Stratech
betrokken
kennispartner

Contact
Postbus 3
7500 AA Enschede

053 480 40 80
info@stratech.nl
www.stratech.nl

Artikel 1. Toepasselijkheid

1. Deze Privacy Voorwaarden Stratech zijn, naast de Algemene Voorwaarden Stratech en eventuele andere voorwaarden, van toepassing op alle offertes, opdrachtbevestigingen en overeenkomsten van Stratech Holding bv, gevestigd aan het Pantheon 15 te Enschede, alsmede van alle werkmaatschappijen van Stratech Holding bv, hierna te noemen leverancier.
2. Indien bepalingen met betrekking tot persoonsgegevens / privacy uit offertes, opdrachtbevestigingen, overeenkomsten of andere toepasselijke voorwaarden strijdig zijn met bepalingen in deze Privacy Voorwaarden Stratech, prevaleren de bepalingen uit deze Privacy Voorwaarden Stratech.

Artikel 2. Definities

In de Privacy Voorwaarden Stratech wordt verstaan onder:

- Persoonsgegevens: “persoonsgegevens” als bedoeld in de Algemene Verordening Gegevensbescherming (AVG), welke zijn omschreven in bijlage 1;
- Verwerkingsverantwoordelijke: “verwerkingsverantwoordelijke” als bedoeld in de AVG, zijnde de opdrachtgever die aan leverancier opdracht heeft gegeven tot het verrichten van werkzaamheden;
- Verwerker: “verwerker” als bedoeld in de AVG, zijnde leverancier;
- Werkzaamheden: alle werkzaamheden waartoe door opdrachtgever opdracht is gegeven aan leverancier, of die door leverancier uit andere hoofde worden verricht. Het voorgaande geldt in de ruimste zin van het woord en omvat in ieder geval de werkzaamheden zoals vermeld in de opdrachtbevestiging of overeenkomst.

Artikel 3. Algemeen

1. De Privacy Voorwaarden Stratech zien op alle persoonsgegevens die in het kader van de uitvoering van de overeenkomst door leverancier worden verwerkt voor opdrachtgever, alsmede op alle overige ten behoeve van opdrachtgever verrichte werkzaamheden en de in dat kader te verwerken persoonsgegevens.
2. Bij het verrichten van werkzaamheden verwerkt verwerker bepaalde persoonsgegevens voor verwerkingsverantwoordelijke.
3. De Privacy Voorwaarden Stratech vormen een overeenkomst of andere rechtshandeling als bedoeld in artikel 28 lid 3 AVG.
4. Indien verwerker op grond van de Privacy Voorwaarden Stratech kosten in rekening brengt aan verwerkingsverantwoordelijke, gebeurt dat tegen de dan geldende condities en tarieven van verwerker.

Artikel 4. Reikwijdte

1. Met het geven van de opdracht tot het verrichten van werkzaamheden heeft verwerkingsverantwoordelijke aan verwerker de opdracht gegeven om persoonsgegevens te verwerken namens verwerkingsverantwoordelijke op de wijze zoals omschreven in bijlage 1 in overeenstemming met de bepalingen van de Privacy Voorwaarden Stratech en artikel 30 lid 2 sub b AVG.
2. Verwerker verwerkt de persoonsgegevens in overeenstemming met de Privacy Voorwaarden Stratech. Verwerker bevestigt de persoonsgegevens niet voor andere doeleinden te verwerken.
3. De zeggenschap over de persoonsgegevens komt nooit bij verwerker te rusten.
4. Verwerker verwerkt de persoonsgegevens enkel in de Europese Economische Ruimte.

