders;
- contactpersonen;
- overige natuurlijke personen van wie gegevens door Verwerkingsverantwoordelijke worden ingevoerd.

6. Categorieën persoonsgegevens

- naam;
- e-mailadres;
- gebruikersnaam;
- rol/functie;
- IP-adres;
- browserinformatie;
- apparaatinformatie;
- sessiegegevens;
- loginhistorie;
- gebruiks- en loggegevens;
- eventuele overige persoonsgegevens ingevoerd door Verwerkingsverantwoordelijke.

7. Bijzondere persoonsgegevens

Niet beoogd. Verwerkingsverantwoordelijke zal deze in beginsel niet invoeren. Indien dit toch plaatsvindt, blijft Verwerkingsverantwoordelijke verantwoordelijk voor een toereikende rechtsgrond, noodzaak en aanvullende waarborgen.

8. Frequentie van de verwerking

Doorlopend, voor zover gebruikers gebruik maken van de Software en ondersteunende diensten.

ANNEX II – TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

(ISO 27001-stijl beveiligingsbijlage)

1. Doel en uitgangspunten

1.1 Verwerker hanteert een risicogebaseerde benadering voor informatiebeveiliging.

1.2 Beveiligingsmaatregelen zijn gericht op bescherming van de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van systemen en diensten.

1.3 De inrichting van de beveiliging houdt rekening met:

- aard van de dienst;
- schaal van de organisatie;
- stand van de techniek;
- proportionaliteit;
- het dreigingsprofiel van een internettoegankelijke SaaS-dienst.

2. Governance en verantwoordelijkheden

2.1 Verwerker wijst intern verantwoordelijkheid toe voor:

- technisch beheer;
- beveiligingsbeheer;
- incidentmanagement;
- wijzigingsbeheer.

2.2 Verwerker beoordeelt periodiek of beveiligingsmaatregelen nog passend zijn bij de actuele risico’s.

2.3 Beveiligingsbesluiten, relevante wijzigingen en incidenten worden intern vastgelegd voor zover passend bij de schaal van de organisatie.

3. Asset management en systeemoverzicht

3.1 Verwerker onderhoudt een overzicht van de kerncomponenten van de dienst, waaronder:

- productieomgeving;
- applicatieserver(s);
- database(s);
- reverse proxy / webserver;
- back-upvoorzieningen;
- relevante beheeromgevingen.

3.2 Kritische componenten worden zodanig ingericht dat ongeautoriseerde toegang, wijziging of verwijdering van gegevens wordt beperkt.

4. Toegangsbeveiliging

4.1 Identiteits- en accountbeheer

- Gebruikers beschikken over unieke accounts.
- Accounts zijn persoonsgebonden.
- Accounts worden beheerd via gecontroleerde registratie- en authenticatiemechanismen.
- Overbodige of verouderde accounts worden gedeactiveerd of verwijderd binnen redelijke termijn.

4.2 Authenticatie

- Toegang tot beheerde omgevingen is beschermd met wachtwoorden of vergelijkbare authenticatiemiddelen.
- Authenticatiemechanismen zijn zo ingericht dat ongeautoriseerde toegang wordt bemoeilijkt.
- Wachtwoorden worden niet in leesbare vorm opgeslagen.

4.3 Autorisatie

- Toegang wordt verleend op need-to-know en need-to-access basis.
- Beheertoegang wordt beperkt tot bevoegde personen.
- Rechten worden toegekend op basis van rol of functionele noodzaak.

4.4 Sessiebeheer

- Sessies worden beschermd met passende sessiemechanismen.
- Indien van toepassing worden veilige cookie-attributen gebruikt, zoals httpOnly en secure.
- Sessies verlopen of worden ongeldig gemaakt bij passende gebeurtenissen, zoals uitloggen of reset van authenticatiegegevens.

