

Verwerkersovereenkomst

DesignHypotheek - SiteVandaag

2018

Woerden, 3 mei 2018

Inhoud

Inhoud.....	2
Artikel 1. Begrippen.....	3
Artikel 2. Voorwerp van deze Verwerkersovereenkomst	4
Artikel 3. Inwerkingtreding en duur	4
Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer.....	4
Artikel 5. Beveiliging van de Verwerking	5
Artikel 6. Geheimhouding	5
Artikel 7. Adviseurs, Onderaannemers en Subverwerkers	6
Artikel 8. Bijstand vanwege rechten van Betrokkene.....	6
Artikel 9. Inbreuk in verband met Persoonsgegevens.....	6
Artikel 10. Terugbezorgen of wissen Persoonsgegevens	6
Artikel 11. Informatieverplichting en audit.....	7
Artikel 12. Toepasselijk recht.....	7
Artikel 13. Aansprakelijkheid	7
Bijlage 1. De Verwerking van Persoonsgegevens	8
Bijlage 2. Passende technische en organisatorische maatregelen.....	9
Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens.....	11
Bijlage 4: Overzicht subverwerkers en onderaannemers.....	12

Verwerkersovereenkomst

De ondergetekenden:

1. DesignHypotheek, maatschap, gevestigd te Schildwolde en geregistreerd bij de Kamer van Koophandel onder nummer 67645135, hierna te noemen Opdrachtgever,

en

2. SiteVandaag (ook bekend onder de handelsnamen: Pelatis Innovatie en IBAQ), maatschap, gevestigd te Woerden en geregistreerd bij de Kamer van Koophandel onder nummer 63618141, hierna te noemen: Opdrachtnemer,

hierna gezamenlijk te noemen: Partijen;

OVERWEGENDE DAT:

- voor zover Opdrachtnemer Persoonsgegevens Verwerkt ten behoeve van Opdrachtgever in het kader van de Overeenkomst, Opdrachtgever krachtens artikel 4, onderdeel 7 en onderdeel 8, van de Verordening kwalificeert als verwerkingsverantwoordelijke voor de Verwerking van Persoonsgegevens en Opdrachtnemer als verwerker;
- Partijen in deze Verwerkersovereenkomst, zoals bedoeld in artikel 28, derde lid, van de Verordening, hun afspraken over de Verwerking van Persoonsgegevens door Opdrachtnemer wensen vast te leggen.

KOMEN OVEREEN:

Artikel 1. Begrippen

In deze Verwerkersovereenkomst wordt een aantal begrippen met een beginhoofdletter gebruikt:

1.1 Betrokkene: degene op wie een Persoonsgegeven betrekking heeft.

1.2 Inbreuk in verband met Persoonsgegevens: een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

1.3 Overeenkomst: de overeenkomst tussen Opdrachtgever en Opdrachtnemer [titel] van [datum], met kenmerk [kenmerk].

1.4 Persoonsgegevens: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Opdrachtnemer in het kader van de Overeenkomst ten behoeve van Opdrachtgever verwerkt.

1.5 TOMs: technische en organisatorische maatregelen.

1.6 Verordening: Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van de Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.7 Verwerkersovereenkomst: deze overeenkomst inclusief overwegingen en bijbehorende bijlagen.

1.8 Verwerking: een bewerking of een geheel van bewerkingen in het kader van de Overeenkomst met betrekking tot Persoonsgegevens, of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen.

1.9 Webapplicatie: het online softwareproduct (website of webwinkel) waarin vastlegging en beheer van (Persoons-)gegevens van klanten van de Opdrachtgever plaatsvindt ten behoeve van de verkoop van producten of diensten van de Opdrachtgever.

Artikel 2. Voorwerp van deze Verwerkersovereenkomst

2.1 Deze Verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Opdrachtnemer in het kader van de Overeenkomst.

2.2 De aard en het doel van de Verwerking, het soort Persoonsgegevens en de categorieën van Persoonsgegevens, Betrokkenen en ontvangers zijn in Bijlage 1 omschreven.

2.3 Opdrachtnemer garandeert de toepassing van passende technische en organisatorische maatregelen (TOMs), opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.

