stratech

Contact
Pantheon 15
7521 PR Enschede

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

DATUM	VERSIE	ONDERWERP
01-04-2025	1/2025	Privacy Voorwaarden Stratech (AVG)

Artikel 1. Toepasselijkheid

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

Artikel 2. Algemeen

1. De Privacy Voorwaarden Stratech zien op alle persoonsgegevens die in het kader van de uitvoering van de overeenkomst door Stratech 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 3. 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 en derde landen met een passend beschermingsniveau conform artikel 45 AVG. Verwerkingen van persoonsgegevens buiten de Europese Economische Ruimte zijn als zodanig in bijlage 1 gemarkeerd.

Artikel 4. 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 5. 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 kennisnemen, 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 6. 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 7. 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 benoemd en dienen tevens als de beschrijving zoals bedoeld in artikel 30 lid 2 letter d AVG.

Artikel 8. 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 7 – zal verwerker ter uitvoering van het bepaalde in artikel 28 lid 3 sub h AVG periodiek een audit laten uitvoeren als onderdeel van de Informatie Beveiliging Management Systeem norm NEN-EN-ISO/IEC 27001:2023/A1:2024 waarvan het toepassingsgebied tenminste de in artikel 7 bedoelde beveiligingsmaatregelen betreft.
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 9. 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 10. 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 11. 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 12. 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 13. 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, volgens de bepalingen in artikel 15 lid 2 van de Software Voorwaarden Stratech, verzoeken om de bij verwerker beschikbare persoonsgegevens van verwerkingsverantwoordelijke aan verwerkingsverantwoordelijke te verstrekken respectievelijk terug te bezorgen.

Artikel 14. 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 de software, 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.

Artikel 15. Wijzigingen

1. Voor bestaande overeenkomsten zijnde de overeenkomsten met opdrachtgever die ten tijde van het van kracht worden van deze Privacy Voorwaarden Stratech van kracht zijn vervangen deze Privacy Voorwaarden Stratech (AVG) de eerdere voorwaarden van Stratech, te weten:
- Privacy Voorwaarden Stratech (AVG)
2. Specifieke afspraken in de bestaande overeenkomst tussen Stratech en opdrachtgever welke betrekking hebben op de eerdere voorwaarden zoals genoemd in lid 1 blijven van toepassing.

Deze Privacy Voorwaarden Stratech zijn ter hand gesteld aan opdrachtgever voorafgaand aan of ten tijde van het sluiten van de overeenkomst waarop deze Privacy Voorwaarden Stratech van toepassing zijn. De voorwaarden zijn ook na te lezen en te downloaden op de website van Stratech: www.stratech.nl.

Deze Privacy Voorwaarden Stratech zijn gedeponeerd bij de Rechtbank Overijssel, locatie Almelo op 10-03-2023 onder nummer 6/2023.

stratech

Contact
Pantheon 15
7521 PR Enschede

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

DATUM	VERSIE	ONDERWERP
01-04-2025	1/2025/Perspectief	Privacy Voorwaarden Stratech / Bijlage 1

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

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 de software 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 door sub-verwerker Root geschrapt; sub-verwerker Previder toegevoegd voor beheerwerkzaamheden ten behoeve van de hostingomgeving.
06-10-2020	Sub-verwerker Root verwijderd.
01-10-2021	Interfaces toegevoegd; Terminologie in lijn gebracht met de leveringsvoorwaarden.
28-11-2022	De versie van Stratech Perspectief waarop de in deze bijlage vermelde informatie betrekking heeft, is verhoogd naar 9.10; Burgerservicenummer toegevoegd aan Persoonsgegevens; Schuldenknooppunt versie 1.1 toegevoegd aan Interfaces; Koppeling BKR hernoemd naar BKR koppeling (BKR-net), gemarkeerd als obsolete en naam vervangen door geboortenaam; Koppeling BKR op basis van APIM webservice toegevoegd aan Interfaces.
01-04-2025	Adres sub-verwerker Microsoft Corporation aangepast; De versie van Stratech Perspectief waarop de in deze bijlage vermelde informatie betrekking heeft, is verhoogd naar 10.9; Huisstijlwijzingen doorgevoerd.