Artikel 5. Verplichtingen verwerkingsverantwoordelijke

1. Verwerkingsverantwoordelijke treft de nodige maatregelen opdat persoonsgegevens, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, juist en nauwkeurig zijn en als zodanig ook aan verwerker worden verstrekt. Verwerkingsverantwoordelijke staat er jegens verwerker voor in dat niet meer persoonsgegevens worden verzameld dan strikt noodzakelijk voor het verrichten van de werkzaamheden. Onverminderd de verplichtingen van verwerker voortvloeiend uit deze Privacy Voorwaarden Stratech en de AVG, is verwerkingsverantwoordelijke verantwoordelijk voor de verwerking van de persoonsgegevens zoals omschreven in bijlage 1, alsmede voor de nakoming van de verplichtingen die op grond van de AVG en aanverwante wet- en regelgeving rusten op opdrachtgever als verwerkingsverantwoordelijke. Verwerkingsverantwoordelijke is verantwoordelijk voor alle verplichtingen welke uit hoofde van de AVG op hem rusten. Meer in het bijzonder neemt verwerkingsverantwoordelijke het bepaalde in artikel 24 en 25 AVG in acht, onder meer – maar daartoe niet beperkt – door, rekening houdend met de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen, het treffen van technische en organisatorische maatregelen om te waarborgen en te kunnen aantonen dat de verwerking in overeenstemming met de AVG geschiedt (artikel 24 lid 1 AVG).
2. Verwerkingsverantwoordelijke zal voorts, rekening houdend met de stand van de techniek, de uitvoeringskosten, en de aard, de omvang, de context en het doel van de verwerking alsook met de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van natuurlijke personen welke aan de verwerking zijn verbonden, zowel bij de bepaling van de verwerkingsmiddelen als bij de verwerking zelf, passende technische en organisatorische maatregelen treffen, zoals pseudonimisering, die zijn opgesteld met als doel de gegevensbeschermingsbeginselen, zoals minimale gegevensverwerking, op een doeltreffende manier uit te voeren en de nodige waarborgen in de verwerking in te bouwen ter naleving van de voorschriften van de AVG en ter bescherming van de rechten van de betrokkenen (artikel 25 lid 1 AVG). Voorts treft verwerkingsverantwoordelijke passende technische en organisatorische maatregelen om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking (artikel 25 lid 2 AVG).
3. Verwerkingsverantwoordelijke geeft naam en contactgegevens en, indien aangesteld, de gegevens van de functionaris voor gegevensbescherming, zoals bedoeld in artikel 30 lid 2 sub a AVG door aan verwerker en informeert verwerker terstond over wijzigingen daarin.
4. Verwerkingsverantwoordelijke garandeert dat hij geen verwerkingen door verwerker zal laten uitvoeren waarbij sprake is van doorgiften van persoonsgegevens aan een derde land of internationale organisatie zoals bedoeld in artikel 30 lid 2 sub c AVG.
5. Verwerkingsverantwoordelijke vrijwaart verwerker voor mogelijke aanspraken van derden, waaronder – maar daartoe niet beperkt – die van betrokkenen als bedoeld in de AVG en die van de Autoriteit Persoonsgegevens, verband houdend met de schending van verplichtingen van verwerkingsverantwoordelijke uit hoofde van het bepaalde in dit artikel en de AVG.

Artikel 6. Geheimhouding

1. Verwerker en de personen die in dienst zijn van verwerker of werkzaamheden voor hem verrichten, voor zover deze personen toegang hebben tot persoonsgegevens, verwerken de persoonsgegevens slechts in opdracht van verwerkingsverantwoordelijke, behoudens afwijkende wettelijke verplichtingen of andersluidende rechterlijke uitspraak.
2. Verwerker en de personen die in dienst zijn van verwerker of werkzaamheden voor hem verrichten, voor zover deze personen toegang hebben tot persoonsgegevens, zijn verplicht tot geheimhouding van de persoonsgegevens waarvan zij kennis nemen, behoudens voor zover enig wettelijk voorschrift of rechterlijke uitspraak hen tot mededeling verplicht of uit een taak de noodzaak tot mededeling voortvloeit. De verplichting als bedoeld in de vorige volzin geldt zowel gedurende de looptijd van de overeenkomst(en) met verwerkingsverantwoordelijke als na afloop daarvan.

Artikel 7. Geen verdere verstrekking

1. Verwerker zal de persoonsgegevens niet delen met of verstrekken aan derden, tenzij verwerker daartoe voorafgaande, schriftelijke toestemming of opdracht heeft verkregen van verwerkingsverantwoordelijke of op grond van wet- of regelgeving of rechterlijke uitspraak daartoe verplicht is.
2. Indien verwerker op grond van wet- of regelgeving of rechterlijke uitspraak verplicht is om de persoonsgegevens te delen met of te verstrekken aan derden, zal verwerker verwerkingsverantwoordelijke hierover schriftelijk informeren, tenzij dit niet is toegestaan onder de genoemde wet- of regelgeving of rechterlijke uitspraak.