2.4 Opdrachtnemer garandeert te voldoen aan de vereisten van de toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

Artikel 3. Inwerkingtreding en duur

3.1 Deze Verwerkersovereenkomst treedt in werking op het moment waarop deze door Partijen is ondertekend.

3.2 Deze Verwerkersovereenkomst eindigt nadat en voor zover Opdrachtnemer alle Persoonsgegevens overeenkomstig artikel 10 heeft gewist of terugbezorgd.

3.3 Geen van Partijen kan deze Verwerkersovereenkomst tussentijds opzeggen.

Artikel 4. Omvang verwerkingsbevoegdheid Opdrachtnemer

4.1 Opdrachtnemer Verwerkt de Persoonsgegevens uitsluitend in opdracht en op basis van schriftelijke instructies van Opdrachtgever behoudens afwijkende wettelijke voorschriften die op Opdrachtnemer van toepassing zijn.

4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Opdrachtnemer in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Opdrachtgever daarvan voorafgaand aan de Verwerking in kennis, tenzij een wettelijk voorschrift deze kennisgeving verbiedt.

4.3 Indien Opdrachtnemer op grond van een wettelijk voorschrift Persoonsgegevens dient te verstrekken, informeert hij Opdrachtgever onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.

4.4 Opdrachtnemer heeft geen zeggenschap over het doel van en de middelen voor de Verwerking van Persoonsgegevens.

Artikel 5. Beveiliging van de Verwerking

5.1 De Opdrachtnemer neemt passende technische en organisatorische maatregelen voor de beveiliging van Persoonsgegevens binnen haar producten, zowel met betrekking tot de verwerking door Opdrachtgever als door de Opdrachtnemer. Deze beveiliging van Persoonsgegevens is in verhouding tot de verantwoordelijkheid van de Opdrachtnemer ten aanzien van het risico voor de Betrokkenen, zoals beschreven in Bijlage 2.

5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Opdrachtnemer waarborgt een op het risico afgestemd beveiligingsniveau.

5.3 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer aanvullende maatregelen treffen met het oog op de beveiliging van de Persoonsgegevens.

5.4 Opdrachtnemer Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk schriftelijk toestemming heeft verkregen van Opdrachtgever en behoudens afwijkende wettelijke verplichtingen.

5.5 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging zodra hij kennis heeft genomen van onrechtmatige Verwerkingen van Persoonsgegevens of inbreuken op beveiligingsmaatregelen zoals genoemd in het eerste en tweede lid.

5.6 Opdrachtnemer verleent Opdrachtgever bijstand bij het doen nakomen van de verplichtingen uit hoofde van de artikelen 32 tot en met 36 van de Verordening.

5.7 Opdrachtgever stemt ermee in dat deze TOMs een passende beveiliging vormen van de Webapplicatie.

5.8 Opdrachtgever erkent dat TOMs als gevolg van technische vooruitgang en innovatie kunnen veranderen om aan beveiligingseisen te blijven voldoen. Opdrachtnemer behoudt zich het recht voor om TOMs zonder kennisgeving te wijzigen, zolang deze wijzigingen niet leiden tot een verminderd beveiligingsniveau.

5.9 Opdrachtgever erkent dat er een inherent beveiligingsrisico zit aan het werken met online software en dat er voor een gepaste beveiliging derhalve ook grote verantwoordelijkheid rust op de Opdrachtgever. Met name met aanzien van het vertrouwelijk behandelen van inloggegevens en het updaten van de door Opdrachtgever gehanteerde systemen van andere partijen (bijvoorbeeld internetbrowser, besturingssystemen, automatisch opslaan van wachtwoorden, etc.).

Artikel 6. Geheimhouding

6.1 Beide partijen garanderen dat Persoonsgegevens en andere gegevens die Opdrachtnemer op grond van deze Verwerkersovereenkomst ontvangt, te allen tijde vertrouwelijk en met de grootste voorzorg behandeld worden.

6.2 Zowel Opdrachtnemer als Opdrachtgever zullen eventuele werknemers, adviseurs en onderaannemers die zich bezighouden met de verwerking van Persoonsgegevens volgens deze overeenkomst, op de hoogte stellen van de vertrouwelijke aard van deze gegevens.

6.3 Beëindiging van de Gebruiksovereenkomst ontslaat Opdrachtnemer en Opdrachtgever niet van de geheimhouding en/of vertrouwelijkheid ten aanzien van Persoonsgegevens zoals hier beschreven.