5. Netwerk- en communicatiebeveiliging

5.1 Verkeer tussen gebruiker en de internettoegankelijke dienst wordt waar passend beschermd met TLS/HTTPS.

5.2 Externe toegang tot beheersystemen wordt zoveel mogelijk beperkt en afgeschermd.

5.3 Reverse proxy-, firewall- of vergelijkbare netwerkmaatregelen worden ingezet om ongeautoriseerde verbindingen en veelvoorkomende netwerkbedreigingen te mitigeren.

5.4 Openstaande netwerkdiensten en poorten worden beperkt tot wat functioneel noodzakelijk is.

5.5 Verwerker treft redelijke maatregelen tegen aanvallen zoals brute force, ongewenste geautomatiseerde toegang en misbruik van authenticatie-eindpunten.

6. Endpoint-, server- en platformbeveiliging

6.1 Productieomgevingen worden gescheiden gehouden van ontwikkel- of testactiviteiten voor zover redelijk en passend.

6.2 Servers en containers worden zodanig ingericht dat:

- alleen noodzakelijke services actief zijn;
- onnodige software en functionaliteit wordt vermeden;
- updates en patches binnen redelijke termijn worden doorgevoerd.

6.3 Beheertoegang tot servers en infrastructuur wordt beperkt tot bevoegde personen.

6.4 Verwerker treft redelijke maatregelen ter voorkoming van malware, ongeautoriseerde code-uitvoering en misbruik van systeemtoegang.

7. Applicatiebeveiliging

7.1 Verwerker past redelijke beveiligingsmaatregelen toe in het ontwikkel- en onderhoudsproces van de Software.

7.2 Daarbij wordt aandacht besteed aan onder meer:

- inputvalidatie;
- foutafhandeling;
- authenticatie en autorisatie;
- sessiebeveiliging;
- bescherming tegen ongeautoriseerde toegang tot data;
- beperking van onbedoelde datalekken via interfaces of logica.

7.3 Wijzigingen aan de Software worden voor zover redelijk getest voordat deze in productie worden genomen.

7.4 Kritieke bugs en beveiligingskwetsbaarheden worden met passende prioriteit behandeld.

8. Encryptie en sleutelbeheer

8.1 Gegevens in transit worden waar passend versleuteld met actuele transportbeveiliging.

8.2 Gegevens at rest kunnen, afhankelijk van infrastructuur en hostingopzet, beschermd worden door platform- of schijfversleuteling, OS-level maatregelen of vergelijkbare beveiliging.

8.3 Sleutels, geheimen, tokens en wachtwoorden worden niet onnodig in broncode opgenomen en worden zoveel mogelijk beheerd via configuratie of gescheiden geheimbeheer.

9. Logging en monitoring

9.1 Verwerker legt voor zover passend beveiligings- en operationeel relevante gebeurtenissen vast, zoals:

- loginpogingen;
- fouten;
- systeemevents;
- beveiligingsrelevante acties;
- applicatie-incidenten.

9.2 Logs worden beschermd tegen ongeautoriseerde toegang en onrechtmatige wijziging voor zover redelijk mogelijk.

9.3 Logs worden gebruikt voor:

- foutanalyse;
- incidentonderzoek;
- beveiligingsmonitoring;
- operationele continuïteit.

9.4 Logretentie wordt afgestemd op nut, proportionaliteit en technische mogelijkheden.

10. Back-up en herstel

10.1 Verwerker maakt periodieke back-ups van relevante productiegegevens voor zover passend bij de aard van de dienst.

10.2 Back-ups worden zodanig ingericht dat gegevens na een incident binnen redelijke grenzen kunnen worden hersteld.

10.3 Back-upretentie is beperkt tot wat redelijk nodig is voor herstel, continuïteit en beheer.

10.4 Herstelprocedures worden periodiek beoordeeld en waar passend getest.

11. Beschikbaarheid, continuïteit en veerkracht

11.1 Verwerker richt de dienst in met het doel een redelijke mate van beschikbaarheid en operationele continuïteit te bieden.

11.2 Verwerker neemt redelijke maatregelen tegen voorzienbare verstoringen, waaronder:

- hardware- of softwarestoringen;
- operationele fouten;
- netwerkuitval;
- beveiligingsincidenten.

