Verwerkersovereenkomst

Verwerkersovereenkomst

Tussen:

PTH Groep bv, gevestigd aan de Harm Smidswei 9 te Kollumersweach, rechtsgeldig vertegenwoordigd door M.de Jong, directeur, hierna: 'Verwerkingsverantwoordelijke';

en

Naam Verwerker, gevestigd aan de ..... te ....., rechtsgeldig vertegenwoordigd door naam, functie, hierna: 'Verwerker';

Hierna gezamenlijk te noemen: 'Partijen'.

Artikel 1. Begripsbepalingen

De in deze Verwerkersovereenkomst gebruikte begrippen hebben de betekenis zoals bedoeld in de Algemene Verordening Gegevensbescherming (AVG). Aanvullend:

- 'Betrokkene': De natuurlijke persoon op wie de persoonsgegevens betrekking hebben.
- 'Bijlage(n)': onlosmakelijk verbonden documenten waarin verwerkingen, beveiliging en procedures zijn uitgewerkt.
- 'Datalek': elke inbreuk in verband met persoonsgegevens zoals omschreven in artikel 4 lid 12 AVG;
- 'Derden': Iedere andere persoon of organisatie dan de betrokkene, de verwerkingsverantwoordelijke, de verwerker en de personen die onder rechtstreeks gezag van de verwerkingsverantwoordelijke of verwerker gemachtigd zijn om persoonsgegevens te verwerken.
- 'Hoofdovereenkomst': De tussen Partijen gesloten overeenkomst waarin de aard, duur en inhoud van de dienstverlening is overeengekomen en op grond waarvan de Verwerker in opdracht van de Verwerkingsverantwoordelijke persoonsgegevens verwerkt.
- 'Sub-verwerker': iedere partij die namens Verwerker persoonsgegevens verwerkt;
- 'Verwerking': Elke bewerking of elk geheel van bewerkingen met betrekking tot persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés. Hieronder valt onder meer het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens.

Artikel 2. Onderwerp en toepassingsgebied

Deze Verwerkersovereenkomst is van toepassing op alle verwerkingen van persoonsgegevens door Verwerker ten behoeve van Verwerkingsverantwoordelijke, zoals overeengekomen in de Hoofdovereenkomst. Bij tegenstrijdigheid prevaleert deze Verwerkersovereenkomst.

Artikel 3. Doeleinden en instructies

1. Verwerker verwerkt persoonsgegevens uitsluitend op basis van schriftelijke instructies van Verwerkingsverantwoordelijke.
2. Verwerker mag persoonsgegevens niet voor eigen doeleinden verwerken.
3. Verwerker mag de persoonsgegevens niet aan derden ter beschikking stellen
4. Verwerker mag de persoonsgegevens ook niet gepseudonimiseerd of geanonimiseerd aan derden ter beschikking stellen nog de gegevens in algemene zin voor andere doeleinden laten verwerken.

Artikel 4. Categorieën gegevens en betrokkenen

In het kader van deze Verwerkersovereenkomst kunnen de volgende categorieën persoonsgegevens worden verwerkt: NAW-gegevens (naam, adres, woonplaats), contactgegevens (telefoonnummer, e-mailadres), geslacht, geboortedatum, en mogelijk andere gegevens afhankelijk van de specifieke diensten zoals overeengekomen in de Hoofdovereenkomst. De categorieën van betrokkenen omvatten doorgaans klanten, werknemers en andere relaties van de Verwerkingsverantwoordelijke. De aard en doeleinden van de verwerking, evenals een gedetailleerd overzicht van de sub-verwerkers en eventuele verwerkingen buiten de EER, worden nader gespecificeerd in Bijlage 1.

Artikel 5. Beveiliging

1. Verwerker hanteert minimaal hetzelfde niveau van beveiliging van de persoonsgegevens als Verwerkingsverantwoordelijke.
2. Verwerker treft passende technische en organisatorische maatregelen (zie Bijlage 2) om verlies of onrechtmatige verwerking te voorkomen.
3. Deze maatregelen houden rekening met:
    - De stand van de techniek;
    - De uitvoeringskosten;
    - De aard en omvang van de verwerking;
    - De risico's voor de rechten van betrokkenen.

