

Verwerkersovereenkomst

INTRAMED ONLINE

April 2018

INLEIDING

Dit document vormt de verwerkersovereenkomst voor Convenient OnLine BV Producten en Diensten. In deze verwerkersovereenkomst leggen de Partijen vast wat over en weer de rechten, plichten, rollen en verantwoordelijkheden zijn met betrekking tot het veilig en rechtmatig Verwerken van Persoonsgegevens in het kader van de verstrekking van Convenient OnLine BV Producten en Diensten. De Partijen geven met deze verwerkersovereenkomst invulling aan hun verplichtingen onder de Algemene Verordening Gegevensbescherming (AVG).

ARTIKEL 1: DEFINITIES

De in dit document met een beginhoofdletter geschreven termen kennen dezelfde definities als in de gebruiksovereenkomst, tenzij en voor zover daar in dit document uitdrukkelijk van is afgeweken.

Hieronder is een lijst met aanvullende definities opgenomen.

Betrokkene	degene op wie een Persoonsgegeven betrekking heeft.
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.
Persoonsgegevens	alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon, die Convenient OnLine BV in het kader van de overeenkomst ten behoeve van Klant verwerkt.
Subverwerker	de Partij die door Verwerker wordt ingeschakeld als Verwerker ten behoeve van de Verwerking van de Persoonsgegevens in het kader van deze verwerkersovereenkomst en de gebruiksovereenkomst
Verwerken	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.
Verwerker	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van de Verwerkingsverantwoordelijke Persoonsgegevens verwerkt; hierna te noemen Convenient OnLine BV.
Verwerkings-verantwoordelijke	een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt; wanneer de doelstellingen van en de middelen voor deze Verwerking in het Unierecht of het lidstatelijk recht worden vastgesteld, kan daarin

worden bepaald wie de Verwerkingsverantwoordelijke is of volgens welke criteria deze wordt aangewezen; hierna te noemen Klant.

ARTIKEL 2: ROLLEN EN VERANTWOORDELIJKHEDEN

- 2.1 Partijen erkennen dat Convenient OnLine BV in haar Producten en Diensten Persoonsgegevens zal Verwerken waar Klant volgens de Verordening de Verwerkersverantwoordelijke voor is. Naar opvatting van de Partijen vormt Convenient OnLine BV daarbij de Verwerker.
- 2.2 Deze verwerkersovereenkomst regelt de Verwerking van Persoonsgegevens door Convenient OnLine BV.
- 2.3 Convenient OnLine BV garandeert de toepassing van passende technische en organisatorische maatregelen, opdat de Verwerking aan de vereisten van de Verordening voldoet en de bescherming van de rechten van de Betrokkene is gewaarborgd.
- 2.4 Verwerker en Verantwoordelijke zullen ieder zorgdragen voor de naleving van de op hen van toepassing zijnde wet- en regelgeving, waaronder in ieder geval begrepen de wet- en regelgeving op het gebied van de bescherming van Persoonsgegevens, zoals de AVG.

ARTIKEL 3: LOOPTIJD

- 3.1 De verwerkersovereenkomst kent dezelfde looptijd als de Intramed OnLine gebruiksovereenkomst.
- 3.2 Deze verwerkersovereenkomst is van kracht voor zolang als Verwerker (toegang tot) Persoonsgegevens heeft in het kader van de levering van Producten of Diensten aan Verantwoordelijke. Deze verwerkersovereenkomst kan slechts eindigen wanneer Verwerker geen Persoonsgegevens van Verantwoordelijke meer bezit.
- 3.3 Geen van Partijen kan deze verwerkersovereenkomst tussentijds opzeggen.

ARTIKEL 4: VERWERKINGSBEVOEGDHEID CONVENIENT ONLINE BV

- 4.1 Convenient OnLine BV Verwerkt de Persoonsgegevens uitsluitend in opdracht van en op basis van Schriftelijke instructies van Klant behoudens afwijkende wettelijke voorschriften die op Convenient OnLine BV van toepassing zijn.
- 4.2 Indien een instructie als bedoeld in het eerste lid naar het oordeel van Convenient OnLine BV in strijd is met een wettelijk voorschrift inzake gegevensbescherming, stelt hij Klant daarvan voorafgaand aan de Verwerking in kennis.
- 4.3 Indien Convenient OnLine BV op grond van een wettelijke verplichting Persoonsgegevens dient te verstrekken, informeert hij Klant onmiddellijk, en zo mogelijk voorafgaand aan de verstrekking.
- 4.4 Convenient OnLine BV heeft geen zeggenschap over het doel van de Verwerking van Persoonsgegevens.

