

## Verwerkersovereenkomst SecuDoc

Over deze overeenkomst .....	2
De Verwerkersovereenkomst .....	3
Artikel 1: Definities.....	3
Artikel 2: Voorwerp van de Verwerkersovereenkomst.....	5
Artikel 3: Verwerking van Persoonsgegevens .....	5
Artikel 4: Verlenen van bijstand en medewerking .....	5
Artikel 5: Toegang tot Persoonsgegevens .....	7
Artikel 6: Beveiliging.....	8
Artikel 7: Audit .....	8
Artikel 8: Inbreuk in verband met Persoonsgegevens .....	9
Artikel 9: Doorgifte van Persoonsgegevens .....	9
Artikel 10: Vertrouwelijkheid van Persoonsgegevens.....	10
Artikel 11: Aansprakelijkheid en vrijwaring .....	10
Artikel 12: Wijziging .....	10
Artikel 13: Duur en beëindiging .....	12
Artikel 14: Toepasselijk recht en geschillenbeslechting.....	12
Bijlage A: Specificatie van de Verwerking van Persoonsgegevens.....	13
Bijlage B: Beveiligingsmaatregelen .....	15
Bijlage C: Informatie die moet worden verstrekt bij een Inbreuk in verband met Persoonsgegevens .....	16

## Over deze overeenkomst

In het kader van de AVG-wetgeving (internationaal ook wel GDPR genoemd) bieden wij u als klant deze verwerkersovereenkomst. Hierin spreken wij met u af hoe wij omspringen met in het specifiek de persoonsgegevens die wij namens u verwerken, welke afspraken wij daarover naar u maken en hoe wij deze afspraken kunnen borgen.

Omdat de AVG relatief nieuw is en interpretatie van deze wetgeving nog niet goed is uitgekristalliseerd, houden wij een dynamische versie aan. Dit betekent dat deze versie van kracht blijft tot er een nieuwe versie beschikbaar is. Wanneer er een nieuwe versie beschikbaar komt zullen wij u per e-mail op de hoogte stellen. Het huidige model is gebaseerd op de SURF Model Verwerkersovereenkomst (okt 2017 versie).

U kunt altijd een recente versie vinden onder:

[www.secudoc.nl/avg](http://www.secudoc.nl/avg)

Arnhem, 18 juni 2018

Nicolaj Nijenhuis  
Commercieel Directeur  
SecuDoc / PowerAssist B.V.

## De Verwerkersovereenkomst

**Uw organisatie** als klant van SecuDoc (geëxploiteerd door PowerAssist B.V.), in de periode dat u een betaald (buiten proefperiode zijnde) SecuDoc-abonnement afneemt (hierna: “**Verwerkingsverantwoordelijke**”);

en

**SecuDoc / PowerAssist B.V.**, gevestigd aan Nieuwe Plein 3 te Arnhem, Kamer van Koophandel nummer 53414489 en rechtsgeldig vertegenwoordigd door **Nicolaj Nijenhuis** (hierna: “**Verwerker**”);

Hierna gezamenlijk te noemen: “**Partijen**” en individueel te noemen “**Partij**”;

NEMEN HET VOLGENDE IN AANMERKING:

- Partijen hebben tijdens de afname van een SecuDoc-abonnement een zakelijke relatie die betrekking heeft op deze Overeenkomst. Ter uitvoering van de Overeenkomst verwerkt Verwerker ten behoeve van Verwerkingsverantwoordelijke Persoonsgegevens;
- In het kader van het uitvoeren van de Overeenkomst is **PowerAssist B.V.** aan te merken als Verwerker in de zin van de AVG en is uw organisatie aan te merken als verwerkingsverantwoordelijke in de zin van de AVG;
- Partijen wensen zorgvuldig en in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens om te gaan met de Persoonsgegevens die ter uitvoering van de Overeenkomst verwerkt (zullen) worden;
- Partijen wensen in overeenstemming met de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens hun rechten en plichten ten aanzien van de Verwerking van Persoonsgegevens van Betrokkenen Schriftelijk vast te leggen in deze Verwerkersovereenkomst.

### Artikel 1: Definities

In deze Verwerkersovereenkomst hebben de met hoofdletter geschreven begrippen de in dit artikel opgenomen betekenis. Waar de definitie in dit artikel in het enkelvoud is opgenomen, wordt ook het meervoud daaronder begrepen en vice versa, tenzij uitdrukkelijk anders vermeld of uit de context anders blijkt.

1.1 AVG: de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de Verwerking van Persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming).

1.2 Betrokkene: de geïdentificeerde of identificeerbare natuurlijke persoon op wie de Persoonsgegevens betrekking hebben, zoals bedoeld in artikel 4 onder 1) AVG.

1.3 Bijlage: een bijlage bij deze Verwerkersovereenkomst, die een integraal onderdeel vormt van deze Verwerkersovereenkomst.

1.4 Bijzondere categorieën Persoonsgegevens: Persoonsgegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, en genetische gegevens, biometrische gegevens met het oog op de unieke identificatie van een persoon, of gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid, zoals bedoeld in artikel 9 AVG.

