

DATUM  
01-04-2025

VERSIE  
01/2025

ONDERWERP  
Privacy Voorwaarden Strattech Shipment

## Artikel 1. Toepasselijkheid

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

## Artikel 2. Definities

In de Privacy Voorwaarden Strattech Shipment 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 Strattech opdracht heeft gegeven tot het verrichten van werkzaamheden;
- Verwerker: "verwerker" als bedoeld in de AVG, zijnde Strattech;
- Werkzaamheden: alle werkzaamheden waartoe door opdrachtgever opdracht is gegeven aan Strattech, of die door Strattech uit anderen hoofde worden verricht dan wel behoren te worden verricht. Het voorgaande geldt in de ruimste zin van het woord en omvat in ieder geval de werkzaamheden voortvloeiende uit de overeenkomst.

## Artikel 3. Algemeen

1. De Privacy Voorwaarden Strattech Shipment zien op alle persoonsgegevens die in het kader van de uitvoering van de overeenkomst door Strattech 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 Strattech Shipment vormen een overeenkomst of andere rechtshandeling als bedoeld in artikel 28 lid 3 AVG.
4. Indien verwerker op grond van de Privacy Voorwaarden Strattech Shipment 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 Strattech Shipment en artikel 30 lid 2 sub b AVG.
2. Verwerker verwerkt de persoonsgegevens in overeenstemming met de Privacy Voorwaarden Strattech Shipment. 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 Strattech Shipment 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 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 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 Shipment –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 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 8 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 zijn begrepen in de kosten voor het abonnement op de online dienst.
4. 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.

## 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 Shipment 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 Shipment 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 Strattech Shipment 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 Strattech Shipment 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 Strattech Shipment 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 Strattech Shipment.

## 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 Strattech Shipment 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 Strattech Shipment nietig zijn of vernietigd worden, blijven de overige voorwaarden volledig van toepassing. Indien enige bepaling van de Privacy Voorwaarden Strattech Shipment 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 Strattech Shipment

Verwerker is gerechtigd de Privacy Voorwaarden Strattech Shipment, 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 online dienst, 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 Strattech Shipment heeft ontvangen.

De Privacy Voorwaarden Strattech Shipment, waaronder ook de daarbij behorende bijlage(n), zijn gedeponeerd bij de Rechtbank Overijssel, locatie Almelo op 10-03-2023 onder nummer 6/2023.

DATUM  
01-04-2025

VERSIE  
01/2025

ONDERWERP  
Privacy Voorwaarden Stratech Shipment - bijlage 1

Deze bijlage is bijlage 1 als genoemd in de Privacy Voorwaarden Stratech Shipment voor verwerkingsverantwoordelijken die gebruik maken van de online dienst Stratech Shipment 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 wijzigingen of uitbreidingen van functionaliteit van de online dienst en kan daardoor, bijvoorbeeld als gevolg van een update, wijzigen.

## 1. Versiebeheer

| DATUM      | WIJZIGING                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 12-06-2020 | Versiebeheer toegevoegd;<br>Douane toegevoegd aan werkzaamheid Interfacing;<br>In verband met de migratie van de hostingomgeving van Root naar Previder: <ul style="list-style-type: none"> <li>beheerwerkzaamheden ten behoeve van de hostingomgeving door sub-verwerker Root geschrapt;</li> <li>sub-verwerker Previder toegevoegd voor beheerwerkzaamheden ten behoeve van de hostingomgeving.</li> </ul> |
| 06-10-2020 | Sub-verwerker Root verwijderd.                                                                                                                                                                                                                                                                                                                                                                               |
| 01-08-2022 | Terminologie in lijn gebracht met de leveringsvoorwaarden;<br>Werkzaamheid Interfacing aangepast;<br>Werkzaamheid Analyses toegevoegd;<br>Werkzaamheid Consultancy toegevoegd;<br>Werkzaamheid Serviceverlening aangepast.                                                                                                                                                                                   |
| 11-01-2023 | Sub-verwerker Userlane GmbH toegevoegd.                                                                                                                                                                                                                                                                                                                                                                      |
| 01-04-2025 | Adres sub-verwerker Microsoft Corporation aangepast.                                                                                                                                                                                                                                                                                                                                                         |

## 2. Persoonsgegevens<sup>1</sup>

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

- Gegevens van gebruikers;
- Gegevens van relaties.