11.3 Waar passend worden herstelmaatregelen en fallback-procedures gehanteerd om de impact van incidenten te beperken.

12. Incidentmanagement

12.1 Verwerker onderhoudt een intern proces voor het registreren, beoordelen, escaleren en afhandelen van beveiligingsincidenten.

12.2 Incidenten worden geclassificeerd op basis van ernst, impact en urgentie.

12.3 Indien een incident betrekking heeft op persoonsgegevens of de beveiliging daarvan kan raken, wordt beoordeeld of sprake is van een datalek in de zin van de AVG.

12.4 Corrigerende en preventieve maatregelen worden waar passend vastgelegd en opgevolgd.

13. Wijzigingsbeheer

13.1 Wijzigingen aan productieomgevingen, configuraties en relevante applicatieonderdelen worden beheerst doorgevoerd.

13.2 Bij significante wijzigingen wordt vooraf beoordeeld of deze:

- risico’s introduceren;
- invloed hebben op beveiliging;
- de beschikbaarheid van de dienst raken.

13.3 Waar passend worden rollback-mogelijkheden of herstelpaden voorzien.

14. Leveranciers- en subverwerkerbeheer

14.1 Verwerker selecteert subverwerkers en leveranciers met inachtneming van passende zorgvuldigheid ten aanzien van beveiliging en betrouwbaarheid.

14.2 Voor relevante leveranciers wordt beoordeeld of zij passende beveiligingsmaatregelen bieden voor de aard van hun rol.

14.3 Contractuele afspraken met subverwerkers bevatten passende beveiligings- en vertrouwelijkheidsverplichtingen.

15. Personeelsmaatregelen en vertrouwelijkheid

15.1 Personen die toegang hebben tot persoonsgegevens of kritieke systemen zijn gebonden aan geheimhouding.

15.2 Toegang wordt ingetrokken of aangepast wanneer deze niet langer nodig is, bijvoorbeeld bij functiewijziging of uitdiensttreding.

15.3 Verwerker stimuleert beveiligingsbewustzijn bij personen die betrokken zijn bij beheer, ontwikkeling en support.

16. Fysieke beveiliging

16.1 Voor zover Verwerker gebruik maakt van externe hosting- of datacenterfaciliteiten, rust de fysieke beveiliging primair op de betreffende hostingprovider.

16.2 Verwerker selecteert in beginsel providers die passende fysieke beveiligingsmaatregelen treffen, zoals:

- toegangscontrole;
- cameratoezicht;
- stroom- en klimaatbeheersing;
- brandpreventie.

17. Gegevensminimalisatie en privacy by design

17.1 Verwerker streeft ernaar om niet meer persoonsgegevens te verwerken dan noodzakelijk is voor de dienst.

17.2 Bij ontwerp- en wijzigingskeuzes wordt, voor zover redelijk, rekening gehouden met privacy- en beveiligingsprincipes.

17.3 Functionaliteiten worden, voor zover passend, zodanig ontworpen dat onnodige blootstelling van persoonsgegevens wordt beperkt.

18. Kwetsbaarheden en patchmanagement

18.1 Verwerker beoordeelt bekende kwetsbaarheden en beveiligingsmeldingen die relevant kunnen zijn voor de gebruikte stack en infrastructuur.

18.2 Kritieke beveiligingspatches worden met passende prioriteit toegepast.

18.3 Minder kritieke patches worden gepland op basis van risico, stabiliteit en impact op de dienstverlening.

19. Beëindiging en veilige verwijdering

19.1 Bij beëindiging van diensten worden persoonsgegevens verwijderd of teruggegeven conform de DPA en de Hoofdovereenkomst.

19.2 Verwerker neemt redelijke maatregelen om te waarborgen dat verwijdering ordelijk en veilig gebeurt.

19.3 Apparatuur of opslagmedia die buiten gebruik worden gesteld, worden op passende wijze opgeschoond, vernietigd of hergebruikt met waarborging van gegevensbescherming.