1.5 Derde: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, niet zijnde de Betrokkene, noch de Verwerkingsverantwoordelijke, noch de Verwerker, noch de personen die onder rechtstreeks gezag van de Verwerkingsverantwoordelijke of de Verwerker gemachtigd zijn om Persoonsgegevens te verwerken, zoals bedoeld in artikel 4 onder 10) AVG.

1.6 Dienst: de op grond van de Overeenkomst te leveren dienst(en) door Verwerker aan Verwerkingsverantwoordelijke.

1.7 Inbreuk in verband met Persoonsgegevens: een (vermoeden van een) inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte Persoonsgegevens, zoals bedoeld in artikel 4 onder 12) AVG.

1.8 Medewerker: de door Verwerker ingeschakelde werknemers en andere personen waarvan de werkzaamheden onder zijn verantwoordelijkheid vallen en die worden ingeschakeld door Verwerker ter uitvoering van de Overeenkomst.

1.9 Ontvanger: een natuurlijke persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan, al dan niet een Derde, aan wie/waaraan de Persoonsgegevens worden verstrekt, zoals bedoeld in artikel 4 onder 9) AVG.

1.10 Overeenkomst: de overeenkomst die tussen Verwerkingsverantwoordelijke en Verwerker is gesloten en op grond waarvan Verwerker Persoonsgegevens ten behoeve van de uitvoering van deze overeenkomst voor Verwerkingsverantwoordelijke verwerkt.

1.11 Persoonsgegeven: alle informatie over een Betrokkene; als identificeerbaar wordt beschouwd een natuurlijke persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identicator zoals een naam, een identificatienummer, locatiegegevens, een online identicator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon, zoals bedoeld in artikel 4 onder 1) AVG.

1.12 PIA: de gegevensbeschermingseffectbeoordeling (privacy impact assessment) die vóór de Verwerking ten aanzien van het effect van de beoogde verwerkingsactiviteiten op de bescherming van Persoonsgegevens wordt uitgevoerd, zoals bedoeld in artikel 35 AVG.

1.13 Schriftelijk: op schrift gesteld of langs de elektronische weg, zoals bedoeld in artikel 6:227a van het Burgerlijk Wetboek.

1.14 Sub-verwerker: een andere verwerker, waaronder maar niet beperkt tot groepsmaatschappijen, zustermaatschappijen, dochtermaatschappijen en hulpleveranciers, die Verwerker inschakelt om voor rekening van de Verwerkingsverantwoordelijke specifieke verwerkingsactiviteiten te verrichten.

1.15 Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens: de toepasselijke wet- en regelgeving en/of (nadere) verdragen, verordeningen, richtlijnen, besluiten, beleidsregels, instructies en/of aanbevelingen van een bevoegde overheidsinstantie betreffende de Verwerking van Persoonsgegevens, tevens omvattende toekomstige wijziging hiervan en/of aanvulling hierop, inclusief lidstaatrechtelijke uitvoeringswetten van de AVG en de Telecommunicatiewet.

1.16 Toezichthoudende autoriteit: één of meer onafhankelijke overheidsinstanties die verantwoordelijk is of zijn voor het toezicht op de toepassing van de AVG, teneinde de grondrechten en fundamentele vrijheden van natuurlijke personen in verband met de Verwerking van hun Persoonsgegevens te beschermen en het vrije verkeer van Persoonsgegevens binnen de Unie te vergemakkelijken, zoals bedoeld in artikel 4 onder 21) en artikel 51 AVG. In Nederland is dit de Autoriteit Persoonsgegevens.

1.17 Verwerkersovereenkomst: de onderhavige overeenkomst inclusief Bijlagen, zoals bedoeld in artikel 28 lid 3 AVG.

1.18 Verwerking: een bewerking of een geheel van bewerkingen met betrekking tot Persoonsgegevens of een geheel van Persoonsgegevens, al dan niet uitgevoerd via geautomatiseerde procedés, zoals het verzamelen, vastleggen, ordenen, structureren, opslaan, bijwerken of wijzigen, opvragen, raadplegen, gebruiken,

verstrekken door middel van doorzending, verspreiden of op andere wijze ter beschikking stellen, aligneren of combineren, afschermen, wissen of vernietigen van gegevens, zoals bedoeld in artikel 4 onder 2) AVG.

## Artikel 2: Voorwerp van de Verwerkersovereenkomst

2.1 De Verwerkersovereenkomst vormt een aanvulling op de Overeenkomst en vervangt eventuele eerder gemaakte afspraken tussen Partijen ten aanzien van de Verwerking van Persoonsgegevens. Bij tegenstrijdigheid tussen de bepalingen uit de Verwerkersovereenkomst en de Overeenkomst, prevaleren de bepalingen uit de Verwerkersovereenkomst.

2.2 De bepalingen uit de Verwerkersovereenkomst gelden voor alle Verwerkingen die plaatsvinden ter uitvoering van de Overeenkomst. Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker reden heeft om aan te nemen dat Verwerker niet langer aan de Verwerkersovereenkomst kan voldoen.