2. Persoonsgegevens[1]

Verwerkingsverantwoordelijke verwerkt gegevens van personen die afzonderlijk of gecombineerd redelijkerwijs een natuurlijk persoon identificeren (identificerende persoonsgegevens).
Verwerkingsverantwoordelijke maakt daarvoor gebruik van de software Stratech Perspectief van Stratech.
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);

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

- Nummer van identiteitsbewijs;
- Burgerservicenummer (BSN).

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).

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 Stratech 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 de software en waarbij de medewerker toegang heeft tot de persoonsgegevens.

4. Sub-verwerkers

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

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

Naam: Microsoft Corporation
Contactgegevens: One Microsoft Place, South County Business Park, Carmanhall And Leopardstown, Dublin, D18 P521, Ierland
Werkzaamheden: beheerwerkzaamheden ten behoeve van de hostingomgeving van verwerker.

5. Interfaces

Onderstaande opsomming biedt per interface een overzicht van de mogelijkheden tot uitwisseling van persoonsgegevens en is mede bedoeld als informatie om verwerkingsverantwoordelijke te ondersteunen bij het beoordelen van zijn verantwoordelijkheden.

De informatie heeft betrekking op Stratech-Perspectief vanaf versie 10.9.

MODULE	BESCHRIJVING
Zaaksysteem Koppeling	Met de module Zaaksysteem Koppeling is het mogelijk om zaak- en documentgegevens vanuit Stratech Perspectief op te slaan in uw zaaksysteem. Het uitwisselen van zaak- en documentgegevens tussen Stratech Perspectief en het zaaksysteem vindt plaats op basis van de standaard Zaak- en Documentservices 1.1. De zaak- en documentgegevens kunnen persoonsgegevens bevatten. Enkele algemene kenmerken van deze koppeling: ● Het traject van de cliënt in Stratech Perspectief staat gelijk aan de zaak in het zaaksysteem. ● Gegevens die op zaakniveau worden uitgewisseld zijn: NAW-cliënt, zaaktype, begin- en einddatum, begeleider, status en resultaat. ● In Stratech Perspectief gegenereerde en/of bewerkte brieven of los toegevoegde dossierstukken worden automatisch opgeslagen in het zaaksysteem. ● De volledige documentenlijst van de gekoppelde zaak kan in Stratech Perspectief getoond worden in het tabblad 'Dossier' van de cliënt. Ook wanneer er via een andere bron dan Stratech Perspectief documenten aan de zaak zijn toegevoegd, bijvoorbeeld door een postregistratie systeem. ● Documenten openen vanuit het cliëntdossier opent het document uit het zaaksysteem. Vanuit de hostingomgeving wordt niet rechtstreeks gecommuniceerd met het zaaksysteem, dit wordt gedaan vanuit de door opdrachtgever gebruikte Stratech Perspectief client applicatie op de werkplek. Voor de beveiliging van de communicatie met het zaaksysteem kan gebruik gemaakt worden van https eventueel aangevuld met tweezijdige SSL-verificatie. Deze koppeling is een Dienst Derden.

MODULE	BESCHRIJVING
StUF-BG-BRP Koppeling	Met de module StUF-BG-BRP Koppeling is het mogelijk gegevens, waaronder persoonsgegevens, op te halen uit de Basisregistratie Personen (BRP) en deze op te slaan in Stratech Perspectief. Het ophalen en actualiseren van gegevens uit de BRP verloopt via een gegevensmakelaar op basis van de standaard StUF-BG 3.10. Enkele algemene kenmerken van deze koppeling: ● Het ophalen van de (persoons)gegevens vindt plaats vanuit de cliëntkaart op basis van BSN. Een gebruiker kan zelf de meest actuele gegevens ophalen. ● Per cliënt kan een afnemersindicatie gestuurd worden. Vanaf dat moment krijgt Stratech Perspectief een melding bij een wijziging van de persoon in de BRP. De cliënt krijgt dan een markering. ● Gewijzigde of toegevoegde gegevens worden blauw gemarkeerd, zodat de gebruiker inzichtelijk heeft wat er is gewijzigd en dit kan controleren alvorens deze definitief op te slaan. ● De koppeling wordt gelegd met één van de gangbare gegevensmakelaars, bijvoorbeeld Centric Key2datadistributie, PinkRoccade MakelaarSuite. Het is mogelijk met meerdere gegevensmakelaars te koppelen, bijvoorbeeld bij een gemeentelijke samenwerking. Voor het ontvangen en verzenden van berichten wordt gebruik gemaakt van webservices. De webservice van Stratech Perspectief is ondergebracht in de applicatieserver. Het verkeer tussen de webservices is beveiligd met tweezijdige SSL-verificatie. Betrokken persoonsgegevens: ● Naam ● Geboortedatum ● Geboorteplaats ● Geslacht ● Nationaliteit ● Adresgegevens ● Burgerlijke staat ● Verblijfstitel ● Burgerservicenummer (BSN) Deze koppeling is een Dienst Derden.
Koppeling BKR (APIM webservice)	Met de module Koppeling BKR op basis van APIM webservice is het mogelijk om cliënten te toetsen en kredieten en schuldregelingen te registreren bij het BKR. Onderstaande verwerkingen zijn mogelijk: ● Toetsen CKI ● Door toetsen ● Aanmelden contract bij het BKR ● Afmelden contract bij het BKR ● Registeren mutaties in de gegevens van het contract ● Bijzonderheidsmeldingen op het contract ● Verwerken registraties ● Proactief bepalen van Sterposten ● Beoordelen van Sterposten BKR