ARTIKEL 5: BEVEILIGING VAN DE VERWERKING

- 5.1 Partijen zullen gezamenlijk zorg dragen voor een passend beveiligingsniveau voor de Verwerkte Persoonsgegevens. Klant draagt daarbij als Verantwoordelijke de hoofdverantwoordelijkheid.
- 5.2 Partijen erkennen dat het waarborgen van een passend beveiligingsniveau voortdurend kan dwingen tot het treffen van aanvullende beveiligingsmaatregelen. Convenient OnLine BV waarborgt een op het risico afgestemd beveiligingsniveau.
- 5.3 Convenient OnLine BV Verwerkt Persoonsgegevens niet buiten de Europese Unie, tenzij hij daarvoor uitdrukkelijk Schriftelijk toestemming heeft verkregen van Klant en behoudens afwijkende wettelijke verplichtingen.
- 5.4 Convenient OnLine BV verleent Klant bijstand bij het doen nakomen van de verplichtingen te weten: beveiliging, melding van datalekken en gegevens effect beoordeling (Data Protect Impact Assessment).
- 5.5 Convenient OnLine BV zal indien daar aanleiding toe is Klant op de hoogte stellen van de beveiligingsmaatregelen die zij en haar Subverwerkers nemen en om die maatregelen correct ten uitvoer te (doen) brengen.
- 5.6 Klant heeft tot de taak om zich ervan te vergewissen dat de technische en organisatorische beveiligingsmaatregelen die van toepassing zijn op de Producten en/of Diensten, passend zijn gelet op de risico's die de Verwerkingen en de aard van de Persoonsgegevens met zich meebrengen, de kosten en de stand der techniek.
- 5.7 Klant verklaart na ondertekening van het Aanvraagformulier dat de bijbehorende gebruiksovereenkomst, service level agreement en verwerkersovereenkomst van toepassing zijn. Klant vrijwaart Convenient OnLine BV tegen aanspraken van derden die gebaseerd zijn op de stelling dat de maatregelen zoals beschreven in de gebruiksovereenkomst, service level agreement en verwerkersovereenkomst, mits correct nageleefd, niet passend zouden zijn.
- 5.8 Klant staat ervoor in dat hij alleen op geheel rechtmatige wijze Persoonsgegevens in zal voeren in de systemen van Convenient OnLine BV of anderszins ter beschikking zal stellen aan Convenient OnLine BV.
- 5.9 Convenient OnLine BV staat er voor in dat een ieder die handelt onder het gezag van Convenient OnLine BV , voor zover deze toegang heeft tot Persoonsgegevens waar Klant de verantwoordelijke voor is, deze slechts verwerkt in overeenstemming met de overeengekomen beveiligingsmaatregelen en in opdracht van Klant, behoudens afwijkende wettelijke verplichtingen.

ARTIKEL 6: GEHEIMHOUDING

- 6.1 De Persoonsgegevens hebben een Vertrouwelijk karakter.
- 6.2 Alle medewerkers van Convenient OnLine BV die gemachtigd zijn tot het Verwerken van Persoonsgegevens hebben zich ertoe verbonden geheimhouding in acht te nemen.

ARTIKEL 7: SUBVERWERKER

- 7.1 Wanneer Convenient OnLine BV, een andere Verwerker inschakelt om ten behoeve van Klant verwerkingsactiviteiten te verrichten, worden aan deze andere Verwerker bij een overeenkomst dezelfde verplichtingen inzake gegevensbescherming opgelegd als die welke in deze verwerkersovereenkomst zijn opgenomen.
- 7.2 Convenient OnLine BV zal geen nieuwe Subverwerkers gegevens laten Verwerken zonder Klant daarover via de nieuwsbrief tijdig te informeren. Klant kan, indien hij dat nodig acht, binnen 7 dagen na bekendmaking bezwaar maken bij Convenient OnLine BV tegen de Subverwerker. Bezwaar door Klant moet Schriftelijk en gemotiveerd worden ingediend bij Convenient OnLine BV.

ARTIKEL 8: BIJSTAND VANWEGE RECHTEN VAN BETROKKENE

- 8.1 Convenient OnLine BV verwijst Betrokkene indien deze een verzoek aan Convenient OnLine BV doet altijd door naar Klant.
- 8.2 Convenient OnLine BV stelt Klant in staat om te voldoen aan haar plichten volgens de Verordening, indien Betrokkene hun privacy rechten uitoefenen zoals het recht op inzage, correctie, gegevens wissen en dataportibiliteit.