ANNEX III – SUBVERWERKERS

Onderstaande annex beschrijft de categorieën van subverwerkers die door Verwerker kunnen worden ingezet.

1. Hosting en infrastructuur

Mogelijke functies:

- hosting van applicatie en database;
- netwerk- en reverse proxy-infrastructuur;
- opslag;
- back-up.

Voorbeeldcategorie:

- Europese hostingprovider, zoals Hetzner.

2. E-mail en notificaties

Mogelijke functies:

- verzending van accountmails;
- wachtwoordreset;
- service-notificaties.

Voorbeeldcategorie:

- SMTP-provider of e-mailrelaydienst.

3. Monitoring en beheerhulpmiddelen

Mogelijke functies:

- operationele monitoring;
- foutdiagnostiek;
- infrastructuurbeheer.

Alleen voor zover toegepast.

4. Contractuele borging

Voor iedere relevante subverwerker zorgt Verwerker voor:

- passende contractuele privacy- en beveiligingsverplichtingen;
- een passend niveau van vertrouwelijkheid;
- instructies die aansluiten bij de aard van de verwerking.

ANNEX IV – SERVICE LEVEL AGREEMENT (SLA)

1. Doel

1.1 Deze SLA beschrijft de serviceniveaus die Verwerker nastreeft voor de levering, ondersteuning, beschikbaarheid en incidentafhandeling van Map My Plant.

1.2 Deze SLA is een inspanningsverbintenis, tenzij uitdrukkelijk anders overeengekomen.

1.3 Deze SLA geldt alleen voor de door Verwerker beheerde online SaaS-omgeving. Zij geldt niet voor:

- lokaal of offline gebruik buiten de infrastructuur van Verwerker;
- storingen veroorzaakt door internetproviders van klant;
- storingen in systemen van Verwerkingsverantwoordelijke;
- storingen door onjuist gebruik of ongeautoriseerde wijzigingen door klant.

2. Definities

2.1 Beschikbaarheid

Het percentage tijd waarin de productieomgeving van de online dienst toegankelijk is voor regulier gebruik, exclusief uitgesloten periodes zoals gepland onderhoud en overmacht.

2.2 Incident

Een ongeplande onderbreking, storing, fout of beveiligingsgebeurtenis die invloed heeft op de beschikbaarheid, integriteit, vertrouwelijkheid of bruikbaarheid van de dienst.

2.3 Service window

De periode waarin de dienst in beginsel beschikbaar behoort te zijn: 24 uur per dag, 7 dagen per week, behoudens uitzonderingen.

2.4 Kantooruren

Maandag tot en met vrijdag van 09:00 tot 17:00 uur Nederlandse tijd, exclusief algemeen erkende feestdagen in Nederland.

3. Beschikbaarheidsdoelstelling

3.1 Verwerker streeft naar een **maandelijkse beschikbaarheid van 99,5%** van de online productieomgeving.

3.2 Beschikbaarheid wordt berekend als:

Beschikbaarheid (%) = ((Totale tijd - ongeplande downtime) / Totale tijd) x 100

3.3 De volgende periodes tellen niet mee als ongeplande downtime:

- aangekondigd onderhoud;
- spoedonderhoud dat redelijkerwijs noodzakelijk is;
- storingen aan de zijde van klant;
- storingen in internetverbindingen buiten de invloedssfeer van Verwerker;
- overmachtssituaties;
- uitval door derden buiten redelijke beheersing van Verwerker;
- uitval veroorzaakt door integraties, scripts, apparaten of software van klant.

3.4 Verwerker garandeert geen ononderbroken of foutloze werking.

4. Onderhoud

4.1 Verwerker mag gepland onderhoud uitvoeren om de veiligheid, stabiliteit en prestaties van de dienst te behouden of te verbeteren.

4.2 Verwerker zal gepland onderhoud, indien redelijk mogelijk, vooraf aankondigen.

4.3 Verwerker streeft ernaar gepland onderhoud zoveel mogelijk buiten reguliere kantooruren uit te voeren, maar is daartoe niet verplicht.