Artikel 7. Adviseurs, Onderaannemers en Subverwerkers

7.1 Opdrachtnemer mag adviseurs, onderaannemers en Subverwerkers inschakelen voor de Verwerking van Persoonsgegevens. Bijlage C bevat een overzicht van de reeds door Opdrachtnemer ingeschakelde Subverwerkers. Indien Opdrachtnemer deze Subverwerkers vervangt of nieuwe Subverwerkers toevoegt, stelt Opdrachtnemer Opdrachtgever hiervan op de hoogte. Opdrachtgever krijgt de mogelijkheid tegen het gebruik van specifieke Subverwerkers bezwaar te maken. Opdrachtnemer zal Opdrachtgever op verzoek inzage verlenen in de lijst met Subverwerkers.

7.2 De door Opdrachtnemer ingeschakelde Subverwerkers zullen de Persoonsgegevens enkel verwerken volgens de instructies van Opdrachtnemer en Opdrachtgever. De Subverwerkers verwerken de Persoonsgegevens niet voor hun eigen doeleinden.

7.3 Zowel Opdrachtgever als Opdrachtnemer zullen adviseurs, onderaannemers en Subverwerkers aan dezelfde contractuele verplichtingen houden zoals deze bestaan in de Gebruiksovereenkomst overeengekomen tussen Opdrachtgever en Opdrachtnemer.

Artikel 8. Bijstand vanwege rechten van Betrokkene

8.1 Opdrachtnemer verleent Opdrachtgever bijstand bij het vervullen van diens plicht om verzoeken om uitoefening van de in hoofdstuk III van de Verordening vastgelegde rechten van de Betrokkene te beantwoorden.

Artikel 9. Inbreuk in verband met Persoonsgegevens

9.1 Opdrachtnemer informeert Opdrachtgever zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens, overeenkomstig de afspraken zoals vastgelegd in Bijlage 3.

9.2 Opdrachtnemer informeert Opdrachtgever ook na een melding op grond van het eerste lid over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.

9.3 Partijen dragen elk de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

Artikel 10. Terugbezorgen of wissen Persoonsgegevens

10.1 Na afloop van de Gebruiksovereenkomst en deze Verwerkersovereenkomst zal opdrachtnemer de door Opdrachtgever verstrekte (Persoons-)gegevens voor de periode van 1 maand bewaren. Binnen deze termijn kan Opdrachtgever Opdrachtnemer verzoeken tot het retourneren van door Opdrachtgever verzamelde (Persoons-)gegevens. Voor zover deze gegevens toebehoren aan Opdrachtgever en deze niet afkomstig zijn uit webapplicatie, zal Opdrachtnemer deze gegevens retourneren. Als deze termijn verstreken is, zal Opdrachtnemer deze gegevens en alle kopieën daarvan direct en definitief verwijderen, tenzij toepasselijk recht anders voorschrijft.

10.1 Na afloop van de Overeenkomst draagt Opdrachtnemer, naar gelang de keuze van Opdrachtgever, zorg voor het terugbezorgen aan Opdrachtgever of het wissen van alle Persoonsgegevens. Opdrachtnemer verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.

10.3 Mocht Opdrachtnemer om welke reden dan ook niet tot de volledige teruggave en/of verwijdering van Persoonsgegevens van Opdrachtgever in staat zijn, dan zal zij Opdrachtgever hiervan op de hoogte brengen. Opdrachtnemer is hiervoor op geen enkele manier aansprakelijk.

Artikel 11. Informatieverplichting en audit

11.1 Opdrachtnemer stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze Verwerkersovereenkomst zijn en worden nagekomen.

11.2 Opdrachtnemer verleent alle benodigde medewerking aan audits.

11.3 De kosten voor een audit worden gedragen door de Opdrachtgever.

Artikel 12. Toepasselijk recht

12.1 Opdrachtnemer zal voldoen aan de Relevante Wetgeving, voor zover de verplichtingen zich rechtstreeks tot Verwerkers richten.

12.2 Op deze Verwerkersovereenkomst is uitsluitend het Nederlands recht van toepassing.

12.3 Geschillen tussen Opdrachtnemer en Opdrachtgever die ontstaan in verband met deze Verwerkersovereenkomst zullen worden voorgelegd aan een bevoegde rechter.

Artikel 13. Aansprakelijkheid

13.1 Opdrachtnemer zal Opdrachtgever vrijwaren voor alle schade waar Opdrachtnemer als Verwerker voor aansprakelijk is, tot maximaal het bedrag waarvoor Opdrachtnemer verzekerd is.