MODULE	BESCHRIJVING
	Betrokken persoonsgegevens: ● Adresgegevens (inclusief postcode) ● Geboortedatum ● Geslacht ● Geboortenaam ● Overeenkomst(en) met de zakelijke klant(en) ● De achterstanden, herstelmeldingen en bijzonderheden die zich voordoen gedurende de looptijd van die overeenkomst(en) ● De beëindiging van die overeenkomst(en) De verbinding tussen Stratech Perspectief en het BKR is beveiligd conform de door BKR vereiste beveiligingsnormen en per deelnemernummer is een client side certificaat vereist. Deze koppeling is een Dienst Derden.
Koppeling BKR (BKR-net) Obsolete	Met de module Koppeling BKR is het mogelijk om cliënten te toetsen en kredieten en schuldregelingen te registreren bij het BKR. Onderstaande verwerkingen zijn mogelijk: ● Toetsen CKI ● Door toetsen ● Aanmelden contract bij het BKR ● Afmelden contract bij het BKR ● Registeren mutaties in de gegevens van het contract ● Bijzonderheidsmeldingen op het contract ● Verwerken registraties ● Proactief bepalen van Sterposten ● Beoordelen van Sterposten BKR Voor de werking van de BKR-module is aansluiting met beveiligde BKR-lijn noodzakelijk. Vanuit de hostingomgeving wordt niet rechtstreeks gecommuniceerd met het BKR, dit wordt gedaan vanuit de door opdrachtgever gebruikte Stratech Perspectief client applicatie op de werkplek. Betrokken persoonsgegevens: ● Adresgegevens (inclusief postcode) ● Geboortedatum ● Geslacht ● Geboortenaam ● Overeenkomst(en) met de zakelijke klant(en) ● De achterstanden, herstelmeldingen en bijzonderheden die zich voordoen gedurende de looptijd van die overeenkomst(en) ● De beëindiging van die overeenkomst(en) Deze koppeling is een Dienst Derden.

MODULE	BESCHRIJVING
StUF-BG-NHR Koppeling	Met de module StUF-BG-NHR Koppeling is het mogelijk gegevens, waaronder persoonsgegevens, op te halen uit het Nationaal Handelsregister (NHR) en deze op te slaan in Stratech Perspectief. Het ophalen en actualiseren van gegevens uit het NHR verloopt via een gegevensmakelaar op basis van de standaard StUF-BG 3.10. Enkele algemene kenmerken van deze koppeling: ● Het ophalen van de gegevens vindt plaats op basis van het KvK nummer. Een gebruiker kan zelf de meest actuele gegevens ophalen. ● Gewijzigde of toegevoegde gegevens worden blauw gemarkeerd, zodat de gebruiker inzichtelijk heeft wat er is gewijzigd en dit kan controleren alvorens deze definitief worden opgeslagen. ● De koppeling wordt gelegd met één van de gangbare gegevensmakelaars van bijvoorbeeld Centric en PinkRoccade Voor het ontvangen en verzenden van berichten wordt gebruik gemaakt van webservices. De webservice van Stratech Perspectief is ondergebracht in de applicatieserver. Het verkeer tussen de webservices is beveiligd met tweezijdige SSL-verificatie. Betrokken persoonsgegevens: ● Bezoekadres ● Postadres ● Naam Deze koppeling is een Dienst Derden.
Bewindvoering inclusief Koppeling Rechtspraak	Met de Koppeling Rechtspraak is het mogelijk om digitaal te communiceren met de Rechtspraak voor een cliënt die onder bewind is gesteld. Met de koppeling kunnen de volgende onderdelen met de Rechtspraak worden uitgewisseld: ● Boedelbeschrijving ● (Eind)Rekening & Verantwoording ● Vijfjaarlijkse evaluatie ● Berichten ● Machtigingsverzoeken Er wordt gebruik gemaakt van een PKIoverheid-certificaat en een KvK nummer om de verbinding met rechtspraak tot stand te kunnen brengen. Communicatie vindt plaats vanuit zowel de Stratech Perspectief cliënt applicatie op de werkplek alsmede de Stratech Perspectief applicatieserver. Voor de tot stand komen van de relatie tussen cliënt en zaak worden er eenmalig persoonsgegevens verzonden van Rechtspraak naar Stratech Perspectief. Er worden geen NAW-gegevens verzonden naar Rechtspraak nadat de koppeling is gelegd tussen zaak en cliënt.

