STANDAARD VERWERKERSOVEREENKOMST

Normveilig

Voor opdrachten waarin Normveilig persoonsgegevens verwerkt namens de opdrachtgever.

Toepassing

Deze standaard verwerkersovereenkomst geldt wanneer zij in een offerte, opdrachtbevestiging of andere hoofdovereenkomst van toepassing is verklaard. De juridische partijgegevens volgen uit die hoofdovereenkomst. Afwijkende of aanvullende afspraken worden in de hoofdovereenkomst of een projectspecifieke bijlage vastgelegd.

Partijen en rolverdeling

In deze verwerkersovereenkomst betekent “Opdrachtgever” de contractspartij die met Normveilig de hoofdovereenkomst aangaat en ten behoeve van wie persoonsgegevens worden verwerkt. “Normveilig” betekent de contractspartij die in de hoofdovereenkomst als Normveilig is aangeduid.

Opdrachtgever is voor de betreffende persoonsgegevens verwerkingsverantwoordelijke, of treedt zelf als verwerker op voor een derde. In dat laatste geval treedt Normveilig als subverwerker op. Partijen worden gezamenlijk aangeduid als “Partijen”.

Inhoud

1. Doel, toepasselijkheid en rangorde
2. Onderwerp en instructies
3. Geheimhouding en toegang
4. Beveiliging van persoonsgegevens
5. Subverwerkers
6. Rechten van betrokkenen
7. Bijstand aan opdrachtgever
8. Datalekken
9. Doorgifte buiten de EER
10. Informatie, audits en aantoonbaarheid
11. Teruggave en verwijdering
12. Aansprakelijkheid en kosten

13. Looptijd en beëindiging
14. Slotbepalingen
Bijlage 1 - Standaardomschrijving van de verwerking
Bijlage 2 - Technische en organisatorische maatregelen
Bijlage 3 - Subverwerkers en wijzigingen

1. Doel, toepasselijkheid en rangorde

Deze verwerkersovereenkomst geeft uitvoering aan artikel 28 van de Algemene verordening gegevensbescherming (AVG) voor zover Normveilig in het kader van de hoofdovereenkomst persoonsgegevens verwerkt ten behoeve van Opdrachtgever.

Deze verwerkersovereenkomst vormt één geheel met de hoofdovereenkomst. Bij tegenstrijdigheid over de bescherming of verwerking van persoonsgegevens gaat deze verwerkersovereenkomst voor, tenzij Partijen uitdrukkelijk schriftelijk anders overeenkomen en dit verenigbaar is met toepasselijke privacywetgeving.

De begrippen persoonsgegevens, verwerking, verwerkingsverantwoordelijke, verwerker, betrokkene, inbreuk in verband met persoonsgegevens en toezichthoudende autoriteit hebben de betekenis die de AVG daaraan geeft.

2. Onderwerp en instructies

Normveilig verwerkt persoonsgegevens uitsluitend voor de uitvoering van de overeengekomen dienstverlening en uitsluitend op gedocumenteerde instructies van Opdrachtgever. De standaardomschrijving van de verwerking staat in Bijlage 1. Een opdrachtbevestiging kan die omschrijving beperken, aanvullen of nader specificeren.

Normveilig verwerkt persoonsgegevens niet voor eigen, onverenigbare doeleinden en verstrekt persoonsgegevens niet aan derden, behalve voor de uitvoering van de opdracht, wanneer dit wettelijk verplicht is of wanneer Opdrachtgever daarvoor schriftelijk toestemming heeft gegeven.

Indien Normveilig van oordeel is dat een instructie in strijd is met de AVG of andere toepasselijke privacywetgeving, informeert Normveilig Opdrachtgever zonder onredelijke vertraging. Normveilig mag de betreffende instructie opschorten totdat Partijen duidelijkheid hebben verkregen.

Wanneer een wettelijke verplichting Normveilig tot een verwerking of doorgifte verplicht buiten de instructies van Opdrachtgever, informeert Normveilig Opdrachtgever vooraf, tenzij de wet dat verbiedt.