2.3 Verwerkingsverantwoordelijke geeft Verwerker opdracht en instructies om de Persoonsgegevens te verwerken namens de Verwerkingsverantwoordelijke. De instructies van Verwerkingsverantwoordelijke zijn nader omschreven in de Verwerkersovereenkomst en de Overeenkomst. Verwerkingsverantwoordelijke kan naar redelijkheid Schriftelijk aanvullende of afwijkende instructies geven.

2.4 Verwerker verwerkt de Persoonsgegevens uitsluitend in opdracht van Verwerkingsverantwoordelijke en op basis van de instructies van Verwerkingsverantwoordelijke. Verwerker verwerkt de Persoonsgegevens uitsluitend voor zover de Verwerking noodzakelijk is ter uitvoering van de Overeenkomst, nimmer ten eigen nutte, ten nutte van Derden en/of voor reclamadoeleinden c.q. andere doeleinden, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

2.5 Verwerker en Verwerkingsverantwoordelijke leven de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens na. Verwerker stelt de Verwerkingsverantwoordelijke onmiddellijk in kennis indien naar mening van Verwerker een instructie van Verwerkingsverantwoordelijke inbreuk oplevert op de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

2.6 Indien Verwerker in strijd met de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens het doel en de middelen van de Verwerking van Persoonsgegevens bepaalt, wordt Verwerker voor die Verwerkingen als Verwerkingsverantwoordelijke beschouwd.

## Artikel 3: Verwerking van Persoonsgegevens

3.1 Voorafgaand aan het sluiten van de Verwerkersovereenkomst informeert Verwerker Verwerkingsverantwoordelijke in Bijlage A volledig en naar waarheid over de Verwerkingen die Verwerker ter uitvoering van de Overeenkomst uitvoert, tenzij in Bijlage A is opgenomen dat Verwerkingsverantwoordelijke de betreffende informatie in deze Bijlage opneemt. Verwerker is uitsluitend tot de in Bijlage A gespecificeerde Verwerkingen gerechtigd.

## Artikel 4: Verlenen van bijstand en medewerking

4.1 Verwerker verleent Verwerkingsverantwoordelijke alle benodigde bijstand en medewerking bij het doen nakomen van de op Partijen rustende verplichtingen op grond van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens. Verwerker verleent Verwerkingsverantwoordelijke in ieder geval bijstand met betrekking tot:

- (i) De beveiliging van Persoonsgegevens;

- (ii) Het uitvoeren van controles en audits;
- (iii) Het uitvoeren van PIA's;
- (iv) Voorafgaande raadpleging van de Toezichthoudende autoriteit;
- (v) Het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie;
- (vi) Het voldoen aan verzoeken van Betrokkenen;
- (vii) Het melden van Inbreuken in verband met Persoonsgegevens.

4.2 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van Betrokkenen, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.2.1 Verwerker neemt alle redelijke maatregelen om ervoor te zorgen dat Betrokkene zijn rechten kan uitoefenen.

4.2.2 Indien een Betrokkene met betrekking tot de uitvoering van zijn rechten direct contact opneemt met Verwerker, dan gaat Verwerker hier – behoudens uitdrukkelijke andersluidende instructie van Verwerkingsverantwoordelijke – niet (inhoudelijk) op in, maar bericht Verwerker dit onverwijld aan Verwerkingsverantwoordelijke met een verzoek om nadere instructies.

4.2.3 Indien Verwerker de Dienst rechtstreeks aanbiedt aan Betrokkene, is Verwerker verplicht om Betrokkene namens de Verwerkingsverantwoordelijke te informeren over de Verwerking van de Persoonsgegevens van Betrokkene op een wijze die in overeenstemming is met de rechten van Betrokkene.

4.3 Onder het verlenen van bijstand en medewerking met betrekking tot het voldoen aan verzoeken van de Toezichthoudende autoriteit of een andere overheidsinstantie, worden in ieder geval de volgende verplichtingen voor Verwerker verstaan:

4.3.1 Indien Verwerker een verzoek of een bevel van een Nederlandse en/of buitenlandse overheidsinstantie ontvangt met betrekking tot Persoonsgegevens, waaronder maar niet beperkt tot een verzoek van de Toezichthoudende autoriteit, informeert Verwerker Verwerkingsverantwoordelijke onverwijld, voor zover dat wettelijk is toegestaan. Bij de behandeling van het verzoek of bevel neemt Verwerker alle instructies van Verwerkingsverantwoordelijke in acht en verleent Verwerker alle redelijkerwijs benodigde medewerking aan Verwerkingsverantwoordelijke.

4.3.2 Indien het Verwerker wettelijk is verboden om te voldoen aan zijn verplichtingen op grond van artikel 4.3.1, behartigt Verwerker de redelijke belangen van Verwerkingsverantwoordelijke. Hieronder wordt in ieder geval verstaan:

4.3.2.1 Verwerker laat juridisch toetsen in hoeverre: (i) Verwerker wettelijk verplicht is om aan het verzoek of bevel te voldoen; en (ii) het Verwerker daadwerkelijk is verboden om aan zijn verplichtingen jegens Verwerkingsverantwoordelijke op grond van artikel 4.3.1 te voldoen.