MODULE	BESCHRIJVING
	Betrokken persoonsgegevens: ● Adres ● Geboortedatum ● Geboorteland ● Geboorteplaats ● Geslacht ● Naam Deze koppeling is een Dienst Derden.
RaboDirectConnect (RDC)	Met de module RabobankDirectConnect (RDC) is het mogelijk om geautomatiseerd bankbestanden (financiële mutaties) uit te wisselen tussen Stratech Perspectief en de Rabobank. Hierdoor is inloggen op de Rabobank website en het handmatig up- en downloaden van bankbestanden niet meer nodig. Er wordt gebruik gemaakt van een SFTP-server om bankbestanden uit te wisselen tussen Stratech Perspectief en de Rabobank. Er wordt gebruik gemaakt van certificaten voor ondertekening en IP-controle ten behoeve van authenticatie. Betrokken persoonsgegevens: ● Rekeningnummers ● Te naam stelling van de rekening ● Financiële mutaties en saldo's ● Betalingskenmerk(en) Deze koppeling is een Dienst Derden.
Schulinck Koppeling	Schulinck In-Take Schuldhulp is in samenwerking met Stadsring51 uit Amersfoort ontwikkeld. De Stratech Perspectief koppeling met Schulinck In-Take zorgt ervoor dat cliëntgegevens geautomatiseerd verzonden worden naar Schulinck. Er wordt gebruikt van webservices met een unieke URL. Het verkeer is beveiligd met een SSL-certificaat. Voor authenticatie wordt er gebruik gemaakt van een gebruikersnaam en wachtwoord. Betrokken persoonsgegevens: ● Naamgegevens ● Adresgegevens ● E-mailadres ● Geboortedatum ● Geslacht ● Telefoonnummer Vanuit de hostingomgeving wordt niet rechtstreeks gecommuniceerd met Schulinck, dit wordt gedaan vanuit de door opdrachtgever gebruikte Stratech Perspectief client applicatie. Deze koppeling is een Dienst Derden.