ARTIKEL 9: INBREUK IN VERBAND MET PERSOONSgegevens/DATALEKKEN

- 9.1 Convenient OnLine BV informeert Klant zonder onredelijke vertraging, zodra hij kennis heeft genomen van een Inbreuk in verband met Persoonsgegevens.
- 9.2 Convenient OnLine BV informeert Klant ook na een melding op grond van het eerste lid van artikel 8 over ontwikkelingen betreffende de Inbreuk in verband met Persoonsgegevens.
- 9.3 Klant kan Convenient OnLine BV op de hoogte stellen van een mogelijk datalek door contact op te nemen met het service centrum van Intramed OnLine via 0182 - 621121 of via helpdesk@intramed.nl
- 9.4 Convenient OnLine BV en/of Klant dragen de door henzelf in verband met de melding aan de bevoegde toezichthoudende autoriteit en Betrokkene te maken kosten.

ARTIKEL 10: TERUGGAVE PERSOONSgegevens

- 10.1 Na afloop van de overeenkomst draagt Convenient OnLine BV, naar gelang de keuze van Klant, zorg voor het terugbezorgen aan Klant of het wissen van alle Persoonsgegevens. Convenient OnLine BV verwijdert kopieën, behoudens afwijkende wettelijke voorschriften.
- 10.2 Persoonsgegevens worden in de door Convenient OnLine BV aangegeven vorm en op de door Convenient OnLine BV aangegeven wijze afdoende beveiligd terugbezorgd in een gangbaar bestandsformat via een downloadlink of via een gangbare datadrager.

ARTIKEL 11: INFORMATIEPLICHT EN AUDIT

- 11.1 Convenient OnLine BV stelt alle informatie ter beschikking die nodig is om aan te tonen dat de verplichtingen uit deze verwerkersovereenkomst zijn en worden nagekomen.
- 11.2 De informatiebeveiliging van Convenient OnLine BV is gecertificeerd voor de normen ISO 27001 en NEN 7510. Deze certificaten zijn in te zien via onze website. Om deze certificeringen te behouden laat Convenient OnLine BV audits uitvoeren door een onafhankelijk terzake kundig auditbureau. Klant kan op verzoek inzage krijgen in de resultaten van deze externe audits.
- 11.3 Indien Klant daar ondanks de in artikel 10.2 genoemde certificering en audits aanleiding toe ziet, zal Convenient OnLine BV medewerking verlenen aan audits om te bepalen dat de gegevensverwerking voldoet aan de eisen van de AVG. Dergelijke audits kunnen maximaal één keer per jaar worden uitgevoerd door een onafhankelijke en terzake kundige partij. De kosten hiervan worden volledig gedragen door de Klant.
- 11.4 Convenient OnLine BV kan Klant op verzoek zijn medewerking verlenen als Klant een Data Protection Impact Assessment (DPIA) laat uitvoeren door inzicht te verschaffen in gegevensstromen en beveiligingsmaatregelen.

ANNEX A : VERWERKINGSREGISTER

Dit document is separaat verstrekt.

ANNEX B: BEVEILIGINGSMAATREGELEN

Dit document is separaat verstrekt.

Beveiligingsmaatregelen

INTRAMED

#	Onderwerp	Maatregel
1	Informatiebeveiliging- en privacybeleid	Er is een informatiebeveiligings- en privacybeleid dat voldoet aan de AVG en eventuele richtsnoeren van de Autoriteit Persoonsgegevens en aansluit op de standaarden voor informatiebeveiliging ISO 27001 en NEN 7510. Dit beleid is intern gecommuniceerd en concreet geïmplementeerd door middel van gedocumenteerde procedures.
2	Certificering	Er is een managementsysteem voor informatiebeveiliging (gecombineerd ISMS/DPMS). Dit managementsysteem is opgezet en ingericht conform de standaarden voor informatiebeveiliging ISO 27001 en NEN 7510. Het systeem is gecertificeerd door de onafhankelijke auditpartij BSI.
3	Access management	De principes van 'least privilege' en 'need-to-know' worden toegepast op personeel en toegestane Subverwerkers. Gebruikerstoegang wordt tijdig ingetrokken of gewijzigd bij enige verandering in de status van personeel, leveranciers, klanten, zakelijke partners of derden. Er wordt gebruik gemaakt van actuele en algemeen als veilig beschouwde vormen van versleuteling en encryptie ten behoeve van identificatie, authenticatie en autorisatie.
4	Personeel	Medewerkers worden geïnformeerd over hun verantwoordelijkheden m.b.t. privacy en informatiebeveiliging en er wordt erop toegezien dat zij hun verplichtingen nakomen. Medewerkers die toegang hebben tot patiëntgegevens zijn gebonden aan geheimhouding.
5	Contractmanagement (Sub)verwerkers	Met iedere toegestane (Sub)verwerker wordt een (sub)verwerkersovereenkomst gesloten, die de (Sub)verwerker contractueel verplicht tot nakoming van dezelfde verplichtingen in verband met de verwerking als in de verwerkersovereenkomst waar deze bijlage bij hoort.
6	Security incident & response	Er is een gedocumenteerd security incident response plan dat geschikt is om Datalekken te detecteren, op te lossen en te melden, in overeenstemming met de verplichtingen in deze verwerkersovereenkomst.
7	Vulnerability / patchmanagement	Er wordt periodiek beoordeeld of er kwetsbaarheden binnen de gebruikte applicaties, systemen en netwerken zijn. Patches en updates voor gevonden kwetsbaarheden worden doorgevoerd.