4.4 Verwerker mag spoedonderhoud zonder voorafgaande aankondiging uitvoeren indien dit redelijkerwijs noodzakelijk is voor:

- beveiliging;
- integriteit van data;
- stabiliteit van systemen;
- herstel van incidenten.

5. Supportkanalen

5.1 Incidenten en supportverzoeken kunnen door klant worden gemeld via de door Verwerker aangewezen kanalen, zoals:

- e-mail;
- supportformulier;
- ticketingmechanisme in de software, indien beschikbaar.

5.2 Klant verstrekt bij een melding voor zover redelijk mogelijk:

- een duidelijke omschrijving van het probleem;
- tijdstip van constatering;
- relevante foutmeldingen;
- stappen om het probleem te reproduceren;
- impact op gebruikers of processen.

6. Incidentclassificatie

Prioriteit 1 – Kritiek

Volledige of nagenoeg volledige onbeschikbaarheid van de kernfunctionaliteit van de online dienst, of een ernstig beveiligingsincident met hoge impact.

Voorbeelden:

- applicatie niet bereikbaar;
- login voor alle gebruikers niet mogelijk;
- ernstig datalek of acute beveiligingscompromittering;
- database of kernservice onbruikbaar.

Prioriteit 2 – Hoog

Essentiële functionaliteit werkt niet correct, maar de dienst is niet volledig uitgevallen.

Voorbeelden:

- belangrijke functionaliteit faalt voor meerdere gebruikers;
- opslag of laden van data mislukt structureel;
- ernstige performanceproblemen die kerngebruik blokkeren.

Prioriteit 3 – Middel

Niet-kritieke functionaliteit werkt onjuist of beperkt, met workaround mogelijk.

Voorbeelden:

- onderdeel van een scherm functioneert niet goed;
- fout bij specifieke workflow met tijdelijke workaround;
- beperkte visuele of functionele defecten.

Prioriteit 4 – Laag

Kleine fouten, cosmetische issues, vragen of verzoeken zonder directe operationele impact.

Voorbeelden:

- tekstuele fout;
- kleine UI-onvolkomenheid;

- algemeen gebruiksvraagstuk;
- verbetervoorstel.

7. Reactie- en afhandelingstijden

7.1 Doelreactietijden tijdens kantooruren

Prioriteit	Eerste reactie	Start analyse / triage
P1 Kritiek	binnen 4 uur	zo spoedig mogelijk
P2 Hoog	binnen 1 werkdag	binnen 1 werkdag
P3 Middel	binnen 2 werkdagen	binnen redelijke termijn
P4 Laag	binnen 5 werkdagen	op planningbasis

7.2 Doelafhandeling

Verwerker geeft geen harde oplosgarantie, maar streeft naar redelijke en proportionele afhandeling afhankelijk van ernst, complexiteit, afhankelijkheden en risico. Problemen worden primair telefonisch doorgegeven.

7.3 Tijdelijke maatregelen

Verwerker mag incidenten afhandelen door middel van:

- een workaround;
- tijdelijke mitigatie;
- configuratiewijziging;
- rollback;
- gefaseerde structurele oplossing.

8. Escalatie en communicatie

8.1 Bij ernstige incidenten houdt Verwerker klant naar redelijkheid op de hoogte van:

- status;
- impact;
- verwachte vervolgstappen;
- eventuele tijdelijke maatregelen.

8.2 Interne escalatie vindt plaats wanneer:

- impact groter blijkt dan eerst ingeschat;
- beveiliging of dataverlies dreigt;
- herstel meer specialistische inzet vereist.

8.3 Voor P1-incidenten streeft Verwerker naar actieve opvolging totdat de dienst redelijkerwijs is gestabiliseerd.

9. Beveiligingsincidenten

9.1 Beveiligingsincidenten worden beoordeeld op:

- waarschijnlijkheid van misbruik;
- impact op persoonsgegevens;
- impact op vertrouwelijkheid, integriteit en beschikbaarheid.