3. Geheimhouding en toegang

Normveilig beperkt toegang tot persoonsgegevens tot personen die deze toegang nodig hebben voor de overeengekomen werkzaamheden, op basis van need-to-know en least privilege.

Personen die onder het gezag van Normveilig persoonsgegevens verwerken zijn gebonden aan passende geheimhoudingsverplichtingen en ontvangen passende instructie over informatiebeveiliging en privacy.

Toegangsrechten worden toegekend, gewijzigd en ingetrokken volgens een beheerst proces en worden verwijderd zodra toegang niet langer noodzakelijk is.

4. Beveiliging van persoonsgegevens

Normveilig treft, rekening houdend met de stand van de techniek, uitvoeringskosten, aard, omvang, context en doeleinden van de verwerking en de risico's voor betrokkenen, passende technische en organisatorische maatregelen overeenkomstig artikel 32 AVG.

De basismaatregelen zijn opgenomen in Bijlage 2. Indien een concrete opdracht vanwege het risicoprofiel aanvullende maatregelen vereist, leggen Partijen die schriftelijk vast.

Normveilig beoordeelt de maatregelen periodiek en past deze waar redelijkerwijs nodig aan. Materiële wijzigingen die de overeengekomen verwerking wezenlijk beïnvloeden worden met Opdrachtgever afgestemd.

5. Subverwerkers

Opdrachtgever verleent Normveilig algemene schriftelijke toestemming om subverwerkers in te schakelen voor zover dit noodzakelijk is voor de dienstverlening.

Normveilig informeert Opdrachtgever vooraf over een voorgenomen toevoeging of vervanging van een subverwerker die persoonsgegevens van Opdrachtgever zal verwerken. Opdrachtgever kan binnen de meegedeelde redelijke termijn gemotiveerd bezwaar maken op privacy- of beveiligingsgronden.

Normveilig legt aan de subverwerker schriftelijk materieel dezelfde gegevensbeschermingsverplichtingen op als in deze verwerkersovereenkomst. Normveilig blijft tegenover Opdrachtgever verantwoordelijk voor de nakoming van de gegevensbeschermingsverplichtingen door de subverwerker.

6. Rechten van betrokkenen

Rekening houdend met de aard van de verwerking verleent Normveilig redelijke bijstand zodat Opdrachtgever kan voldoen aan verzoeken van betrokkenen, waaronder inzage, rectificatie, verwijdering, beperking, bezwaar en gegevensoverdraagbaarheid.

Ontvangt Normveilig rechtstreeks een verzoek van een betrokkene dat betrekking heeft op persoonsgegevens die namens Opdrachtgever worden verwerkt, dan stuurt Normveilig het verzoek zo spoedig mogelijk door naar Opdrachtgever. Normveilig reageert inhoudelijk alleen op instructie van Opdrachtgever, tenzij een wettelijke verplichting anders vereist.

7. Bijstand aan opdrachtgever

Normveilig verleent, rekening houdend met de aard van de verwerking en de informatie waarover Normveilig beschikt, redelijke bijstand bij het voldoen aan de artikelen 32 tot en met 36 AVG, waaronder beveiliging, beoordeling en melding van datalekken, gegevensbeschermingseffectbeoordelingen (DPIA) en eventuele voorafgaande raadpleging van de toezichthouder.

Normveilig verstrekt op verzoek relevante informatie over de getroffen maatregelen voor zover dit redelijkerwijs nodig is om naleving aan te tonen en geen vertrouwelijke informatie van andere klanten of onevenredige beveiligingsrisico's onthult.

8. Datalekken

Normveilig informeert Opdrachtgever zonder onredelijke vertraging nadat Normveilig kennis heeft genomen van een bevestigde of redelijkerwijs vermoede inbreuk in verband met persoonsgegevens die onder deze overeenkomst valt. Normveilig streeft naar een eerste melding binnen 24 uur na bevestiging van het incident.