Artikel 8. Beveiligingsmaatregelen

1. Verwerker zal – rekening houdend met de van toepassing zijnde wet- en regelgeving op het gebied van de beveiliging van de verwerking van persoonsgegevens, de stand van de techniek, de uitvoeringskosten, alsook met de aard, de omvang, de context en de verwerkingsdoeleinden en de qua waarschijnlijkheid en ernst uiteenlopende risico's voor de rechten en vrijheden van personen – technische en organisatorische beveiligingsmaatregelen treffen om een op het risico afgestemd beveiligingsniveau te waarborgen, en de door verwerker verwerkte persoonsgegevens te beveiligen tegen inbreuken in verband met persoonsgegevens zoals bedoeld in artikel 4 sub 12 AVG. De maatregelen zijn er mede op gericht om verzameling en verdere verwerking van persoonsgegevens, anders dan strikt noodzakelijk voor het verrichten van de werkzaamheden, te voorkomen. Waar in artikel 4 sub 12 AVG wordt gesproken over doorgezonden persoonsgegevens, ziet de verantwoordelijkheid van verwerker uitsluitend op door haar in het kader van een overeengekomen werkzaamheid ontvangen persoonsgegevens die aan haar zijn doorgezonden en niet op persoonsgegevens die door verwerker zijn doorgezonden naar verwerkingsverantwoordelijke en/of derden, niet zijnde sub-verwerker(s).
2. De beveiligingsmaatregelen die thans zijn genomen, en waarvan partijen vaststellen dat deze als passend worden beschouwd als bedoeld in artikel 32 lid 1 AVG, zijn in bijlage 2 bepaald en dienen tevens als de beschrijving zoals bedoeld in artikel 30 lid 2 letter d AVG.

Artikel 9. Toezicht op naleving

1. In het kader van het toezicht op de naleving door verwerker van de Privacy Voorwaarden Stratech –uitsluitend ten aanzien van de in dat verband genomen beveiligingsmaatregelen als bedoeld in artikel 8 – zal verwerker ter uitvoering van het bepaalde in artikel 28 lid 3 sub h AVG eenmaal per (kalender)jaar een auditrapportage (ISAE 3000) laten opstellen door een door verwerker aan te wijzen externe deskundige. Bedoelde rapportage zal door verwerker aan verwerkingsverantwoordelijke worden verstrekt.
2. De in artikel 28 lid 3 sub h AVG genoemde audits, waaronder inspecties, zullen niet door verwerkingsverantwoordelijke zelf worden uitgevoerd. Conform het in genoemd artikel bepaalde, machtigt verwerkingsverantwoordelijke verwerker om namens verwerkingsverantwoordelijke een controleur (de extern deskundige als bedoeld in lid 1) aan te wijzen voor de controle op de naleving als bedoeld in lid 1.
3. De kosten van de in lid 1 bedoelde audit, alsmede van eventuele overige werkzaamheden van verwerker ten behoeve van het toezicht op de naleving van verplichtingen uit hoofde van artikel 28 lid 3 sub h AVG, komen voor rekening van verwerkingsverantwoordelijke. In geval van hosting zijn de kosten van de jaarlijkse audit begrepen in de kosten van de hosting.

Artikel 10. Datalek

1. Conform het bepaalde in artikel 33 lid 2 AVG informeert verwerker verwerkingsverantwoordelijke zonder onredelijke vertraging zodra hij kennis heeft genomen van een inbreuk in verband met persoonsgegevens. Verwerker zal, voor zover mogelijk, informatie (als bedoeld in artikel 28 lid 3 sub f AVG) verstrekken over: de aard van de inbreuk in verband met persoonsgegevens, de waarschijnlijk gevolgen van de inbreuk in verband met de persoonsgegevens en de maatregelen die verwerker heeft getroffen en zal treffen.
2. Het bepaalde in lid 1 van dit artikel laat onverlet de verplichtingen van verwerkingsverantwoordelijke welke voortvloeien uit de AVG in geval van inbreuken als bedoeld in lid 1, meer in het bijzonder – maar daartoe niet beperkt – de verplichtingen op grond van artikel 33 en 34 AVG.