Artikel 6. Sub-verwerkers

1. Verwerker stelt een actueel overzicht van alle subverwerkers beschikbaar.

2. Verwerker mag uitsluitend subverwerkers inzetten na digitale kennisgeving naar Verwerkingsverantwoordelijke en er door Verwerkingsverantwoordelijke binnen 30 dagen na kennisgeving geen bezwaar op het inzetten van deze subverwerker is gekomen.
3. Wanneer er wijzigingen in subverwerkers hebben plaatsgevonden, levert Verwerker een geactualiseerd overzicht van Bijlage 1: Overzicht verwerkingen, aan.
4. Verwerkingsverantwoordelijke heeft te allen tijde het recht bezwaar te maken tegen subverwerkers, bijvoorbeeld door wijzigingen in de markt of in wet- en regelgeving.
5. Subverwerkers dienen contractueel ten minste aan dezelfde verplichtingen te voldoen als opgenomen in deze overeenkomst.
6. Verwerker blijft verantwoordelijk voor het nakomen van de verplichtingen van de subverwerker(s).

Artikel 7. Specifieke bepalingen ten aanzien van doorgifte van persoonsgegevens naar derde landen

1. Definities:
    a) 'Derde land': elk land dat geen onderdeel is van de Europese Economische Ruimte (EER) Autoriteit Persoonsgegevens.
    b) 'Doorgifte': elke handeling waarbij persoonsgegevens worden overgedragen of beschikbaar gesteld aan een ontvanger in een derde land, inclusief toegang op afstand.
2. Voorwaarden voor doorgifte:
    a) Verwerker zal persoonsgegevens uitsluitend doorgeven aan een derde land op grond van schriftelijke, voorafgaande en ondubbelzinnige instructies van de verwerkingsverantwoordelijke, ook als er sprake is van een adequaatheidsbesluit.
    b) Elke doorgifte vindt plaats op basis van ten minste één van de instrumenten in overeenstemming met Hoofdstuk V AVG, zoals:

        I. een adequaatheidsbesluit van de Europese Commissie;
        II. door de Europese Commissie goedgekeurde standaardcontractbepalingen (SCC's);
        III. bindende bedrijfsvoorschriften of andere door de AVG toegestane waarborgen.
        IV. Verwerker overlegt voorafgaand aan enige doorgifte:
        V. het beoogde derde land en de concrete locatie(s) van verwerking;
        VI. de categorieën betrokkenen en de aard van de persoonsgegevens;

VII. de gehanteerde waarborgen (bijv. SCC's of BCR's) en de beoogde rechtsgrondslag.

3. Toezicht en naleving:
    a) Verwerker draagt zorg dat sub-verwerkers in derde landen dezelfde verplichtingen uit deze overeenkomst naleven en blijft hiervoor aansprakelijk.
    b) Verwerker stelt de verwerkingsverantwoordelijke onverwijld op de hoogte van iedere wijziging in toepasselijke lokale wet- en regelgeving in het derde land die de rechtsgeldigheid van de doorgifte kan beïnvloeden.
4. Meldplicht en documentatie:
    a) Verwerker houdt een register bij van alle doorgiften naar derde landen, waarin minimaal de in lid 2.3 genoemde gegevens zijn opgenomen.
    b) Op verzoek verstrekt verwerker alle benodigde documentatie en ondersteuning om aan te tonen dat bij elke doorgifte is voldaan aan de AVG-eisen.