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

<sup>1</sup> De mogelijkheid tot het verwerken van bepaalde (categorieën van) persoonsgegevens kan afhankelijk zijn van de configuratie van de door verwerkingsverantwoordelijke gebruikte online dienst.

### 3. Werkzaamheden

Verwerker verwerkt ten behoeve van verwerkingsverantwoordelijke hierboven beschreven (categorieën van) persoonsgegevens. De werkzaamheden vloeien voort uit de tussen Strattech 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) via interfaces met systemen van derden zoals Kamer van Koophandel, Douane en ERP-systemen.
- **Analyses;**
- Dit betreft veelal geautomatiseerde werkzaamheden waarbij gegevens waaronder persoonsgegevens worden geanalyseerd ten behoeve van het verkrijgen van geanonimiseerde statistische gegevens, het verbeteren en optimaliseren van de online dienst, het opsporen en herstellen van fouten en de ondersteuning van opdrachtgever.
- **Consultancy;**  
Dit betreft veelal werkzaamheden 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 of, via remote toegang, vanaf locatie van verwerker op locatie van verwerkingsverantwoordelijke, worden uitgevoerd in het kader van servicemeldingen betreffende ondersteuning met betrekking tot de online dienst 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 servicemeldingen betreffende storingen en gebreken met betrekking tot de online dienst 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 Microsoft Azure Core Services.

Naam: Userlane GmbH

Contactgegevens: Rosenheimerstraße 143C, D-81671 Munich, Duitsland

Werkzaamheden: beheerwerkzaamheden ten behoeve van Userlane services.



DATUM  
01-04-2025

VERSIE  
1/2025/Strattech

ONDERWERP  
Privacy Voorwaarden / Bijlage 2

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

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;<br>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.<br>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 Strattech en opdrachtgever gesloten overeenkomsten. Verwerker werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten NEN-EN-ISO/IEC 27001:2023/A1:2024 nl.

DATUM  
01-04-2025

VERSIE  
1/2025/Stratech

ONDERWERP  
Privacy Voorwaarden / Bijlage 2

## 2.1. ISO certificaat

CERTIFICAAT

  
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

Datum eerste certificaat:  
12 mei 2023

**NAMENS**



Marco Bijl  
DigiTrust B.V.

Dit certificaat is geldig tot:  
12 mei 2026

Dit certificaat vervangt nr:  
DGT271721337



**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.



MGMT. SYS.  
RvA C 618

Pagina 1 van 2

DATUM  
01-04-2025

VERSIE  
1/2025/Strattech

ONDERWERP  
Privacy Voorwaarden / Bijlage 2

CERTIFICAAT

  
CERTIFICATION OF MANAGEMENT SYSTEMS

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

Werkmaatschappijen en geregistreerde activiteiten

---

**Strattech 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.

Strattech 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

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 2 van 2

## 2.2. Verklaring van toepasselijkheid (VVT)

| ISO27001:2023/A1:2024(NL) VERKLARING VAN TOEPASSELIJKHEID<br>STRATECH<br>VERSIE 2.2<br><br>DATUM: 24-2-2025 |                                                           |                                                                                                                                                                                                                                                                                                                               | VAN TOEPASSING? | GEÏMPLEMENTEERD? | VAN TOEPASSING VANUIT WET-<br>EN REGELGEVING | VAN TOEPASSING VANUIT<br>CONTRACT EN/OF SLA | RISICO ANALYSE | ONDERBOUWING WAAROM<br>NIET VAN TOEPASSING |
|-------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|------------------|----------------------------------------------|---------------------------------------------|----------------|--------------------------------------------|
| Nr.                                                                                                         | Onderwerp                                                 | Beheersmaatregel                                                                                                                                                                                                                                                                                                              |                 |                  |                                              |                                             |                |                                            |
| <b>5</b>                                                                                                    | <b>Organisatorische beheersmaatregelen</b>                |                                                                                                                                                                                                                                                                                                                               |                 |                  |                                              |                                             |                |                                            |
| 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                                                                                                                                                                                                                                                                 | Ja              | Ja               |                                              |                                             | X              |                                            |