Artikel 11. Sub-verwerkers

1. Verwerker is gerechtigd bij de uitvoering van de werkzaamheden uit hoofde van de Privacy Voorwaarden Stratech derden (sub-verwerkers, zoals genoemd in bijlage 1) in te schakelen, waarvoor verwerkingsverantwoordelijke algemene toestemming verleent als bedoeld in artikel 28 lid 2 AVG. Verwerker licht verwerkingsverantwoordelijke in over beoogde veranderingen inzake de toevoeging of vervanging van sub-verwerkers, waarbij verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. Bezwaar zal binnen tien dagen na kennisgeving als hiervoor bedoeld door verwerker zijn ontvangen, bij gebreke waarvan verwerkingsverantwoordelijke wordt geacht geen bezwaar te hebben. In alle gevallen zal bezwaar niet op onredelijke gronden worden ingediend. Verwerkingsverantwoordelijke is gerechtigd met onmiddellijke ingang de overeenkomsten met verwerker waarop de beoogde verandering waartegen bezwaar is gemaakt betrekking heeft, op te zeggen indien de inschakeling van betreffende sub-verwerker meebrengt dat voortzetting van die overeenkomsten binnen de kaders van de Privacy Voorwaarden Stratech in redelijkheid niet van verwerkingsverantwoordelijke kan worden gevergd. Verwerker is gerechtigd met onmiddellijke ingang de overeenkomsten met verwerkingsverantwoordelijke waarop de beoogde verandering waartegen bezwaar is gemaakt betrekking heeft, op te zeggen indien zonder inschakeling van betreffende sub-verwerkers voortzetting van die overeenkomsten binnen de kaders van de Privacy Voorwaarden Stratech in redelijkheid niet van verwerker kan worden gevergd.
2. Wanneer een verwerker een sub-verwerker inschakelt, legt verwerker aan de betreffende sub-verwerker de Privacy Voorwaarden Stratech op, of sluit verwerker met deze sub-verwerker een (sub)verwerkersovereenkomst betreffende de verplichtingen van de sub-verwerker waarin aan de sub-verwerker dezelfde verplichtingen inzake gegevensbescherming worden opgelegd als die welke op basis van de Privacy Voorwaarden Stratech op verwerker rusten. Wanneer de sub-verwerker zijn verplichtingen inzake de gegevensbescherming niet nakomt, blijft verwerker ten aanzien van verwerkingsverantwoordelijke volledige verantwoordelijk voor het nakomen van de verplichtingen van bedoelde sub-verwerker.

Artikel 12. Aansprakelijkheid

Verwerker is slechts aansprakelijk, een en ander overeenkomstig hetgeen in artikel 82 lid 2 AVG is bepaald, voor schade voor zover die ontstaat door zijn werkzaamheden, als bedoeld in artikel 82 lid 2 AVG. Verwerker is slechts aansprakelijk voor schade welke het directe en uitsluitende gevolg is van niet-nakoming van verplichtingen door verwerker onder de Privacy Voorwaarden Stratech.

Artikel 13. Medewerking bij verzoeken tot bijstand

1. Op verzoek van verwerkingsverantwoordelijke zal verwerker, rekening houdend met de aard van de verwerking, door middel van passende technische en organisatorische maatregelen, voor zover mogelijk, verwerkingsverantwoordelijke bijstand verlenen als bedoeld in artikel 28 lid 3 sub e AVG.

2. Op verzoek van verwerkingsverantwoordelijke zal verwerker, rekening houdend met de aard van de verwerking en de hem ter beschikking staande informatie verwerkingsverantwoordelijke bijstand verlenen als bedoeld in artikel 28 lid 3 sub f AVG.
3. Verwerker is gerechtigd om de kosten die zij moet maken in verband met het bepaalde in lid 1 en 2 bij verwerkingsverantwoordelijke in rekening te brengen.