13.2 Opdrachtnemer is enkel aansprakelijk voor schade die is ontstaan door (1) het niet naleven van de wettelijke verplichtingen in de Relevante Wetgeving die zich rechtstreeks tot Verwerkers richten, of (2) het niet naleven van de afspraken met Opdrachtgever zoals vastgelegd in deze Verwerkersovereenkomst;

13.3 Opdrachtnemer is niet aansprakelijk voor schade die is ontstaan uit het volgen van de instructies van Opdrachtgever, indien deze instructies in strijd met de Relevante Wetgeving of anderszins onrechtmatig zijn.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

Groningen, [3 mei]

Woerden, 3 mei 2018

Namens de Opdrachtgever:
L. Janszen

Namens de Opdrachtnemer:
W.G.F. Janszen

Bijlage 1. De Verwerking van Persoonsgegevens

In deze bijlage moet in ieder geval het volgende worden gespecificeerd:

Het onderwerp/aard en doel van de Verwerking	Tijdelijk en vaste klanten van en binnen de Webapplicatie "DesignHypotheek.nl" en "Checkrente.nl". Betreft: vastlegging van persoonsgegevens om financiële dienstverlening aan de betreffende klant te kunnen uitvoeren.
Het soort Persoonsgegevens	"Gewone persoonsgegevens"
Beschrijving categorieën Persoonsgegevens	"Gewone persoonsgegevens": Voornaam, achternaam, bedrijfsnaam, adres, postcode, plaats, land, telefoonnummer, emailadres, ip-adres, bankrekeningnummer.
Beschrijving categorieën Betrokkenen	Beheerder Webapplicatie: De Opdrachtnemer
Beschrijving categorieën ontvangers van Persoonsgegevens	DesignHypotheek, te Schildwolde

Voor de inhoud van deze bijlage kan onder meer gebruik worden gemaakt van de registratie die de Verwerkingsverantwoordelijke op grond van artikel 30 van de Verordening dient aan te houden.

Bijlage 2. Passende technische en organisatorische maatregelen

Hier volgt een puntsgewijs overzicht van de Technische en Organisatorische Beveiligingsmaatregelen die Opdrachtnemer neemt in het licht van de Verwerking van Persoonsgegevens. De maatregelen zijn te allen tijde afgestemd op het risico voor alle Betrokkenen. In willekeurige volgorde:

ARTIKEL B1 HOSTING & FIREWALLS

- a. Opdrachtnemer gebruikt een Virtual Private Server provider voor het hosten van applicaties en databases. De provider hiervan neemt adequate beveiligingsmaatregelen.
- b. Op alle individuele hosts wordt gebruik gemaakt van een firewall om ongeautoriseerde toegang tot persoonlijke data te voorkomen.
- c. Op alle hosts wordt intrusion prevention methodieken toegepast om brute-force aanvallen tegen te gaan.
- d. Opdrachtnemer gebruikt een externe opslagdienst voor het opslaan van Opdrachtgeversbestanden. Deze dienst bevindt zich binnen de EU en neemt adequate beveiligingsmaatregelen.
- e. Opdrachtnemer past "system hardening" toe op alle hosts. Dit bestaat uit sterke wachtwoord-authenticatie, het verwijderen van ongebruikte accounts, het uitschakelen van ongebruikte ports en log-management.
- f. Alle hosting (inclusief externe diensten) bevinden zich binnen de EU en vallen onder de AVG.

ARTIKEL B2 BEHEER VAN INCIDENTEN

- a. Opdrachtnemer hanteert protocollen en organisatorische maatregelen ten behoeve van incidentenbeheer.
- b. In geval van een beveiligingsincident is het mogelijk om gegevens te herstellen.

ARTIKEL B3 BACK-UPS & HERSTEL VAN GEGEVENS

- a. Er wordt elke dag een volledige back-up gemaakt van alle databases.
- b. Back-ups worden opgeslagen bij een externe opslagdienst.

ARTIKEL B4 CHANGE MANAGEMENT & DOCUMENTATIE

- a. Opdrachtnemer gebruikt change management processen voor alle systeemonderdelen die persoonlijke data verwerken.
- b. Opdrachtnemer onderhoud documentatie over systeemarchitectuur, relevante processen en de beveiliging van systemen.
- c. Opdrachtnemer verzamelt geautomatiseerde logs op systeemactiviteiten van alle medewerkers van Opdrachtnemer die toegang hebben tot Persoonsgegevens.