4.3.2.2 Verwerker werkt alleen mee aan het verzoek of bevel indien Verwerker hiertoe wettelijk verplicht is en waar mogelijk maakt Verwerker (in rechte) bezwaar tegen het verzoek of bevel of het verbod om Verwerkingsverantwoordelijke hierover te informeren of de instructies van Verwerkingsverantwoordelijke op te volgen.

4.3.2.3 Verwerker verstrekt niet meer Persoonsgegevens dan strikt noodzakelijk om aan het verzoek of bevel te voldoen.

4.3.2.4 Verwerker onderzoekt indien sprake is van doorgifte in de zin van artikel 9 de mogelijkheden om te voldoen aan de artikelen 44 tot en met 46 AVG.

## Artikel 5: Toegang tot Persoonsgegevens

5.1 Verwerker beperkt de toegang tot Persoonsgegevens aan Medewerkers, Subverwerkers, Derden en andere Ontvangers van Persoonsgegevens tot een noodzakelijk minimum.

5.2 Verwerker verschaft uitsluitend toegang aan die Medewerkers voor wie ter uitvoering van de Overeenkomst deze toegang tot Persoonsgegevens noodzakelijk is. De categorieën Medewerkers zijn in Bijlage A gespecificeerd.

5.3 Verwerker verschaft Sub-verwerkers geen toegang tot Persoonsgegevens zonder voorafgaande algemene of specifieke Schriftelijke toestemming van Verwerkingsverantwoordelijke. Algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend indien dit expliciet in Bijlage A is opgenomen. Specifieke toestemming voor het inschakelen van Sub-verwerkers is slechts verleend aan Sub-verwerkers die in Bijlage A zijn gespecificeerd.

5.4 Verwerker licht Verwerkingsverantwoordelijke in geval van algemene Schriftelijke toestemming voor het inschakelen van Sub-verwerkers uiterlijk drie (3) maanden voorafgaand aan beoogde veranderingen inzake de toevoeging, vervanging of wijziging van Sub-verwerker(s), Schriftelijk in, waarbij de Verwerkingsverantwoordelijke de mogelijkheid wordt geboden tegen deze veranderingen bezwaar te maken. Partijen treden hierop in onderhandeling.

5.5. De algemene of specifieke toestemming van Verwerkingsverantwoordelijke voor het inschakelen Sub-verwerkers laat de verplichtingen voor Verwerker voortvloeiende uit de Verwerkersovereenkomst, waaronder maar niet beperkt tot artikel 9, onverlet. Verwerkingsverantwoordelijke kan zijn algemene of specifieke Schriftelijke toestemming voor het inschakelen van Sub-verwerkers intrekken, indien Verwerker niet of niet langer voldoet aan de verplichtingen uit de Verwerkersovereenkomst, de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

5.6 Verwerker verstrekt op eerste verzoek van Verwerkingsverantwoordelijke een overzicht van de door Verwerker ingeschakelde Sub-verwerkers aan Verwerkingsverantwoordelijke.

5.7 Verwerker legt de in de Verwerkersovereenkomst opgenomen verplichtingen op aan de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers. Verwerker draagt er zorg voor dat de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, de in de Verwerkersovereenkomst opgenomen verplichtingen naleven door middel van een Schriftelijke overeenkomst.

5.8 Verwerker brengt Verwerkingsverantwoordelijke onverwijld op de hoogte indien Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, in strijd handelen met de Verwerkersovereenkomst en/of de met Verwerker gesloten Schriftelijke overeenkomst zoals bedoeld in artikel 5.7.

5.9 Verwerker verstrekt op verzoek van Verwerkingsverantwoordelijke een afschrift van de Schriftelijke overeenkomst tussen Verwerker en de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers.

5.10 Verwerker blijft ten aanzien van de Verwerkingsverantwoordelijke volledig verantwoordelijk en volledig aansprakelijk voor het nakomen van de verplichtingen door de door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, voortvloeiende uit de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens en de verplichtingen voortvloeiende uit de Overeenkomst en de Verwerkersovereenkomst.

## Artikel 6: Beveiliging

6.1 Verwerker treft passende technische en organisatorische maatregelen om een op het risico afgestemd beveiligingsniveau te waarborgen, opdat de Verwerking aan de vereisten van de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet en de bescherming van de rechten van Betrokkenen is gewaarborgd. Verwerker treft hiertoe tenminste de technische en organisatorische maatregelen die zijn opgenomen in Bijlage B.

6.2 Bij de beoordeling van het passende beveiligingsniveau houdt Verwerker rekening met 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, vooral als gevolg van de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens, hetzij per ongeluk hetzij onrechtmatig.

6.3 Verwerker legt zijn beveiligingsbeleid Schriftelijk vast. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker inzage in het beveiligingsbeleid van Verwerker.

6.4 Het aansluiten bij een goedgekeurde gedragscode als bedoeld in artikel 40 AVG of een goedgekeurd certificeringsmechanisme als bedoeld in artikel 42 AVG kan worden gebruikt als element om aan te tonen dat de in dit artikel bedoelde vereisten worden nageleefd.