Artikel 14. Duur en beëindiging

1. Zolang door verwerker werkzaamheden worden verricht ten behoeve van verwerkingsverantwoordelijke zijn de Privacy Voorwaarden Stratech daarop van toepassing.
2. Indien verwerker na het einde van de overeenkomst tussen verwerkingsverantwoordelijke en verwerker Unierechtelijk of lidstaatrechtelijk verplicht is tot opslag van persoonsgegevens gedurende een wettelijke termijn, zal verwerker zorgdragen voor de verwijdering van deze persoonsgegevens na het verstrijken van één maand na het einde van de wettelijke bewaarplicht. De kosten van het voldoen aan genoemde wettelijke bewaarplicht kunnen door verwerker aan verwerkingsverantwoordelijke worden doorbelast.
3. Bij beëindiging van de overeenkomst tussen verwerkingsverantwoordelijke en verwerker kan verwerkingsverantwoordelijke aan verwerker éénmalig, binnen een maand na het einde van de overeenkomst, verzoeken om de bij verwerker beschikbare persoonsgegevens op kosten van verwerkingsverantwoordelijke aan verwerkingsverantwoordelijke te verstrekken respectievelijk terug te bezorgen op een door verwerker te bepalen gegevensdrager of door middel van elektronische overdracht. Na het verstrijken van genoemde termijn van één maand na het einde van de overeenkomst, zullen de persoonsgegevens worden gewist.

Artikel 15. Nietigheid

Indien één of meerdere bepalingen uit de Privacy Voorwaarden Stratech nietig zijn of vernietigd worden, blijven de overige voorwaarden volledig van toepassing. Indien enige bepaling van de Privacy Voorwaarden Stratech nietig is of vernietigd wordt, zullen partijen over de inhoud van een nieuwe bepaling onderhandelen, welke bepaling de inhoud van de oorspronkelijke bepaling zo dicht mogelijk benadert.

Artikel 16. Wijziging Privacy Voorwaarden Stratech

Verwerker is gerechtigd de Privacy Voorwaarden Stratech, waaronder ook de daarbij behorende bijlage(n), eenzijdig te wijzigen indien dit naar het oordeel van verwerker redelijkerwijs aangewezen is in verband met onder meer wijziging van wet- en regelgeving, jurisprudentie met betrekking tot de (uitleg van de) AVG, wijziging van functionaliteit van het softwarepakket, wijziging van de werkzaamheden en/of de beveiligingsmaatregelen en/of wijziging van het beleid van verwerker. Een wijziging is van kracht vanaf het moment dat verwerkingsverantwoordelijke de gewijzigde Privacy Voorwaarden Stratech heeft ontvangen.

Stratech
betrokken
kennispartner

Contact
Postbus 3
7500 AA Enschede

053 480 40 80
info@stratech.nl
www.stratech.nl

Deze bijlage is bijlage 1 als genoemd in de Privacy Voorwaarden Stratech voor verwerkingsverantwoordelijken die gebruik maken van het softwarepakket Stratech Perspectief van leverancier.

Verwerkingsverantwoordelijke laat verwerker werkzaamheden verrichten. Als onderdeel van deze werkzaamheden kunnen gegevens van personen verwerkt worden. In deze bijlage is vastgelegd welke persoonsgegevens worden verwerkt en welke werkzaamheden verwerker in dat kader voor verwerkingsverantwoordelijke uitvoert.

Deze bijlage is mede afhankelijk van wijziging van functionaliteit van het softwarepakket en kan daardoor, bijvoorbeeld als gevolg van een update, wijzigingen.

1. Versiebeheer

Datum	Wijziging
03-05-2018	Eerste versie.
01-05-2020	Versiebeheer toegevoegd; In verband met de migratie van de hostingomgeving van Root naar Previder: ▪ beheerwerkzaamheden ten behoeve van de hostingomgeving van leverancier door sub-verwerker Root geschrapt; ▪ sub-verwerker Previder toegevoegd voor beheerwerkzaamheden ten behoeve van de hostingomgeving van leverancier.
06-10-2020	Sub-verwerker Root verwijderd.

2. Persoonsgegevens[1]

Verwerkingsverantwoordelijke verwerkt gegevens van personen die afzonderlijk of gecombineerd redelijkerwijs een natuurlijk persoon identificeren (identificerende persoonsgegevens). Verwerkingsverantwoordelijke maakt daarvoor gebruik van het softwarepakket Stratech Perspectief van leverancier. Het betreft onderstaande (categorieën van) gegevens:

- Naamgegevens (zoals voornaam, achternaam);
- Adresgegevens (zoals straat, huisnummer, postcode, plaats, land);
- Contactgegevens (zoals e-mailadres, telefoonnummer);
- Geboortedatum;
- Bankgegevens (zoals IBAN, BIC);
- Nummer van identiteitsbewijs.