ARTIKEL B5 PATCH MANAGEMENT

- a. Patch management wordt uitgevoerd op hosts en applicaties die persoonlijke data verwerken;
- b. Opdrachtnemer zal relevante patches ten aanzien van de beveiliging van systemen, wanneer technisch mogelijk, binnen 30 dagen na kennisneming toepassen.

ARTIKEL B6 AUTHENTICATIE & AUTORISATIE

- a. Opdrachtnemer hanteert een restrictieve toegang tot systemen op basis van het "least privilege principle".
- b. Toegang tot de Webapplicatie is uitsluitend mogelijk met een unieke combinatie van inlognaam en wachtwoord (dat aan enkele specifieke eisen moet voldoen).
- c. Toegang tot systemen en beheerde data is uitsluitend mogelijk met public key infrastructure (PKI).

ARTIKEL B7 VERSLEUTELING

- a. De opgeslagen back-ups worden versleuteld. Ook de communicatie tussen hosts bij het verplaatsen van back-ups is versleuteld.
- b. Dataverkeer met persoonlijke gegevens is versleuteld.

ARTIKEL B8 ORGANISATORISCHE MAATREGELEN

- a. Opdrachtnemer draagt er zorg voor dat alle medewerkers op de hoogte zijn van het gehanteerde beveiligingsbeleid.
- b. Voor medewerkers met toegang tot Persoonsgegevens wordt een interne "code of conduct" gehanteerd om hen te wijzen op de vertrouwelijke aard van het werk. Ook vinden er periodiek trainingen plaats op het gebied van privacy en Persoonsgegevens.
- c. In de arbeidsovereenkomst van Opdrachtnemer met haar personeel is een geheimhoudingsclausule opgenomen. Ook onderaannemers en adviseurs worden ten aanzien van privacy en bescherming van Persoonsgegevens aan dezelfde contractuele bepaling gehouden.
- d. Er zijn voldoende voorzieningen getroffen voor de fysieke beveiliging van de werkplek.

Bijlage 3: Afspraken betreffende Inbreuken in verband met Persoonsgegevens

In deze bijlage moeten de afspraken over hoe Opdrachtnemer Opdrachtgever over Inbreuken in verband met Persoonsgegevens gaat informeren worden gespecificeerd.

B3.1 Opdrachtnemer informeert Opdrachtgever over hoe, wat en wanneer van de inbreuk, welke (Persoons-)gegevens zijn geraakt.

B3.2 Opdrachtnemer adviseert Opdrachtgever welke (tegen-)maatregelen er genomen moeten worden om eventuele schade door de inbreuk te doen verminderen cq in de toekomst kan worden voorkomen.

Informatie die tenminste door Opdrachtnemer moet worden verstrekt:

Aard van de Inbreuk in verband met Persoonsgegevens
De Persoonsgegevens en Betrokkene
Waarschijnlijke gevolgen van de Inbreuk in verband met Persoonsgegevens
Maatregelen die Opdrachtnemer heeft voorgesteld of genomen om de Inbreuk in verband met Persoonsgegevens aan te pakken, waaronder, in voorkomend geval, de maatregelen ter beperking van de eventuele nadelige gevolgen daarvan

Bijlage 4: Overzicht subverwerkers en onderaannemers

De subverwerkers en onderaannemers die binnen de Webapplicatie van de Opdrachtgever mogelijk Persoonsgegevens verwerken, zijn (A-Z):

1. TransIP B.V. | Hostingbedrijf, gebruikt voor het hosten van de Webapplicatie en bijbehorende Persoonsgegevens. Locatie EU (Nederland);
2. Google | Analytics, gebruikt voor het analyseren van geanonimiseerd bezoek van de site (qua aantallen, gedrag in volgorde bezoek pagina's, devices). Locatie EU (Ierland)
3. Google | MijnBedrijf, gebruikt voor het achterlaten van reviews door klanten
4. Google | Adwords, gebruikt voor advertenties ter verhoging naamsbekendheid en aangeboden dienstenassortiment (niet toegesneden op individu). Locatie EU (Ierland)
5. Facebook | Facebook, gebruikt voor het achterlaten van reviews door klanten. Locatie USA