MODULE	BESCHRIJVING
Elektronisch bankieren (SEPA)	De module Elektronisch bankieren (SEPA) biedt de mogelijkheid tot het inlezen van bankafschriften waarin persoonsgegevens staan. De door de bank aangeleverde gegevens behoren conform de standaard 'Bank to Customer Statement Message ISO20022' en de voor Nederland geldende specifieke eisen te zijn. Vanuit de hostingomgeving worden geen bankafschriften ingelezen, dit wordt gedaan door de door opdrachtgever gebruikte cliënt waarbij het bestand ingelezen wordt van een buiten de verantwoordelijkheid van verwerker vallende locatie.
Stratech Insight	Stratech Insight is een gebruiksvriendelijke en intuïtieve tool waarmee op eenvoudige en visuele wijze gegevens uit Stratech Perspectief geanalyseerd kunnen worden en deze gegevens om te zetten naar managementinformatie. De koppeling met Stratech Insight biedt de mogelijkheid tot het versturen van persoonsgegevens. Onderstaande geldt voor Stratech Insight draaiende in de hostingomgeving. Het versturen van gegevens ten behoeve van Stratech Insight naar de hostingomgeving is beveiligd via https. De verbinding met de Stratech Insight website is beveiligd met https. Een gebruiker die toegang wil tot de website dient te beschikken over een gebruikersnaam en wachtwoord. Opdrachtgever verstuurt periodiek gegevens ten behoeve van analyses naar de hostingomgeving. Onderdeel van deze gegevens zijn cliënt (persoons)gegevens zoals: ● Geslacht ● Burgerlijke staat ● Woonsituatie ● Samenlevingsverband ● Geboorteland ● Geboortedatum ● Achternaam ● Postcode ● Plaats ● Gemeente ● Gegevens over trajecten
Stratech Connect voor cliënten	Met het Stratech Connect portaal voor cliënten, kunt u uw cliënten inzicht geven in de actuele financiële status, het budgetplan, de voortgang in het traject en het schuldenoverzicht. Tevens heeft u de mogelijkheid om de cliënt bankafschriften, in uw eigen opmaak, als printbare versie beschikbaar te stellen. Het versturen van maandelijkse rekeningoverzichten is hierdoor overbodig. Het cliëntenportaal is beveiligd met een SSL-certificaat, username en wachtwoord en tweefactorauthenticatie (2FA).

MODULE	BESCHRIJVING
	De betrokken persoonsgegevens zijn afhankelijk van inrichting, minimaal zijn hier de volgende persoonsgegevens bij betrokken: ● E-mailadres ● Naam
Generieke Import	Met de module Generieke Import is het mogelijk om geautomatiseerd gegevens te importeren en exporten. Deze functionaliteit is bijvoorbeeld te gebruiken voor het automatisch verwerken van aanmeldingen. Ook kan deze functionaliteit gebruikt worden voor het bijwerken van gegevens. Er zijn mogelijk persoonsgegevens betrokken bij deze module, dit is afhankelijk van inrichting.
VTLB	Voor de berekening van het vrij te laten bedrag (VTLB) wordt de voorgeschreven VTLB-berekeningsmodule van Bureau WSNP gebruikt. De met deze module uit te wisselen gegevens (VTLB-gegevens) worden voorgeschreven door Bureau WSNP. Deze koppeling is een Dienst Derden.
Schuldenknooppunt (versie 1.1)	De koppeling met het Schuldenknooppunt wisselt gegevens uit met het Schuldenknooppunt. De met deze module uit te wisselen gegevens worden voorgeschreven door het Schuldenknooppunt conform het Handboek Schuldenknooppunt, berichtenset versie 1.1. De verbinding tussen Stratech Perspectief en het Schuldenknooppunt is beveiligd conform de door het Schuldenknooppunt vereiste beveiligingsnormen. Deze koppeling is een Dienst Derden.

stratech

Contact
Pantheon 15
7521 PR Enschede

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

DATUM	VERSIE	ONDERWERP
01-04-2025	1/2025/Stratech	Privacy Voorwaarden / Bijlage 2

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

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.
18-05-2021	Overlappende beveiligingsmaatregelen verwijderd.
01-10-2021	Terminologie in lijn gebracht met de leveringsvoorwaarden.
04-07-2023	Beveiligingsmaatregelen aangepast wegens NEN-EN-ISO/IEC 27001:2017+A11:2020 certificering van verwerker.
01-04-2025	Beveiligingsmaatregelen aangepast wegens NEN-EN-ISO/IEC 27001:2023/A1:2024 nl certificering van verwerker.

2. Beveiligingsmaatregelen

Verwerker verwerkt ten behoeve van verwerkingsverantwoordelijke in bijlage 1 genoemde persoonsgegevens. De werkzaamheden vloeien voort uit de tussen Stratech en opdrachtgever gesloten overeenkomsten. Verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten NEN-EN-ISO/IEC 27001:2023/A1:2024 nl.

2.1. ISO certificaat

CERTIFICAAT

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Management Systeem Certificaat

Dit certificaat met nummer DGT271721769 is uitgegeven voor het managementsysteem van:

Stratech Automatisering B.V.