Naast de identificerende persoonsgegevens verwerkt verwerkingsverantwoordelijke de navolgende aanvullende (categorieën van) persoonsgegevens die betrekking hebben op de natuurlijk persoon:

- Gebruikershistorie;
- Schulden;
- Vermogen en bezittingen;
- Cliënthistorie (zoals trajecten, gebruik portal);
- Sociale netwerk;
- Inkomsten en uitgaven;
- Gegevens die noodzakelijk zijn voor de berekening van de afloscapaciteit (VTLB gegevens)
- Gegevens die noodzakelijke zijn voor het aanleveren van de WSNP verklaring
- Aanvullende gegevens van cliënten (zoals geslacht, geboorteland, partner en kinderen, opleidingsniveau, verblijfsstatus, et cetera).

[1] De mogelijkheid tot het verwerken van bepaalde (categorieën van) persoonsgegevens kan afhankelijk zijn van de configuratie van het door verwerkingsverantwoordelijke gebruikte softwarepakket.

Verwerkingsverantwoordelijke legt geen andere dan de hiervoor genoemde (categorieën van) persoonsgegevens vast.

3. Werkzaamheden

Verwerker verwerkt ten behoeve van verwerkingsverantwoordelijke hierboven beschreven (categorieën van) persoonsgegevens. De werkzaamheden vloeien voort uit de tussen leverancier en opdrachtgever gesloten overeenkomsten en betreffen één of meerdere van de hieronder genoemde werkzaamheden:

- Hosting;
  Dit betreft tot het hosten behorende beheerwerkzaamheden waarbij de persoonsgegevens in de hostingomgeving van verwerker staan.
- Interfacing;
  Dit betreft geautomatiseerde werkzaamheden vanuit de hostingomgeving van verwerker waarbij persoonsgegevens worden uitgewisseld (ontvangen of doorgezonden) met systemen van derden via interfaces van modules zoals diverse koppelingen, Stratech Insight en Stratech Connect.
- Analyses;
  Dit betreft geautomatiseerde werkzaamheden waarbij persoonsgegevens worden geanalyseerd en gepresenteerd zoals met Stratech Insight.
- Consultancy;
  Dit betreft veelal inrichtingswerkzaamheden die door (een consultant van) verwerker op locatie van verwerkingsverantwoordelijk of vanaf locatie van verwerker worden uitgevoerd en waarbij de medewerker (remote) toegang heeft tot de persoonsgegevens.
- Serviceverlening.
  Dit betreft werkzaamheden die door (een servicedesk medewerker van) verwerker, veelal vanaf locatie van verwerker, worden uitgevoerd en waarbij de medewerker (remote) toegang heeft tot de persoonsgegevens.
  Dit betreft werkzaamheden die door (een medewerker van) verwerker, veelal op locatie van verwerker of, via remote toegang, vanaf locatie van verwerker op locatie van verwerkingsverantwoordelijke, worden uitgevoerd in het kader van het voorkomen en opsporen van onvolkomenheden in het softwarepakket en waarbij de medewerker toegang heeft tot de persoonsgegevens.

4. Sub-verwerkers

Voor de uitvoering van werkzaamheden maakt leverancier gebruik van onderstaande sub-verwerkers.

Naam: Previder BV
Contactgegevens: Expolaan 50, 7556 BE te Hengelo
Werkzaamheden: beheerwerkzaamheden ten behoeve van de hostingomgeving van leverancier.

Stratech
betrokken
kennispartner

Contact
Postbus 3
7500 AA Enschede

053 480 40 80
info@stratech.nl
www.stratech.nl

Deze bijlage is bijlage 2 als genoemd in de Privacy Voorwaarden Stratech voor verwerkingsverantwoordelijken die gebruik maken van het in bijlage 1 (als genoemd in de Privacy Voorwaarden Stratech) genoemde softwarepakket van leverancier.

Verwerkingsverantwoordelijke laat verwerker werkzaamheden verrichten. Als onderdeel van deze werkzaamheden kunnen gegevens van personen verwerkt worden. In deze bijlage is vastgelegd welke beveiligingsmaatregelen verwerker heeft getroffen.