De melding bevat, voor zover op dat moment beschikbaar, de aard van het incident, vermoedelijke categorieën en aantallen betrokkenen en gegevens, waarschijnlijke gevolgen, reeds genomen of voorgestelde maatregelen, relevante tijdstippen en een contactpunt. Ontbrekende informatie wordt gefaseerd aangevuld zodra deze beschikbaar komt.

Opdrachtgever blijft verantwoordelijk voor de beoordeling en eventuele melding aan de Autoriteit Persoonsgegevens en/of betrokkenen, tenzij toepasselijke wetgeving Normveilig rechtstreeks tot een melding verplicht. Normveilig werkt redelijkerwijs mee aan onderzoek, beperking en herstel.

9. Doorgifte buiten de EER

Normveilig verwerkt persoonsgegevens in beginsel binnen de Europese Economische Ruimte (EER). Indien verwerking of toegang vanuit een land buiten de EER noodzakelijk is, vindt dit alleen plaats op een geldige grondslag overeenkomstig hoofdstuk V AVG en, waar van toepassing, volgens de instructies van Opdrachtgever.

Waar vereist past Normveilig passende waarborgen toe, zoals de door de Europese Commissie vastgestelde standaardcontractbepalingen (SCC's), en worden waar nodig aanvullende technische en organisatorische maatregelen getroffen.

10. Informatie, audits en aantoonbaarheid

Normveilig stelt Opdrachtgever de informatie ter beschikking die redelijkerwijs noodzakelijk is om naleving van artikel 28 AVG aan te tonen.

Opdrachtgever mag maximaal eenmaal per kalenderjaar, en vaker bij een onderbouwd vermoeden van ernstige niet-naleving of na een materieel datalek, een audit laten uitvoeren. Partijen stemmen scope, timing, vertrouwelijkheid en wijze van uitvoering vooraf af zodat bedrijfsvoering en beveiliging van Normveilig en andere klanten niet onnodig worden verstoord.

Normveilig mag in eerste instantie relevante onafhankelijke audit-, assurance- of certificeringsinformatie verstrekken voor zover die de onderzoeksvraag voldoende afdekt. Een aanvullende audit vindt plaats indien deze informatie onvoldoende is. Redelijke externe auditkosten komen voor rekening van Opdrachtgever, tenzij de audit een materiële tekortkoming van Normveilig aantoont.

11. Teruggave en verwijdering

Na beëindiging van de dienstverlening verwijdert of retourneert Normveilig, naar keuze van Opdrachtgever, persoonsgegevens die namens Opdrachtgever zijn verwerkt en verwijdert Normveilig bestaande kopieën, tenzij een wettelijke bewaarplicht verdere opslag vereist.

Tenzij anders overeengekomen voert Normveilig verwijdering uit binnen 60 dagen na het einde van de opdracht of een geldig schriftelijk verwijderverzoek. Back-ups kunnen gedurende de normale back-upretentie blijven bestaan, mits deze afgeschermd blijven, niet voor andere doeleinden worden gebruikt en volgens de reguliere cyclus worden overschreven of vernietigd.

Verplichtingen die naar hun aard voortduren, waaronder geheimhouding en verplichtingen rond reeds ontstane datalekken, blijven na beëindiging van kracht.

12. Aansprakelijkheid en kosten

Voor aansprakelijkheid tussen Partijen geldt primair de aansprakelijkheidsregeling in de hoofdovereenkomst, voor zover deze niet strijdig is met dwingend recht of rechten van betrokkenen onder de AVG.

Normale bijstand die rechtstreeks samenhangt met de uitvoering van deze overeenkomst is inbegrepen voor zover zij redelijk is binnen de overeengekomen dienstverlening. Uitzonderlijke, omvangrijke of door Opdrachtgever veroorzaakte aanvullende werkzaamheden kunnen na voorafgaande afstemming op basis van de overeengekomen tarieven worden doorbelast.

13. Looptijd en beëindiging

Deze verwerkersovereenkomst treedt in werking zodra zij in de hoofdovereenkomst van toepassing is verklaard of zodra Normveilig feitelijk persoonsgegevens voor Opdrachtgever gaat verwerken, afhankelijk van wat eerder is.