## Artikel 7: Audit

7.1 Verwerker is verplicht periodiek een onafhankelijke, externe deskundige een audit te laten uitvoeren ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.2 Verwerker verricht tenminste een keer per twee jaar een periodieke audit, zoals bedoeld in artikel 7.1. Indien Bijzondere categorieën Persoonsgegevens worden verwerkt, verricht Verwerker tenminste eenmaal per jaar een periodieke audit zoals bedoeld in artikel 7.1.

7.3 Verwerker is enkel niet gehouden tot het verrichten van een periodieke audit zoals bedoeld in artikel 7.1, indien Verwerker uitsluitend Persoonsgegevens verwerkt met een laag risico en uitdrukkelijk in Bijlage A is opgenomen dat Verwerker niet gehouden is tot het verrichten van een periodieke audit. Verwerkingsverantwoordelijke stelt vast of er sprake is van een laag risico.

7.4 Verwerker is verplicht de bevindingen van de onafhankelijke, externe deskundige, op verzoek aan Verwerkingsverantwoordelijke ter beschikking te stellen in de vorm van een verklaring, waarin de deskundige een oordeel geeft over de kwaliteit van de door Verwerker getroffen technische en organisatorische beveiligingsmaatregelen met betrekking tot de Verwerkingen die Verwerker ten behoeve van Verwerkingsverantwoordelijke verricht.

7.5 Verwerkingsverantwoordelijke heeft het recht om op zijn verzoek een audit te laten uitvoeren door een door Verwerkingsverantwoordelijke gemachtigde (rechts)persoon, ten aanzien van de organisatie van Verwerker, teneinde aan te tonen dat Verwerker aan het bepaalde in de Overeenkomst, de Verwerkersovereenkomst, de AVG en andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet.

7.6 De kosten van de periodieke audit komen voor rekening van Verwerker. De kosten van de audit op verzoek van Verwerkingsverantwoordelijke komen voor rekening van Verwerkingsverantwoordelijke, tenzij uit de bevindingen van de audit blijkt dat Verwerker de bepalingen uit de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de



Verwerking van Persoonsgegevens niet is nagekomen. Deze bepaling laat de overige rechten van Verwerkingsverantwoordelijke, waaronder het recht op schadevergoeding, onverlet.

7.7 Indien tijdens een audit wordt vastgesteld dat Verwerker niet aan het bepaalde in de Overeenkomst en/of de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens voldoet, neemt Verwerker onverwijld alle redelijkerwijs noodzakelijke maatregelen om te zorgen dat Verwerker hieraan alsnog voldoet. De bijbehorende kosten komen voor rekening van Verwerker.

## Artikel 8: Inbreuk in verband met Persoonsgegevens

8.1 Verwerker informeert Verwerkingsverantwoordelijke zonder onredelijke vertraging en uiterlijk binnen 24 uur na kennisneming, over een Inbreuk in verband met Persoonsgegevens of een redelijk vermoeden van een Inbreuk in verband met Persoonsgegevens. Verwerker informeert Verwerkingsverantwoordelijke via de contactpersoon en de contactgegevens van Verwerkingsverantwoordelijke zoals opgenomen in Bijlage A en ten minste ten aanzien van hetgeen is opgenomen in Bijlage C. Verwerker garandeert dat de verstrekte informatie volledig, correct en accuraat is.

8.2 Indien en voor zover het voor Verwerker niet mogelijk is om alle informatie uit Bijlage C gelijktijdig te verstrekken, kan de informatie zonder onredelijke vertraging en uiterlijk binnen 24 uur na het ontdekken, in stappen worden verstrekt aan Verwerkingsverantwoordelijke.

8.3 Verwerker heeft adequaat beleid en adequate procedures ingericht om Inbreuken in verband met Persoonsgegevens in een zo vroeg mogelijk stadium te detecteren, Verwerkingsverantwoordelijke hierover uiterlijk binnen 24 uur te informeren, hierop adequaat en onmiddellijk te reageren, (verdere) onbevoegde kennisneming, wijziging, en verstrekking dan wel anderszins onrechtmatige Verwerking te voorkomen of te beperken en herhaling hiervan te voorkomen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker informatie over en inzage in dit door Verwerker ingerichte beleid en deze door Verwerker ingerichte procedures.

8.4 Verwerker houdt Schriftelijk een register bij van alle Inbreuken in verband met Persoonsgegevens die betrekking hebben op of verband houden met de (uitvoering van de) Overeenkomst, met inbegrip van de feiten omtrent de Inbreuk in verband met Persoonsgegevens, de gevolgen daarvan en de getroffen corrigerende maatregelen. Op verzoek van Verwerkingsverantwoordelijke verschaft Verwerker Verwerkingsverantwoordelijke een afschrift van dit register.

## Artikel 9: Doorgifte van Persoonsgegevens

9.1 Persoonsgegevens mogen enkel worden doorgegeven aan derde landen of internationale organisaties indien sprake is van een passend beschermingsniveau en Verwerkingsverantwoordelijke hiervoor specifieke Schriftelijke toestemming heeft verleend. Deze specifieke Schriftelijke toestemming is slechts verleend indien dit is opgenomen in Bijlage A. Verwerker is uitsluitend gerechtigd tot deze in Bijlage A gespecificeerde doorgiften aan derde landen of internationale organisaties, tenzij een op Verwerker van toepassing zijnde Unierechtelijke of lidstaatrechtelijke bepaling Verwerker tot Verwerking verplicht. In dat geval stelt Verwerker Verwerkingsverantwoordelijke voorafgaand aan de Verwerking Schriftelijk op de hoogte van deze bepaling, tenzij die wetgeving deze kennisgeving om gewichtige redenen van algemeen belang verbiedt.