1. Versiebeheer

Datum	Wijziging
03-05-2018	Eerste versie.
11-06-2019	Versiebeheer toegevoegd; Update beveiligingsmaatregelen.
14-08-2019	NEN certificering verwijderd bij hostingprovider.
11-03-2020	Onder ‘Toegangsbeveiliging’ de maatregel betreffende de toewijzing en het gebruik van speciale bevoegdheden aangescherpt. In verband met de migratie van de hostingomgeving van Root naar Previder onder ‘Leveranciersrelaties’ de term ‘maandelijks’ vervangen door ‘periodiek’.
27-11-2020	Taal correctie onder “Veilig personeel”, betreffende de maatregel “Als onderdeel van de arbeidsvoorwaarden moeten werknemers hun verantwoordelijkheden nakomen ten aanzien van het informatiebeveiliging”. Verwijdering van maatregelen met betrekking tot; disaster recovery procedure, leverancier controle en wijzigingen in leveranciers dienstverlening.

2. Beveiligingsmaatregelen

Verwerker verwerkt ten behoeve van verwerkingsverantwoordelijke in bijlage 1 genoemde persoonsgegevens. De werkzaamheden vloeien voort uit de tussen leverancier en opdrachtgever gesloten overeenkomsten. Verwerker heeft onderstaande technische en organisatorische maatregelen getroffen. De beveiligingsmaatregelen worden vermeld per hoofdbeveiligingscategorie.

Informatiebeveiligingsbeleid
Er is informatiebeveiligingsbeleid opgesteld dat in overeenstemming is met bedrijfseisen en relevante wet- en regelgeving.
Ad-hoc en periodiek wordt het informatiebeveiligingsbeleid getoetst en waar nodig geactualiseerd.
Als onderdeel van het informatiebeveiligingsbeleid is het document Handleiding computergebruik opgesteld. Dit document wordt kenbaar gemaakt naar alle medewerkers.

Organiseren van informatiebeveiliging
Verantwoordelijkheden van werknemers ten aanzien van informatiebeveiliging zijn gedefinieerd en belegd.
Verantwoordelijkheden van IT beheerders en ontwikkelaars zijn gescheiden om gelegenheid voor onbedoelde wijziging van diensten te verminderen.
Er is beleid opgesteld dat zorg moet dragen voor verantwoord telewerken.

Veilig personeel
Als onderdeel van de arbeidsvoorwaarden moeten werknemers hun verantwoordelijkheden nakomen ten aanzien van informatiebeveiliging.
Geheimhouding is opgenomen in de arbeidsovereenkomst.
Management eist van werknemers dat zij beveiliging toepassen overeenkomstig met vastgesteld beleid en vastgestelde procedures.
Er is een disciplinair proces ingericht dat ingezet kan worden bij ongewenst gedrag.
Periodiek wordt er aandacht geschonken aan de awareness ten aanzien van beveiliging.

Beheer van bedrijfsmiddelen
Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming van de locatie worden meegenomen.
Er is formeel beleid vastgesteld en er zijn beveiligingsmaatregelen getroffen ter bescherming tegen risico's van het gebruik van draagbare en desktopcomputers en communicatiefaciliteiten.
Er zijn richtlijnen vastgesteld voor het verantwoord installeren van software door medewerkers.
Er is beleid vastgesteld voor het beheer en gebruik van verwijderbare media.
Datadragers worden op een veilige manier afgevoerd als ze niet langer nodig zijn.
Werknemers zijn verplicht de computer te vergrendelen dan wel af te sluiten wanneer men er geen zicht meer op heeft.

Toegangsbeveiliging
Toegang tot informatiesystemen is op netwerkniveau gescheiden middels netwerksegmentatie.
Er is een formeel registratie proces voor nieuwe en vertrekkende gebruikers ingericht om toegangsrechten aan- en af te kunnen koppelen.
De toegangsrechten van alle werknemers tot informatiesystemen en IT-voorzieningen worden geblokkeerd bij beëindiging van het dienstverband, langdurige afwezigheid of bij een op non-actief stelling.
Er is toegangsbeleid ingericht op basis van de geldende bedrijfseisen.
Aan gebruikers wordt alleen toegang verleend tot diensten waarvoor ze specifiek bevoegd zijn.
De toewijzing en het gebruik van bevoegdheden buiten de standaard autorisaties voortvloeiend uit functionele rollen wordt beperkt en beheerst middels een uitzonderingsprocedure.
Toegang tot systemen en applicaties verloopt via een veilige inlog procedure.
Werknemers moeten goede beveiligingsgewoontes in acht nemen bij het kiezen en gebruiken van wachtwoorden.
Informatiesystemen zijn zo ingericht dat er wachtwoorden van vereiste kwaliteit worden afgedwongen.