De verwerkersovereenkomst eindigt wanneer Normveilig geen persoonsgegevens meer verwerkt ten behoeve van Opdrachtgever en aan de verplichtingen uit artikel 11 is voldaan. Zij kan niet los van de hoofdovereenkomst worden beëindigd zolang de verwerking voortduurt.

14. Slotbepalingen

Wijzigingen van deze verwerkersovereenkomst worden schriftelijk of elektronisch vastgelegd. Normveilig kan een nieuwe standaardversie voorstellen; deze wordt voor een lopende opdracht alleen van toepassing overeenkomstig de wijzigingsafspraken in de hoofdovereenkomst of na instemming van Partijen.

Op deze verwerkersovereenkomst is hetzelfde recht en dezelfde geschillenregeling van toepassing als op de hoofdovereenkomst. Indien de hoofdovereenkomst hierover niets bepaalt, is Nederlands recht van toepassing.

Indien een bepaling nietig of onafdwingbaar blijkt, blijven de overige bepalingen van kracht. Partijen vervangen de betreffende bepaling door een geldige bepaling die doel en strekking zo dicht mogelijk benadert.

Bijlage 1 - Standaardomschrijving van de verwerking

Deze bijlage beschrijft het maximale standaardkader voor Normveilig-projecten. De concrete opdracht kan dit kader beperken, aanvullen of nader specificeren. Normveilig verwerkt uitsluitend persoonsgegevens die noodzakelijk zijn voor de overeengekomen werkzaamheden.

Onderdeel	Standaardafspraak
Onderwerp	Ondersteuning bij informatiebeveiliging en compliance, waaronder ISO/IEC 27001, NEN 7510 en NIS2 / Cyberbeveiligingswet, voor zover in de hoofdovereenkomst overeengekomen.
Aard en doel	Advies, inventarisatie, risicoanalyse, gap-analyse, implementatie, projectbegeleiding, auditvoorbereiding, beoordeling van bewijsstukken, security- en privacyondersteuning en het oplossen of analyseren van beveiligingsvraagstukken.
Duur	Gedurende de looptijd van de hoofdovereenkomst en daarna uitsluitend gedurende de overeengekomen verwijder- en back-uptermijnen.
Frequentie	Incidenteel, periodiek of doorlopend, afhankelijk van de opdracht.
Categorieën betrokkenen	Medewerkers, ingehuurde medewerkers, bestuurders, zakelijke contactpersonen, klanten, cliënten/patiënten, leveranciers en overige personen voor zover hun gegevens voorkomen in informatie die noodzakelijk is voor de opdracht.
Categorieën persoonsgegevens	Naam, zakelijke contactgegevens, functie en organisatie; gebruikers-, account- en autorisatiegegevens; systeem- en loggegevens; incidentinformatie; documentmetadata; projectinformatie en overige persoonsgegevens die noodzakelijk zijn voor de opdracht.
Bijzondere of strafrechtelijke gegevens	Niet bedoeld als standaardverwerking. Deze

Onderdeel	Standaardafspraak
	worden alleen verwerkt wanneer dit noodzakelijk is voor de specifieke opdracht, Opdrachtgever daarvoor een gedocumenteerde instructie geeft en passende aanvullende maatregelen zijn overeengekomen.
Bewaartermijn	Werkbestanden worden verwijderd zodra deze niet meer nodig zijn. Na einde dienstverlening geldt in beginsel een maximale verwijdertermijn van 60 dagen, behoudens back-upretentie of wettelijke bewaarplichten.
Plaats van verwerking	In beginsel binnen de EER. Eventuele doorgifte buiten de EER vindt alleen plaats onder de voorwaarden van artikel 9.
Instructies	De hoofdovereenkomst, opdrachtbevestiging, schriftelijke projectinstructies en deze verwerkersovereenkomst vormen gezamenlijk de gedocumenteerde instructies van Opdrachtgever.

Bijlage 2 - Technische en organisatorische maatregelen

Normveilig hanteert een risicogebaseerd pakket van technische en organisatorische maatregelen. De hieronder genoemde basismaatregelen gelden voor zover relevant voor de concrete verwerking; opdrachtgeverspecifieke aanvullende eisen worden schriftelijk vastgelegd.