9.2 Verwerkingsverantwoordelijke kan aan de Schriftelijke toestemming, zoals bedoeld in artikel 9.1, nadere voorwaarden verbinden, waaronder maar niet beperkt tot het aantonen dat aan de vereisten zoals opgenomen in artikel 9.3 is voldaan.

9.3 Verwerkingsverantwoordelijke kan Verwerker slechts toestemming verlenen voor een doorgifte van Persoonsgegevens aan derde landen of internationale organisaties indien, ofwel:

(i) Een adequaatheidsbesluit overeenkomstig artikel 45 lid 3 AVG is genomen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(ii) Passende waarborgen overeenkomstig artikel 46 AVG met inbegrip van bindende voorschriften zoals bedoeld in artikel 47 AVG, zijn getroffen ten aanzien van het betreffende derde land of de betreffende internationale organisatie; ofwel

(iii) Aan één van de specifieke voorwaarden uit artikel 49 lid 1 AVG is voldaan ten aanzien van het betreffende derde land of de betreffende internationale organisatie.

## Artikel 10: Vertrouwelijkheid van Persoonsgegevens

10.1 Alle Persoonsgegevens worden als vertrouwelijke gegevens gekwalificeerd en dienen als zodanig te worden behandeld.

10.2 Partijen houden alle Persoonsgegevens geheim en maken deze op geen enkele wijze verder intern of extern bekend, behalve voor zover:

(i) Bekendmaking en/of verstrekking van de Persoonsgegevens in het kader van de uitvoering van de Overeenkomst of Verwerkersovereenkomst noodzakelijk is;

(ii) Enig dwingendrechtelijk wettelijk voorschrift of rechterlijke uitspraak Partijen tot bekendmaking en/of verstrekking van die Persoonsgegevens verplicht, waarbij Partijen eerst de andere Partij hiervan op de hoogte stellen;

(iii) Bekendmaking en/of verstrekking van die Persoonsgegevens geschiedt met voorafgaande Schriftelijke toestemming van de andere Partij.

10.3 Overtreding van artikel 10.1 en/of artikel 10.2 wordt beschouwd als een Inbreuk in verband met Persoonsgegevens.

## Artikel 11: Aansprakelijkheid en vrijwaring

11.1 Verwerker is aansprakelijk voor alle schade die voortvloeit uit of verband houdt met het niet nakomen van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

11.2 Verwerker vrijwaart Verwerkingsverantwoordelijke voor alle aanspraken, boeten en/of maatregelen van derden, daaronder begrepen Betrokkenen en de Toezichthoudende autoriteit, die jegens Verwerkingsverantwoordelijke worden ingesteld of opgelegd wegens een schending van de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens door Verwerker en/of door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Subverwerkers.

11.3 Verwerker draagt zorg voor afdoende dekking van de aansprakelijkheid door middel van een aansprakelijkheidsverzekering. Op verzoek van Verwerkingsverantwoordelijke geeft Verwerker Verwerkingsverantwoordelijke inzage in (de polis van) deze aansprakelijkheidsverzekering van Verwerker.

## Artikel 12: Wijziging

12.1 Verwerker is verplicht Verwerkingsverantwoordelijke onmiddellijk te informeren over voorgenomen wijzigingen in de Dienst, de uitvoering van de Overeenkomst en de uitvoering van de Verwerkersovereenkomst die betrekking hebben op de Verwerking van Persoonsgegevens. Hieronder wordt in ieder geval verstaan:

(i) Wijzigingen die invloed (kunnen) hebben op de te verwerken (categorieën) Persoonsgegevens;

(ii) Wijziging van de middelen waarmee de Persoonsgegevens worden verwerkt;

(iii) Het inschakelen van andere Sub-verwerkers;

(iv) Wijziging in de doorgifte van Persoonsgegevens aan derde landen en/of internationale organisaties.

12.2 Indien een wijziging met betrekking tot de Verwerking van Persoonsgegevens of een audit daartoe aanleiding geeft, treden Partijen op eerste verzoek van Verwerkingsverantwoordelijke in overleg over het wijzigen van de Verwerkersovereenkomst.

12.3 Wijzigingen die betrekking hebben op de Verwerking van Persoonsgegevens mogen nooit tot gevolg hebben dat Verwerkingsverantwoordelijke niet kan voldoen aan de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens.

12.4 In geval van nietigheid of vernietigbaarheid van één of meer bepalingen van de Verwerkersovereenkomst, blijven de overige bepalingen onverkort van kracht.

### Artikel 13: Duur en beëindiging

13.1 De duur van de Verwerkersovereenkomst is gelijk aan de duur van de Overeenkomst. De Verwerkersovereenkomst is niet los van de Overeenkomst te beëindigen. Bij beëindiging van de Overeenkomst eindigt de Verwerkersovereenkomst van rechtswege en vice versa.