Vestigingsadres: Pantheon 15, 7521PR te Enschede

Voldoet aan de eisen gesteld in de Informatie Beveiliging Management Systeem norm:

NEN-EN-ISO/IEC 27001:2023/A1:2024 nl

Voor het toepassingsgebied: Informatiebeveiliging gerelateerd aan het ontwikkelen van applicaties, het beschikbaar stellen van deze applicaties aan klanten via hosting, het ondersteunen van deze klanten bij het gebruik van de applicatie via service en consultancy, het adequaat beveiligen van de tot de applicatie behorende databank en de daarin opgeslagen (persoons)gegevens en ondersteunende processen voor veilig personeel en veilige voorzieningen.
Dit alles binnen de kaders van de met klant gesloten overeenkomst inclusief de van toepassing zijnde leveringsvoorwaarden en met uitsluiting van de eigen verantwoordelijkheid van een klant voor afdoende beveiliging van diens eigen systemen, gegevens (waaronder persoonsgegevens) en andere al dan niet gevoelige (bedrijfs)informatie.

In overeenstemming met de verklaring van toepasselijkheid versie 2.2 van 24 februari 2025.

Dit certificaat is alleen geldig in samenhang met het certificaataanhangsel met hetzelfde nummer, waarop de van toepassing zijnde locaties met betrekking tot dit certificaat vermeld zijn.

Dit certificaat is geldig vanaf:
4 maart 2025

Dit certificaat is geldig tot:
12 mei 2026

Datum eerste certificaat:
12 mei 2023

Dit certificaat vervangt nr:
DGT271721337

NAMENS

Marco Bijl
DigiTrust B.V.

MGMT. SYS.
RvA C 618

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

Deze afgifte is uitgevoerd in overeenstemming met en binnen de procedures van DigiTrust zoals ook bekend bij en gecontroleerd door de RvA. Dit certificaat is elektronisch uitgegeven, het is en blijft eigendom van DigiTrust. Het valt daarom onder en is gebonden aan de uitgifte condities van het contract.
Certificaten kunnen worden gevalideerd via de QR-code.

Pagina 1 van 2

CERTIFICAAT

DigiTrust
CERTIFICATION OF MANAGEMENT SYSTEMS

Behorende bij het certificaat met registratienummer: DGT271721769
Het informatiebeveiligingsmanagementsysteem van: Stratech Automatisering B.V.

Werkmaatschappijen en geregistreerde activiteiten

Stratech Automatisering B.V.
Informatiebeveiliging gerelateerd aan het ontwikkelen van applicaties, het beschikbaar stellen van deze applicaties aan klanten via hosting, het ondersteunen van deze klanten bij het gebruik van de applicatie via service en consultancy, het adequaat beveiligen van de tot de applicatie behorende databank en de daarin opgeslagen (persoons)gegevens en ondersteunende processen voor veilig personeel en veilige voorzieningen.
Dit alles binnen de kaders van de met klant gesloten overeenkomst inclusief de van toepassing zijnde leveringsvoorwaarden en met uitsluiting van de eigen verantwoordelijkheid van een klant voor afdoende beveiliging van diens eigen systemen, gegevens (waaronder persoonsgegevens) en andere al dan niet gevoelige (bedrijfs)informatie.

Stratech Opleiding & Advies B.V.
Pantheon 15, 7521 PR Enschede

DigiTrust B.V.: Achtseweg Zuid 159R - 5651 GW Eindhoven - Nederland
Telefoon +31 88 224-5600 - sales@digitrust.nl - www.digitrust.nl - KvK 59396822

2.2. Verklaring van toepasselijkheid (VVT)

ISO27001:2023/A1:2024(NL) VERKLARING VAN TOEPASSELIJKHEID STRATECH VERSIE 2.2 DATUM: 24-2-2025			VAN TOEPASSING?	GEÏMPLEMENTEERD?	VAN TOEPASSING VANUIT WET- EN REGELGEVING	VAN TOEPASSING VANUIT CONTRACT EN/OF SLA	RISICO ANALYSE	ONDERBOUWING WAAROM NIET VAN TOEPASSING
Nr.	Onderwerp	Beheersmaatregel						
5	**Organisatorische beheersmaatregelen**							
5.1	Beleidsregels voor informatiebeveiliging	Informatiebeveiligingsbeleid en onderwerp specifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	Ja	Ja		X	X	
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Ja		X	X	
5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Ja			X	
5.4	Management-verantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie	Ja	Ja			X	
5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja	Ja			X	