Artikel 8. Rechten van betrokkenen

1. Onder verzoeken van betrokkenen worden verstaan alle aanvragen tot uitoefening van de rechten zoals omschreven in artikel 12 tot en met 22 AVG, waaronder inzage, rectificatie, wissing, beperking van verwerking, dataportabiliteit en bezwaar.
2. Verwerker zal ontvangen verzoeken van betrokkenen onverwijld en in elk geval binnen vierentwintig (24) uur schriftelijk doorsturen aan de Verwerkingsverantwoordelijke, zonder verlenging van de wettelijke beantwoordingstermijn.
3. Verwerker draagt zorg voor de implementatie en beschikbaarstelling van passende technische maatregelen (zoals data-extractie- en exportfunctionaliteit, logging en encryptie) om tijdige en volledige uitvoering van verzoeken te waarborgen.
4. Verwerker levert organisatorische ondersteuning voor beantwoording van verzoeken, coördinatie van wissing of rectificatie en rapportage van uitgevoerde acties binnen vijf (5) werkdagen na ontvangst van instructies van de Verwerkingsverantwoordelijke.
5. Verwerker ondersteunt de Verwerkingsverantwoordelijke bij de verificatie van de identiteit van de verzoeker conform de criteria in overweging (64) AVG.
6. Voor verzoeken om dataportabiliteit zal de Verwerker persoonsgegevens aanleveren in een gestructureerd, gangbaar en machineleesbaar formaat.
7. Verwerker houdt een register bij van alle verzoeken van betrokkenen, met daarin datum ontvangst, datum doorsturing, genomen maatregelen en datum

uitvoering, en verstrekt op verzoek een afschrift van dit register aan de Verwerkingsverantwoordelijke.

Artikel 9. Datalekken

1. Verwerker informeert Verwerkingsverantwoordelijke **onverwijld, doch uiterlijk** binnen 48 uur na ontdekking van een datalek.
2. De Verwerker blijft de Verwerkingsverantwoordelijke onverminderd bijstaan bij het onderzoek naar en de afhandeling van het datalek, vanaf de eerste melding tot en met de definitieve afronding, door:
    a) ongevraagd aanvullende informatie en documentatie te verstrekken over oorzaak, omvang en gevolgen van het incident;
    b) technische en organisatorische maatregelen te evalueren, (her)documenteren en waar nodig bij te werken;
    c) te ondersteunen bij interne en externe communicatie, inclusief de voorbereiding van rapportages aan toezichthouders en betrokkenen;
    d) mee te werken aan forensische onderzoeken, audits of andere verificatieactiviteiten;
    e) e. regelmatige statusupdates te geven en deel te nemen aan overleg- of crisissessies.
3. De Verwerker levert alle in lid 9.2 genoemde bijstand binnen de door de Verwerkingsverantwoordelijke gestelde termijnen en in het door hem voorgeschreven formaat.
4. Informatie die verstrekt wordt, omvat minimaal:
    a) aard van het datalek;
    b) soort gegevens;
    c) tijdstip van ontdekking en incident;
    d) beoordeling van gevolgen;
    e) reeds genomen of voorgestelde maatregelen;
    f) contactpersoon.
5. Verwerkingsverantwoordelijke beslist over melding aan toezichthouder en betrokkenen.
6. Zie Bijlage 3 voor de meldprocedure.

Artikel 10. Geheimhouding

1. Verwerker en haar medewerkers/sub-verwerkers houden persoonsgegevens vertrouwelijk.
2. Toegang tot persoonsgegevens is strikt beperkt is tot gemachtigde personen die gebonden zijn aan geheimhouding op basis van een schriftelijke overeenkomst met Verwerker.
3. Uitzonderingen gelden alleen op basis van wettelijke verplichtingen of schriftelijke toestemming.

Artikel 11. Audits en controles

1. Verwerkingsverantwoordelijke heeft het recht éénmaal per jaar een audit te (laten) uitvoeren met twee weken voorafgaande aankondiging.
2. Verwerker verleent alle medewerking, inclusief toegang tot relevante systemen en documentatie.
3. Verwerker stelt alle informatie ter beschikking die nodig is om aantoonbaar te maken dat de verplichtingen op grond van de AVG worden nageleefd.
4. Kosten van de audit zijn voor rekening van Verwerkingsverantwoordelijke; interne kosten van Verwerker zijn voor eigen rekening.
5. Bevindingen worden schriftelijk gedeeld. Verwerker voert noodzakelijke maatregelen binnen redelijke termijn uit.
6. In geval van incidenten of gegronde twijfels heeft Verwerkingsverantwoordelijke het recht om vaker of aanvullende audits uit te (laten) voeren.