13.2 Verwerkingsverantwoordelijke is gerechtigd de Verwerkersovereenkomst op te zeggen, indien Verwerker niet voldoet of niet langer kan voldoen aan de Verwerkersovereenkomst en/of de AVG en/of andere Toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens, zonder dat Verwerker aanspraak maakt op enige schadevergoeding. Bij de opzegging neemt Verwerkingsverantwoordelijke een redelijke opzegtermijn in acht, tenzij de omstandigheden onmiddellijke opzegging rechtvaardigen.

13.3 Binnen een maand nadat de Overeenkomst eindigt, vernietigt en/of retourneert Verwerker alle Persoonsgegevens en/of draagt Verwerker deze over aan Verwerkingsverantwoordelijke en/of een andere door Verwerkingsverantwoordelijke aan te wijzen partij, naar gelang de keuze van Verwerkingsverantwoordelijke. Alle bestaande (overige) kopieën van Persoonsgegevens, zich al dan niet bevindende bij door Verwerker ingeschakelde (rechts)personen, waaronder maar niet beperkt tot Medewerkers en/of Sub-verwerkers, worden hierbij aantoonbaar permanent verwijderd, tenzij opslag van de Persoonsgegevens Unierechtelijk of lidstaatrechtelijk is verplicht.

13.4 Verwerker bevestigt op verzoek van Verwerkingsverantwoordelijke Schriftelijk dat Verwerker aan alle verplichtingen uit artikel 13.3 heeft voldaan.

13.5 Verwerker draagt de kosten voor vernietiging, retournering en/of overdracht van de Persoonsgegevens. Verwerkingsverantwoordelijke kan nadere eisen stellen aan de wijze van vernietiging, retournering en/of overdracht van de Persoonsgegevens, waaronder eisen aan het bestandsformaat.

13.6 Verplichtingen uit de Verwerkersovereenkomst die naar hun aard bestemd zijn om na beëindiging van de Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst voortduren.

### Artikel 14: Toepasselijk recht en geschillenbeslechting

14.1 De Verwerkersovereenkomst en de uitvoering daarvan worden beheerst door Nederlands recht.

14.2 Alle geschillen, die tussen Partijen ontstaan in verband met de Verwerkersovereenkomst, zullen worden voorgelegd aan de bevoegde rechter in de plaats waar Verwerker gevestigd is.

## Bijlage A: Specificatie van de Verwerking van Persoonsgegevens

Omschrijving van de verwerking:

- Het (tijdelijk) opslaan van (versleutelde) bestanden en de opslag/registratie van naam, e-mailadres en wachtwoord van gebruikers en derden aan wie bestanden en/of droplinks worden gestuurd

Doeleinde van de verwerking:

- Het mogelijk maken om (grote) bestanden op een veilige manier te versturen en te ontvangen tussen twee gebruikers (e-mailadressen)

Categorie betrokkenen:

- SecuDoc-gebruikers (inclusief accounthouders, beheerders en externe ontvangers)

Persoonsgegevens:

- Volledige naam – *nodig voor identificatie gebruiker of verzender/ontvanger*
- E-mailadres – *nodig om in te loggen, voor wachtwoordherstel of om bestanden te versturen/ontvangen*
- Wachtwoord – *nodig voor inloggen; wordt versleuteld opgeslagen (als hash)*
- IP-adres – *nodig voor tracking van bestandsoverdrachten en logging*

Periodieke audit:

- Er is voor gekozen om **niet** periodiek een audit uit te voeren, maar alleen wanneer de Verwerkingsverantwoordelijke hier expliciet naar vraagt (binnen de kaders van de Overeenkomst). Dit omdat het type gegevens volgens een vaste methode is beveiligd/gestructureerd die gebonden is aan het systeem, en hiermee regelmatige audits overbodig zijn.

Medewerkers die gegevens verwerken/toegang hebben tot de (persoons)gegevens in SecuDoc:

Naam	Gerelateerde functie	Reden
Wim Wisselink	Technisch Directeur	Onderhoud, probleemoplossing.
Nicolaj Nijenhuis	Commercieel Directeur	Toezichthouder, ondersteuning.
Mehran Khanpour	Account-/Projectmanager	Probleemoplossing, gebruikersondersteuning
Tom Niemantsverdriet	Back-end developer	Onderhoud, probleemoplossing.

Subverwerkers die theoretisch gezien toegang hebben/zouden kunnen verkrijgen tot de data (maar minimaal onder verwerkersovereenkomst staan met PowerAssist B.V.):

Organisatie	Rol	Land van verwerking
TransIP	Hostingplatform (servers zelf zijn echter in eigen beheer)	Nederland
CloudVPS	Hostingplatform (servers zelf zijn echter in eigen beheer)	Nederland

Contactgegevens van de Verwerker (bij Inbreuk in verband met Persoonsgegevens)

Organisatie	Naam	Gerelateerde functie	E-mailadres	Telefoonnummer
PowerAssist B.V.	Nicolaj Nijenhuis	Commercieel Directeur	<a href="mailto:nicolaj@powerassist.nl">nicolaj@powerassist.nl</a>	026-2022045
PowerAssist B.V.	Wim Wisselink	Technisch Directeur	<a href="mailto:wim@powerassist.nl">wim@powerassist.nl</a>	026-2022045