5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja	Ja			X	
5.7	Informatie en analyses over dreigingen	Informatie- met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja	Ja			X	
5.8	Informatiebeveiliging en projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Ja			X	
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja	Ja			X	
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja			X	
5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja	Ja			X	
5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Ja	Ja		X	X	
5.13	Labelen van informatie	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja			X	

5.14	Overdragen van informatie	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Ja		X	X	
5.15	Toegangsbeveiliging	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja	Ja		X	X	
5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Ja			X	
5.17	Authenticatie-informatie	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja	Ja			X	
5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja	Ja			X	
5.19	Informatiebeveiliging en leveranciersrelaties	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	Ja	Ja			X	
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja	Ja	X	X	X	
5.21	Beheren van informatiebeveiliging in	Er moeten processen en procedures worden bepaald en	Ja	Ja			X	

	de ICT-toeleveringsketen	geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.						
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja	Ja			X	
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Ja			X	
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligings-incidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie[1]beveiligingsincidente n te definiëren, vast te stellen en te communiceren.	Ja	Ja			X	
5.25	Beoordelen van en besluiten over informatiebeveiligings-gebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenis sen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Ja			X	
5.26	Reageren op informatiebeveiligings-incidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja			X	
5.27	Leren van informatiebeveiligings-incidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Ja			X	
5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren	Ja	Ja			X	

		voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.						
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Ja			X	
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen	Ja	Ja		X	X	
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	Ja	Ja	X	X	X	
5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja	Ja	X		X	
5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Ja	X		X	
5.34	Privacy en bescherming van persoonsgegevens	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	Ja	Ja	X	X	X	
5.35	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen	Ja	Ja		X	X	

		en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.						
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Ja	X	X	X	
5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Ja			X	
6	**Mensgerichte beheersmaatregelen**							
6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Ja			X	
6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Ja		X	X	
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke	Ja	Ja		X	X	

		beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen						
6.4	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja	Ja		X	X	
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband, moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	Ja		X	X	
6.6	Vertrouwelijkheids- of geheimhoudings-overeenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Ja		X	X	
6.7	Werken op afstand	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja	Ja			X	
6.8	Melden van informatiebeveiligings-gebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligings-gebeurtenissen tijdig via passende kanalen kan melden.	Ja	Ja		X	X	
7	**Fysieke beheersmaatregelen**							

7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken	Ja	Ja			X	
7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligings-maatregelen en toegangspunten.	Ja	Ja		X	X	
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Ja			X	
7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Ja			X	
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	Ja	Ja			X	
7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja			X	
7.7	'Clear desk' en 'clear sereen’	Er moeten ‘clear desk’-regels voor papieren documenten en verwijderbare opslagmedia en ‘clear screen’-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	Ja	Ja			X	
7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Ja			X	
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Ja			X	
7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf,	Ja	Ja			X	

		gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.						
7.11	Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Ja			X	
7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Ja			X	
7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.	Ja	Ja			X	
7.14	Vellig verwijderen of hergebruiken van apparatuur	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja	Ja			X	
8	**Technologische beheersmaatregelen**							
8.1	User endpoint devices	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja	Ja			X	
8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Ja			X	
8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerp specifieke beleid inzake toegangsbeveiliging.	Ja	Ja		X	X	
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten	Ja	Ja			X	

		en softwarebibliotheken moet op passende wijze worden beheerd.						
8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatie technologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja			X	
8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Ja			X	
8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	Ja	Ja			X	
8.8	Beheer van technische kwetsbaarheden	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.	Ja	Ja			X	
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Ja			X	
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja	Ja			X	
8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Ja			X	

8.12	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Ja			X	
8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Ja		X	X	
8.14	Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja		X	X	
8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Ja		X	X	
8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Ja		X	X	
8.17	Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja	Ja			X	
8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Ja			X	

8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Ja			X	
8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja		X	X	
8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Ja		X	X	
8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Ja			X	
8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Ja			X	
8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja	Ja		X	X	
8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja	Ja			X	
8.26	Toepassingsbeveiligings-eisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Ja			X	
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja	Ja			X	

8.28	Vellig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja	Ja		X	X	
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja	Ja			X	
8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Nvt				Software ontwikkeling is niet uitbesteedt.
8.31	Scheiding van ontwikkel-, test en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja	Ja		X	X	
8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja	Ja			X	
8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Ja			X	
8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Ja			X	

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.