Cryptografie
Er is beleid ingericht voor het gebruik van cryptografie ter bescherming van informatie.
Er wordt encryptie toegepast op de op draagbare en desktopcomputers opgeslagen informatie.
Alle publieke sites zijn voorzien van een SSL certificaat ter encryptie van het verkeer en het aantonen van eigenaarschap van de betreffende site. Naast encryptie worden een aantal best practices toegepast ter beveiliging van websites en webservers.

Fysieke beveiliging en beveiliging van de omgeving
Beveiligde zones worden beschermd door passende toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.
Apparatuur is zo geplaatst en beschermd dat risico's voor schade en storingen van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd. De infrastructuur ten behoeve van applicatie hosting is geplaatst in een professioneel datacenter.
Geautomatiseerde back-ups worden op twee fysiek gescheiden locaties opgeslagen.
De back-ups zijn opgeslagen op apparatuur in afgesloten ruimten met toegangsbeveiliging.
Het kantoorpand is voorzien van inbraak alarm en er is een procedure vastgelegd tot opvolging.
Het kantoorpand is voorzien van branddetectie inclusief doormelding.
Het kantoorpand is voorzien van camerabeveiliging en beeld wordt opgenomen.

Beveiliging bedrijfsvoering
Het gebruik van hulpprogrammatuur zoals keyloggers, netwerkinventarisatie tools, waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd, is niet toegestaan behalve op basis van een geformaliseerd uitzonderingsproces.
Servers en werkplek apparatuur zijn voorzien van beveiligingssoftware.
De ICT infrastructuur wordt met regelmaat ge-update, urgente beveiligingspatches worden direct ingepland.
De applicatieomgeving is opgenomen in beschikbaarheidsmonitoring.
Er worden hardeningsprincipes toegepast op servers.

Communicatiebeveiliging
Periodiek worden firewall regels getoetst en waar nodig aangepast.
Het verkeer dat door de firewall geblokkeerd wordt, wordt vastgelegd in een log bestand.
Management van informatiesystemen dient ten aller tijden uitgevoerd te worden met een persoonlijk beheeraccount, met uitzondering van apparaten die dit niet ondersteunen.
Management van netwerkapparatuur is zo ingericht dat deze enkel vanuit interne, daartoe gemachtigde, netwerken beschikbaar is. Uitzonderingen hierop zijn alleen mogelijk op basis van een geformaliseerd uitzonderingsproces.

Beheer van informatiebeveiligingsincidenten
Er is een proces ingericht voor security incidenten (waaronder begrepen inbreuken in verband met persoonsgegevens). Onderdeel van dit proces is het implementeren van verbetermaatregelen.

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
Back-ups worden elke nacht gesynchroniseerd naar een andere fysieke locatie.
Er worden procedures gehanteerd ter controle van de juistheid en volledigheid van de back-ups.
Over elke back-up wordt gerapporteerd om na falen te zorgen voor herstel.
Het server platform is redundant uitgevoerd om in geval van hardware falen de dienstverlening te continueren.

Naleving
Er zijn technische en organisatorische maatregelen getroffen om naleving van het informatiebeveiligingsbeleid te controleren en af te dwingen.

Leveranciersrelaties
Beveiligingskenmerken, niveaus van dienstverlening en beheereisen voor diensten die afgenomen worden van de hostingprovider zijn opgenomen in een overeenkomst.
De hostingprovider voldoet aan norm ISO 27001:2013.
De hostinglocatie voldoet aan norm ISO 27001:2013.
Er zijn procedures ingericht die toezichthouden op de actualisatie van de ISO certificering van de hostingprovider en hostinglocatie.

De beveiligingsmaatregelen worden toegepast op de in bijlage 1 gespecificeerde werkzaamheden. Het toepassen van locatie gebonden beveiligingsmaatregelen is afhankelijk van de feitelijke locatie waar de werkzaamheden worden verricht.

De in deze bijlage genoemde beveiligingsmaatregelen gelden uitsluitend voor de fysieke locaties van verwerker, hardware, interne netwerkverbindingen, organisatie en personen waarvoor verwerker verantwoordelijk is en waarover verwerker zeggenschap heeft.