Domein	Basismaatregel
Governance en verantwoordelijkheid	Vastgelegde verantwoordelijkheid voor informatiebeveiliging en privacy; periodieke beoordeling van risico's, maatregelen en relevante procedures.
Toegangsbeveiliging	Unieke accounts, sterke authenticatie en waar passend MFA; least privilege; periodieke beoordeling van toegangsrechten; tijdige intrekking bij functiewijziging of einde inzet.

Domein	Basismaatregel
Apparaten en werkplekken	Adequaat beveiligde en onderhouden apparaten; schermvergrendeling; malwarebescherming; versleuteling waar passend; terughoudendheid met verwijderbare media en lokale opslag.
Versleuteling en gegevensoverdracht	Versleutelde verbindingen voor overdracht; passende bescherming van opgeslagen gegevens; geen onbeveiligde verzending van vertrouwelijke klantdata.
Patch- en kwetsbaarhedenbeheer	Besturingssystemen en gebruikte software worden onderhouden; beveiligingsupdates worden volgens een risicogebaseerde termijn geïnstalleerd.
Logging en detectie	Waar toepasselijk worden relevante toegangs- en beveiligingsgebeurtenissen gelogd en onderzocht; verdachte gebeurtenissen worden geëscaleerd.
Back-up en continuïteit	Voor systemen waarin klantgegevens duurzaam worden opgeslagen worden passende back-up- en herstelmaatregelen toegepast, afgestemd op de dienstverlening.
Incidentmanagement	Proces voor detectie, triage, beperking, onderzoek, herstel en communicatie van beveiligingsincidenten en datalekken, inclusief vastlegging van relevante feiten en maatregelen.
Leveranciers en subverwerkers	Selectie en beoordeling op relevante beveiligings- en privacywaarborgen; schriftelijke gegevensbeschermingsafspraken; risicogebaseerde herbeoordeling.
Bewustwording en geheimhouding	Personen met toegang tot klantgegevens zijn gebonden aan geheimhouding en ontvangen passende instructie over veilig werken, gegevensdeling, phishing en incidentmelding.

Domein	Basismaatregel
Dataminimalisatie en opslag	Alleen gegevens verwerken die noodzakelijk zijn; waar mogelijk werken in door Opdrachtgever aangewezen omgevingen; lokale kopieën beperken en tijdig verwijderen.
Veilige verwijdering	Digitale en papieren gegevens worden na afloop passend verwijderd of vernietigd, rekening houdend met back-upretentie en wettelijke bewaarplichten.

Bijlage 3 - Subverwerkers en wijzigingen

Normveilig gebruikt alleen subverwerkers voor klantgegevens wanneer dit noodzakelijk is voor de dienstverlening. De concrete subverwerkers kunnen per opdracht verschillen, bijvoorbeeld omdat een klant verplicht stelt dat werkzaamheden uitsluitend in diens eigen cloud- of samenwerkingsomgeving plaatsvinden.

Wanneer een subverwerker persoonsgegevens van Opdrachtgever zal verwerken, maakt Normveilig de identiteit, dienst, verwerkingslocatie en - indien relevant - doorgiftegrond vooraf kenbaar via de offerte, opdrachtbevestiging, projectdocumentatie of een afzonderlijk subverwerkersoverzicht. Een wijziging wordt vooraf gemeld zodat Opdrachtgever overeenkomstig artikel 5 gemotiveerd bezwaar kan maken.

Geen impliciete toestemming voor onbekende doorgiften

Het feit dat een leverancier door Normveilig wordt gebruikt, betekent niet automatisch dat die leverancier persoonsgegevens van Opdrachtgever verwerkt. Alleen partijen die daadwerkelijk als subverwerker optreden vallen onder deze bijlage en de meldingsplicht.

Versiebeheer

Versie 1.0 - 3 september 2026. Eerste openbare standaardversie van de verwerkersovereenkomst van Normveilig.