8	Netwerk- en systeembeveiliging	Er zijn maatregelen getroffen om malware en misbruik van het netwerk en de systemen tegen te gaan en te detecteren (zoals firewalls en antivirussoftware van betrouwbare leveranciers).
9	Fysieke toegangsbeveiliging	Er zijn passende maatregelen (zoals sloten, camera's, alarmsystemen) genomen om de ruimtes waarin de Persoonsgegevens kunnen worden verwerkt, te beveiligen tegen onbevoegde toegang.
10	Logging	Er vindt logging plaats waarmee inzicht wordt verkregen in welke gebruikers op welke momenten inloggen.
11	Locatie	Persoonsgegevens worden verwerkt binnen de grenzen van de Europese Unie.
12	Business continuity & disaster recovery	Er is beleid en er zijn procedures en processen geïmplementeerd om te waarborgen dat de geleverde Diensten of Producten en de verwerkte Persoonsgegevens beschikbaar blijven in geval van onvoorziene omstandigheden en rampen, dan wel zo snel mogelijk volledig worden hersteld.
13	Applicatieontwikkeling – beveiligingsprincipes	Er worden beveiligingsprincipes toegepast om informatiebeveiliging in applicatieontwikkeling te integreren.
14	Onafhankelijke controle	Externe audits, kwetsbaarheidsscans en penetratietests worden periodiek uitgevoerd op applicaties en netwerken om zwakheden en potentiële Datalekken te ontdekken.

Informatiebeveiliging in Intramed

30 augustus 2016 – We vinden het belangrijk dat al je gegevens veilig worden opgeslagen en verwerkt. Daarom hebben we ons managementsysteem voor informatiebeveiliging eind 2015 laten toetsen volgens de ISO 27001 en NEN 7510 normen. Als je met Intramed of Intramed OnLine werkt, kun je er dus op vertrouwen dat de informatiebeveiliging goed geregeld is.

Wat betekenen ISO 27001 en NEN 7510

Informatiebeveiliging wordt steeds belangrijker nu we steeds meer digitaal gaan werken. Dat geldt niet alleen voor de zorgsector, maar het is wel heel belangrijk dat patiëntdossiers niet zomaar 'op straat komen te liggen'.

Daarom hebben wij eind 2015 het [BSI](#) gevraagd om ons managementsysteem te toetsen volgens de ISO 27001 én NEN 7510 normen. ISO 27001 is dé internationale norm voor informatiebeveiliging en NEN 7510 richt zich specifiek op informatiebeveiliging in de gezondheidszorg.

Door te voldoen aan beide normen kunnen wij (en daarmee jij als praktijkhouder ook) waarborgen dat alle financiële en vertrouwelijke gegevens goed beveiligd zijn en de kans op onwettig of ongevoegde toegang tot een absoluut minimum beperkt is. Met behulp van de

NEN 7510 certificering hebben we het BSI gevraagd onze informatiebeveiliging ook specifiek te toetsen op het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van de patiëntinformatie.



Beter beveiligd kan bijna niet

Juist omdat wij informatiebeveiliging zo belangrijk vinden hebben wij het BSI gevraagd ons op beide normeringen te toetsen. Hiermee doen wij meer dan wettelijk noodzakelijk, want alleen voldoen aan NEN 7510 is voldoende. Maar door onszelf strengere eisen op te leggen, doen wij er alles aan om te waarborgen dat jij onbezorgd kunt werken met Intramed.

Ons managementsysteem stelt ons nu bijvoorbeeld in staat om risico's op het gebied van informatiebeveiliging in kaart te brengen en tijdig maatregelen te nemen om deze risico's te verkleinen. Daarnaast kunnen we ook monitoren of de beveiliging goed functioneert en incidenten als datalekken snel signaleren en direct actie ondernemen.

Certificaat ISO 27001

Certificaat NEN 7510