## Bijlage B: Beveiligingsmaatregelen

De door Verwerker getroffen beveiligingsmaatregelen:

#	Type maatregel	Beschrijving
T1	Technisch	Persoonsgegevens in SecuDoc worden altijd versleuteld opgeslagen, en wachtwoorden gehasht (en dubbel gesalt). Wanneer de database uit zou lekken is het niet mogelijk hier wachtwoorden uit te herleiden.
T2	Technisch	Alle opgeleverde SecuDoc-omgevingen zijn minimaal voorzien van een basis SSL-certificaat.
T3	Technisch	Alle medewerkers die beheerderstoegang hebben tot SecuDoc hebben verplicht secundaire authenticatie ingesteld (Google Authenticator of Yubikey)
T4	Technisch	Alle hosting vindt plaats in een ISO 9001, ISO 27001 en NEN 7510 gecertificeerd datacentrum in Amsterdam en/of Delft, Nederland.
T5	Technisch	PowerAssist B.V. heeft geen toegang tot de bestanden die met SecuDoc worden verstuurd doordat deze versleuteld worden opgeslagen waarbij een deel van de sleutel naar de ontvanger wordt gestuurd en niet meer op de server aanwezig is.
T6	Technisch	Toegangslogs (accesslogs) van onze servers die IP-adressen en gebruikersaccounts loggen voor acties op onze websites (zowel beheersysteem als bezoekerstoegang) verwijderen deze gegevens automatisch na 3 maanden.
O1	Organisatorisch	Alleen medewerkers die direct klantondersteuning of technische ondersteuning geven hebben toegang tot de database van SecuDoc en mogelijk ingesloten Persoonsgegevens; zie Bijlage A.
O2	Organisatorisch	Bij het ontwikkelen en probleemoplossen van SecuDoc downloaden wij nooit de live database naar onze lokale systemen of andere online ontwikkelomgevingen.
O3	Organisatorisch	Hardeschijven, USB-sticks en andere gegevensdragers die niet meer in gebruik zijn door PowerAssist B.V. worden vernietigd door een gecertificeerde instantie.
O4	Organisatorisch	PowerAssist B.V. hanteert voor haar medewerkers een no-USB-stick policy; dat betekent dat het medewerkers niet is toegestaan eigen USB-sticks in kantoorcomputers te gebruiken en/of zonder toestemming werk naar huis mee te nemen.
O5	Organisatorisch	PowerAssist B.V. hanteert voor haar medewerkers een lockscreen policy. Dat betekent dat schermen bij afwezigheid van het computerscherm op slot worden gezet.
O6	Organisatorisch	Alle medewerkers met toegang tot Persoonsgegevens hebben een geheimhoudingsverklaring met boeteclausule ondertekend.

## Bijlage C: Informatie die moet worden verstrekt bij een Inbreuk in verband met Persoonsgegevens

- Naam, functie, e-mailadres en telefoonnummer van de melder
- Samenvatting van het incident waarbij Inbreuk op de beveiliging van Persoonsgegevens zich heeft voorgedaan
- Van hoeveel personen zijn Persoonsgegevens betrokken bij de Inbreuk
  - Exact aantal of minimaal & maximaal
- Omschrijf de groep mensen van wie Persoonsgegevens zijn betrokken (Categorieën Betrokkenen) bij de Inbreuk
- Wanneer vond de Inbreuk plaats?
  - Datum (of tussen de volgende data)
  - Tijdstip (of in het volgende tijdvak)
- Wat is de aard van de Inbreuk?
  - Lezen (vertrouwelijkheid)
  - Kopiëren
  - Veranderen (integriteit)
  - Verwijderen of vernietigen (beschikbaarheid)
  - Diefstal
  - Onbekend
- Om welk type Persoonsgegevens gaat het?
  - NAW-gegevens
  - Telefoonnummers
  - E-mailadressen of andere adressen voor elektronische communicatie
  - Toegangs- of identificatiegegevens (bijv. gebruikersnaam en wachtwoord of klantnummer)
  - Financiële gegevens (bijv. rekeningnummer of creditcardnummer)
  - Geuploade databestanden (inhoud van overdrachten)
- Welke gevolgen kan de Inbreuk hebben voor de persoonlijke levenssfeer van de Betrokkenen?
  - Stigmatisering of uitzondering
  - Schade aan de gezondheid
  - Blootstelling aan (identiteits)fraude
  - Blootstelling aan spam of phishing
  - Overige (incl. toelichting)
- Welke maatregelen (technisch en organisatorisch) zijn vanuit de organisatie getroffen om de Inbreuk te beperken, aan te pakken en om verdere Inbreuken te voorkomen?
- Zijn de Persoonsgegevens versleuteld, gehasht of op andere manier onbegrijpelijk of ontoegankelijk gemaakt voor onbevoegden?
  - Ja (incl. methode)
  - Nee (incl. methode)
  - Deels (gespecificeerd per Persoonsgegeven) (incl. methode)
- Heeft de Inbreuk betrekking op personen in andere EU-landen?
  - Ja
  - Nee
  - Onbekend