Artikel 12. Aansprakelijkheid

1. Categorieën van schending en schadevergoeding:
    a) *Geringe tekortkomingen* (bijv. administratieve fouten, beperkte niet-structurele afwijkingen): beperkte directe schadevergoeding tot maximaal de kosten die Verwerkingsverantwoordelijke maakt om de tekortkoming te administreren, te melden en/of te corrigeren.
    b) *Materiële inbreuken* (bijv. ongeoorloofde toegang, verlies of wijziging van persoonsgegevens): vergoeding tot de kosten die Verwerkingsverantwoordelijke maakt om de tekortkoming te administreren, te melden en/of te corrigeren, aangevuld met de kosten die derden daartoe maken.
    c) *Opzet of grove nalatigheid* (inclusief frauduleus handelen): onbeperkte aansprakelijkheid; de in lid 1.a en 1.b opgenomen plafonds zijn niet van toepassing.
2. De in lid 1 opgenomen aansprakelijkheidsbeperkingen gelden per incident, met uitzondering van gevallen van opzet of grove nalatigheid.
3. De Verwerker sluit een beroepsaansprakelijkheidsverzekering af, gericht op dekking van de aansprakelijkheden zoals beschreven in lid 1 en 2.
4. Verwerker vrijwaart de Verwerkingsverantwoordelijke volledig tegen aanspraken van derden voortvloeiend uit tekortkomingen of onrechtmatig handelen door sub-verwerkers en blijft hiervoor aansprakelijk, conform artikel 28 lid 4 AVG.
5. Verwerkingsverantwoordelijke is niet aansprakelijk voor indirecte, gevolg- of gederfde winstschade, met uitzondering van gevallen van opzet of grove nalatigheid.

Artikel 13. Duur en beëindiging

1. Deze overeenkomst geldt zolang Verwerker persoonsgegevens verwerkt in opdracht van Verwerkingsverantwoordelijke.
2. Bij beëindiging van de Hoofdovereenkomst:
    a) Persoonsgegevens worden op schriftelijk verzoek vernietigd of geretourneerd;
    b) Verwerker verklaart schriftelijk de vernietiging;
    c) Verwerker zorgt dat sub-verwerkers dit ook doen en overlegt de schriftelijke bevestig van iedere sub-verwerker hierover aan Verwerkingsverantwoordelijke.

Artikel 14. Wijzigingen en toepasselijk recht

1. Wijzigingen zijn alleen geldig als deze schriftelijk overeengekomen worden.
2. Wijzigingen in privacywetgeving verplichten partijen tot herziening van deze overeenkomst.
3. Op deze overeenkomst is Nederlands recht van toepassing.
4. Geschillen worden voorgelegd aan de bevoegde rechter in het arrondissement van Verwerkingsverantwoordelijke.

Bijlagen:

- Bijlage 1: Overzicht verwerkingen
- Bijlage 2: Technische en organisatorische maatregelen
- Bijlage 3: Procedure datalekken

Aldus overeengekomen en in tweevoud ondertekend te *plaats* op *datum*.

	Verwerker	**Verwerkingsverantwoordelijke**
Naam:		M. J. Dijkstra
Functie:		Kwaliteitsmanager
Handtekening:		

PTH GROEP

Bijlage 1: Overzicht verwerkingen

Nr	Categorie persoonsgegevens	Specifieke doeleinden van verwerking	Categorieën van betrokkenen	Sub-verwerkers	Verwerkingen buiten de EER (ja/nee + toelichting)
1	(bijv. naam, e-mailadres, IP-adres, geboortedatum, telefoonnummer, geslacht, etc.)	(bijv. gebruikersbeheer, klantcommunicatie)	(bijv. klanten, medewerkers, subverwerkers)	(bijv. Mailchimp, AWS/Google/...)	(bijv. ja – opslag via AWS Cloud in EU en in VS met SCC's)
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

Toelichting op kolommen in Bijlage 1:

- Categorie persoonsgegevens: Benoem de exacte velden/gegevens (bijv. geboortedatum, burgerservicenummer, locatiegegevens).
- Specifieke doeleinden van verwerking: Geef het concrete doel aan, niet enkel 'dienstverlening' maar bijv. 'het versturen van facturen' of 'analytics op gebruikersgedrag'.
- Categorieën van betrokkenen: Omschrijf specifiek wie het betreft (bv. 'nieuwsbriefabonnees' i.p.v. alleen 'gebruikers').
- Sub-verwerkers: Vermeld volledige naam + vestigingsland + rol. Bijv. 'Google Ireland – Analytics'.
- Verwerkingen buiten de EER: Vermeld *waarheen*, *welke maatregelen zijn getroffen* (bijv. standaardcontractbepalingen, adequaatheidsbesluit).