9.2 Indien sprake is van een persoonsgegevenslek, geldt daarnaast het datalekregime uit de DPA.

9.3 Verwerker kan bij beveiligingsincidenten onmiddellijk technische maatregelen nemen, waaronder:

- blokkeren van toegang;
- reset van credentials;
- isoleren van systemen;
- tijdelijke deactivering van functionaliteit.

10. Back-up en hersteldoelstellingen

10.1 Verwerker streeft naar periodieke back-ups van relevante productiegegevens.

10.2 Hersteldoelstellingen zijn inspanningsdoelstellingen en geen garanties.

10.3 Richtwaarden, voor zover redelijk haalbaar in de feitelijke infrastructuur:

- **RPO (Recovery Point Objective):** maximaal 24 uur gegevensverlies voor standaard back-upscenario's;
- **RTO (Recovery Time Objective):** herstel binnen redelijke termijn afhankelijk van aard en ernst van het incident.

10.4 Deze richtwaarden gelden niet bij:

- logische corruptie veroorzaakt door klant;
- fouten die lang onopgemerkt zijn gebleven;
- externe afhankelijkheden;
- overmacht;
- situaties waarin forensisch onderzoek of beveiligingscontainment prioriteit vereist.

11. Uitsluitingen

De SLA is niet van toepassing op of geeft geen aanspraak bij:

- problemen veroorzaakt door foutief gebruik door klant;
- gebruik in strijd met documentatie of instructies;
- niet-ondersteunde browsers, apparaten of configuraties;
- storingen in internet- of netwerkverbindingen van klant;
- problemen in externe systemen van klant of derden;
- lokale opslag of offline gebruik buiten de online dienst;
- test-, ontwikkel- of preview-omgevingen, tenzij uitdrukkelijk anders overeengekomen.

12. Wijzigingen en releases

12.1 Verwerker mag de Software wijzigen, verbeteren en actualiseren.

12.2 Niet iedere wijziging wordt vooraf aangekondigd.

12.3 Verwerker streeft ernaar releases zodanig uit te voeren dat verstoringen beperkt blijven.

12.4 Verwerker is niet verplicht om klantspecifieke functionaliteit of featureverzoeken te implementeren, tenzij uitdrukkelijk overeengekomen.

13. Service credits

13.1 Tenzij uitdrukkelijk schriftelijk anders overeengekomen, kent deze SLA **geen service credits, boetes of automatische vergoedingen** bij niet-gehaalde serviceniveaus.

13.2 Afwijkingen van doelstellingen vormen op zichzelf geen tekortkoming die recht geeft op schadevergoeding, ontbinding of opschorting, tenzij sprake is van opzet, grove nalatigheid of andersluidende dwingendrechtelijke bepalingen.

14. Rapportage

14.1 Verwerker kan naar eigen inzicht operationele of beveiligingsinformatie delen indien dat nuttig is voor incidentafhandeling of relatiebeheer.

14.2 Verwerker is niet verplicht tot structurele maatwerkrapportages, tenzij uitdrukkelijk overeengekomen.

15. Samenwerking door klant

15.1 Klant verleent alle redelijke medewerking die nodig is voor support en incidentafhandeling.

15.2 Klant zorgt voor:

- actuele contactpersonen;
- voldoende informatie bij meldingen;
- tijdige terugkoppeling bij verificatie of testen;
- passende lokale IT-voorzieningen aan eigen zijde.

15.3 Vertragingen die ontstaan door uitblijven van redelijke medewerking van klant komen niet voor rekening van Verwerker.

16. Prioriteit van documenten

16.1 Bij tegenstrijdigheid tussen de Hoofdovereenkomst en deze SLA prevaleert de Hoofdovereenkomst, tenzij de Hoofdovereenkomst uitdrukkelijk bepaalt dat deze SLA voorgaat.

16.2 Bij tegenstrijdigheid tussen de DPA en deze SLA prevaleert de DPA voor zover het persoonsgegevens en gegevensbescherming betreft.