|      |                                                                             |                                                                                                                                                                                                                          |    |    |  |   |   |
|------|-----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|--|---|---|
|      |                                                                             | andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.                                                                                                                                   |    |    |  |   |   |
| 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 informatiebeveiligingsincidenten   | 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]beveiligingsincidenten te definiëren, vast te stellen en te communiceren. | Ja | Ja |  |  | X |
| 5.25 | Beeoordelen van en besluiten over informatiebeveiligingsgebeurtenissen        | De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.                                                                                                                       | Ja | Ja |  |  | X |
| 5.26 | Reageren op informatiebeveiligingsincidenten                                  | Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.                                                                                                                                                                 | Ja | Ja |  |  | X |
| 5.27 | Leren van informatiebeveiligingsincidenten                                    | 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 voor het identificeren, verzamelen, verkrijgen en                                                                                                                                                                    | Ja | Ja |  |  | X |

|      |                                                            |                                                                                                                                                                                                                                          |    |    |   |   |   |  |
|------|------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|---|---|---|--|
|      |                                                            | 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 en technologieën, moeten onafhankelijk en met geplande                                   | Ja | Ja |   | X | X |  |



|          |                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |    |    |   |   |   |  |
|----------|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|---|---|---|--|
|          |                                                                   | 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 |  |
| <b>6</b> | <b>Mensgerichte beheersmaatregelen</b>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                         |    |    |   |   |   |  |
| 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 beleidsregels en procedures van                                                                                                                                                                                       | Ja | Ja |   | X | X |  |

|          |                                                                         |                                                                                                                                                                                                                                                                                            |    |    |  |   |   |
|----------|-------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|--|---|---|
|          |                                                                         | 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 |
| <b>7</b> | <b>Fysieke beheersmaatregelen</b>                                       |                                                                                                                                                                                                                                                                                            |    |    |  |   |   |
| 7.1      | Fysieke beveiligingszones                                               | Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door                                                                                                                                                                                        | Ja | Ja |  |   | X |

|      |                                                    |                                                                                                                                                                                                                   |    |    |  |   |   |
|------|----------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|--|---|---|
|      |                                                    | beveiligingszones te definiëren en te gebruiken                                                                                                                                                                   |    |    |  |   |   |
| 7.2  | Fysieke toegangsbeveiliging                        | Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen 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, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.          | Ja | Ja |  |   | X |
| 7.11 | Nutsvoorzieningen                                  | Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden                                                                                                   | Ja | Ja |  |   | X |

|          |                                                   |                                                                                                                                                                                                                                                |    |    |  |   |   |
|----------|---------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|--|---|---|
|          |                                                   | veroorzaakt door storingen in nutsvoorzieningen.                                                                                                                                                                                               |    |    |  |   |   |
| 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 |
| <b>8</b> | <b>Technologische beheersmaatregelen</b>          |                                                                                                                                                                                                                                                |    |    |  |   |   |
| 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 en softwarebibliotheken moet op passende wijze worden beheerd.                                                                                                                     | Ja | Ja |  |   | X |
| 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 gebruikersbewustzijn.                                                                                                                                                | 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                                                                                                                          | Ja | Ja |  | X | X |  |

|      |                                                    |                                                                                                                                                                                                  |    |    |  |   |   |
|------|----------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|----|--|---|---|
|      |                                                    | onderwerpspecifieke beleid inzake back-ups.                                                                                                                                                      |    |    |  |   |   |
| 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                                                                                                                                              | Ja | Ja |  | X | X |

|      |                                                              |                                                                                                                                                                                                          |     |     |  |   |                                            |
|------|--------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|-----|--|---|--------------------------------------------|
|      |                                                              | dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.                                                                                            |     |     |  |   |                                            |
| 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 | Toepassingsbeveiliging s-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.