N.B. Verwerker is gehouden aan de wettelijke bewaartermijnen ten aanzien van de verschillende categorieën persoonsgegevens.

Bijlage 2: Technische en organisatorische maatregelen

a. Minimale maatregelen conform AVG

Volgend de AVG dient de Verwerker ten minste de volgende maatregelen te treffen:

- Encryptie en pseudonimisering van persoonsgegevens om de risico's van gegevensverwerking te beperken.
- Beveiliging van systemen en diensten die persoonsgegevens verwerken, inclusief bescherming tegen ongeautoriseerde toegang.
- Persoonsgegevens vertrouwelijk behandelen en contractuele afspraken vastleggen t.a.v. geheimhouding met medewerkers.
- Beheer van leveranciers en subverwerkers inclusief het vastleggen daarvan in schriftelijke overeenkomsten.
- Het bijhouden van een register van alle categorieën van verwerkingsactiviteiten die namens een Verwerkingsverantwoordelijke worden uitgevoerd.
- Herstelvermogen om de beschikbaarheid en toegang tot persoonsgegevens tijdig te herstellen bij een incident.
- Regelmatige evaluatie en testen van technische en organisatorische maatregelen om de effectiviteit te waarborgen.
- Het na afloop van de bewaartermijn veilig verwijderen van gegevens volgens wet- en regelgeving en vastgesteld beleid.

b. Technische beveiligingsmaatregelen

Maatregel	Beschrijving	Toelichting/Details	Toegepast
Encryptie	Versleuteling van persoonsgegevens tijdens opslag en overdracht.	Bijv. AES-256 voor opslag, TLS 1.2+ voor netwerkverkeer.	j/n
Pseudonimisering	Vervanging van identificeerbare gegevens door pseudoniemen om de herleidbaarheid te verminderen.	Toegepast op datasets voor analyse en testing.	j/n
Toegangsbeveiliging	Implementatie van sterke authenticatie- en autorisatiemechanismen.	Bijv. tweefactorauthenticatie, rolgebaseerde toegang.	j/n

Logging en monitoring	Registratie en bewaking van systeemactiviteiten om ongeautoriseerde toegang of afwijkingen te detecteren.	Logs worden minimaal 6 maanden bewaard en regelmatig geanalyseerd.	j/n
Malwarebescherming	Gebruik van antivirus- en antimalwaresoftware op alle systemen die persoonsgegevens verwerken.	Regelmatige updates en scans volgens vastgesteld beleid.	j/n
Back-up en herstel	Regelmatige back-ups van persoonsgegevens en testprocedures voor gegevensherstel.	Dagelijkse back-ups met een bewaartermijn van 30 dagen; maandelijkse hersteltests.	j/n
Beveiliging van netwerken	Bescherming van netwerken tegen ongeautoriseerde toegang en bedreigingen.	Gebruik van firewalls, intrusion detection/prevention systems (IDS/IPS).	j/n
Beveiliging van fysieke toegang	Beperking van fysieke toegang tot systemen en gegevensdragers.	Toegangscontrole tot serverruimtes, gebruik van beveiligde kasten voor gegevensdragers.	j/n
Aanvullende eigen technische beveiligingsmaatregelen			

c. Organisatorische Beveiligingsmaatregelen

Maatregel	Beschrijving	Toelichting/Details	Toegepast
Beveiligingsbeleid	Formeel beleid dat de aanpak van informatiebeveiliging binnen de organisatie beschrijft.	Beleid wordt jaarlijks herzien en goedgekeurd door het management.	j/n
Toegangsbeheerbeleid	Procedures voor het toekennen, wijzigen en intrekken van toegangsrechten tot systemen en gegevens.	Toegangsrechten worden minimaal jaarlijks geëvalueerd.	j/n
Training en Bewustwording	Voorlichting over gegevensbescherming en beveiligingspraktijken.	Jaarlijkse verplichte AVG-training voor alle medewerkers.	j/n
Incidentresponsplan	Procedures voor het identificeren, melden en afhandelen van beveiligingsincidenten.	Incidenten worden binnen 24 uur gemeld aan de verantwoordelijke functionaris.	j/n
Beheer van leveranciers en subverwerkers	Beoordeling en monitoring van derden die persoonsgegevens verwerken namens de organisatie.	Subverwerkers zijn contractueel verplicht tot naleving van beveiligingsmaatregelen.	j/n
Beleid voor gegevensverwijdering	Procedures voor het veilig verwijderen of anonimiseren van persoonsgegevens die niet langer nodig zijn.	Gegevens worden na afloop van de bewaartermijn veilig verwijderd volgens vastgesteld beleid.	j/n
Aanvullende eigen organisatorische beveiligingsmaatregelen			

Bijlage 3: Procedure Datalekken

Een datalek moet, volgend deze Verwerkersovereenkomst, telefonisch gemeld worden bij de kwaliteitsmanager of directieverantwoordelijke en bovendien via het e-mailadres: kwaliteit@pthgroep.nl

Minimale informatie bij melding datalek

*Deze gegevens **moet** de Verwerker onverwijld verstrekken aan de Verwerkingsverantwoordelijke.*

Onderdeel	Toelichting / Invulveld
Datum en tijdstip ontdekking	
Datum en tijdstip incident (indien anders)	
Aard van het datalek	*Bijv. verlies, onbevoegde toegang, vernietiging, etc.*
Soorten persoonsgegevens	*Bijv. NAW-gegevens, medische data, logingegevens, etc.*
Categorieën van betrokkenen	*Bijv. klanten, medewerkers, studenten, etc.*
Aantal betrokkenen (indien bekend)	*Invullen of inschatting geven*
Waarschijnlijke gevolgen	*Bijv. identiteitsdiefstal, financiële schade, reputatieverlies*
Reeds genomen maatregelen	*Bijv. toegang geblokkeerd, wachtwoorden gereset, meldplicht intern geactiveerd*
Contactpersoon voor nadere informatie	*Naam:* *E-mail:* *Tel:*

Aanvullende informatie

Deze gegevens zijn aanvullend gewenst om de beoordeling en opvolging volledig te maken.
Ze hoeven niet onverwijld verstrekt worden en mogen binnen 48 uur volgend op de initiële melding doorgegeven worden.

Onderdeel	Toelichting / Invulveld
Hoe werd het datalek ontdekt?	*Bijv. via monitoring, melding medewerker, klantmelding, externe melding*
Wie heeft het incident gemeld?	*Naam + rol of afdeling*
Welke gegevens betreft het?	*Bijv. naam, e-mailadres, telefoonnummer*
Bevat het datalek extra gevoelige gegevens?	*Bijv. medische gegevens, strafrechtelijke gegevens, financiële gegevens, inloggegevens*
Zijn derden betrokken (sub-verwerkers of leveranciers)?	*Naam + rol + eventuele maatregelen die zij hebben genomen*
Technische oorzaak (indien bekend)	*Bijv. systeemfout, configuratiefout, hack, menselijke fout, phishing*
Wordt externe forensische ondersteuning ingezet?	*Ja/Nee + naam partij indien van toepassing*
Documentatie beschikbaar?	*Bijv. incidentrapport, screenshots, logbestanden – ja/nee/bijgevoegd*
Communicatie intern gestart?	*Bijv. CISO, Functionaris Gegevensbescherming geïnformeerd – ja/nee*
Al getroffen maatregelen?	*Geef aan of het datalek gestopt is; welke maatregelen correctief genomen zijn om dat te stoppen, welke maatregelen genomen zijn om de gevolgen te beheersen of te beperken en welke correctieve maatregelen getroffen zijn (of worden) om een soortgelijk datalek in de toekomst te voorkomen.*