Gegevensverwerkersovereenkomst

Ondergetekenden:

Wolters Kluwer Nederland BV, statutair gevestigd te 7418 CJ Deventer aan de Staverenstraat 15 (hierna te noemen: "**Verwerker**"),

en

Naam Verantwoordelijke **……..**, gevestigd te postcode **…….** plaats **……..**

aan de *[adres en huisnummer]* **……..**,

(hierna te noemen: "**Verantwoordelijke**"), hierna gezamenlijk te noemen: "**Partijen**" en elk afzonderlijk: een "**Partij**",

verklaren te zijn overeengekomen als volgt:

OVERWEGENDE DAT

Partijen zijn overeengekomen dat Verantwoordelijke gebruikt maak van de Online aangiftesoftware voor fiscale professionals van Verwerker. Verwerker verwerkt persoonsgegevens van de Verantwoordelijke in het kader van de uitvoering van de overeenkomst.

Teneinde Partijen in staat te stellen uitvoering te geven aan hun relatie op een manier die in overeenstemming is met de wet, zijn Partijen deze Gegevensverwerkingsovereenkomst ("GVO") aangegaan, als volgt:

1. Definities

In het kader van deze GVO betekent:

"Toepasselijke Gegevensbeschermingswet"	: de wetgeving die bescherming biedt voor de fundamentele rechten en vrijheden van personen en met name hun recht op privacy met betrekking tot de Verwerking van Persoonsgegevens, welke wetgeving van toepassing is op Verantwoordelijke en Verwerker; de term Toepasselijke Gegevensbeschermingswet omvat tevens de AVG.
"Verantwoordelijke"	: de klant van Verwerker die, als natuurlijke of rechtspersoon, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt;
"Algemene Verordening Gegevensbescherming" of "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 in werking getreden

	20 dagen na publicatie (4 mei 2016) en van toepassing vanaf 25 mei 2018;
“Internationale Organisatie”	: een organisatie en de daaronder vallende internationaal publiekrechtelijke organen of andere organen die zijn opgericht bij of op grond van een overeenkomst tussen twee of meer landen;
“Lidstaat"	: een land dat tot de Europese Unie behoort;
"Persoonsgegevens”	: alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon (Betrokkene);
"Betrokkene"	: een identificeerbare persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon;
"Inbreuk in verband met Persoonsgegevens"	: 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 gegevens;
"Verwerken/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;
"Verwerker"	: Wolters Kluwer Nederland BV;
"Overeenkomst van Dienstverlening"	: de hoofdovereenkomst die is gesloten tussen Verantwoordelijke en Verwerker en waarin de voorwaarden voor het verlenen van de Diensten zijn uiteengezet;
"Diensten"	: de diensten verleend door Verwerker aan Verantwoordelijke en beschreven onder ‘onderwerp van de verwerking’ in Bijlage 1 bij deze GVO;
"Bijzondere Categorieën Gegevens"	: gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken; genetische gegevens, biometrische gegevens die worden Verwerkt met het oog op de unieke identificatie van een natuurlijke persoon; gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;

"Subverwerker"	: een gegevensverwerker die door Verwerker wordt ingeschakeld en die zich bereid verklaart Persoonsgegevens van Verwerker te ontvangen die uitsluitend zijn bedoeld voor Verwerkingsactiviteiten die moeten worden uitgevoerd ten behoeve van Verantwoordelijke in overeenstemming met diens instructies, de voorwaarden van deze GVO en de voorwaarden van een schriftelijke subverwerkingsovereenkomst;
"Toezichthoudende Autoriteit"	: een door een Lidstaat ingevolge artikel 51 AVG ingestelde onafhankelijke overheidsinstantie;
"Technische en Organisatorische Beveiligingsmaatregelen"	: de maatregelen gericht op de bescherming van Persoonsgegevens tegen onopzettelijke vernietiging of onopzettelijk(e) verlies, wijziging, onbevoegde bekendmaking of toegang, met name waar de Verwerking de doorzending van gegevens via een netwerk behelst, en tegen alle andere onrechtmatige vormen van Verwerking; en
“Derde Land”	: een land met betrekking waartoe de Europese Commissie niet heeft beslist dat dat land, of een gebied of een of meer gespecificeerde sectoren binnen dat land, een passend beschermingsniveau garandeert.

2. Details van de Verwerking

De details van de Verwerkingsactiviteiten die door Verwerker ten behoeve van Verantwoordelijke worden verricht als gegevensverwerker die daartoe opdracht heeft gekregen (zoals het onderwerp van de verwerking, de aard en het doel van de verwerking, het soort persoonsgegevens en categorieën van betrokkenen) zijn vermeld in Bijlage 1 bij deze GVO.

3. Rechten en verplichtingen van Verantwoordelijke

Verantwoordelijke blijft de verwerkersverantwoordelijke als bedoeld in de AVG voor de Verwerking van de Persoonsgegevens conform de instructies aan Verwerker op grond van de Overeenkomst van Dienstverlening, deze GVO en eventuele andere instructies. Verantwoordelijke heeft Verwerker opdracht gegeven, en zal Verwerker gedurende de looptijd van de gegevensverwerking waartoe opdracht is gegeven opdracht blijven geven, de Persoonsgegevens uitsluitend te verwerken ten behoeve van Verantwoordelijke en in overeenstemming met de Toepasselijke Gegevensbeschermingswet, de Overeenkomst van Dienstverlening, deze GVO en instructies van Verantwoordelijke. Verantwoordelijke is gerechtigd en verplicht om Verwerker instructies te geven in verband met de Verwerking van de Persoonsgegevens, zowel in het algemeen als in individuele gevallen. Instructies kunnen ook betrekking hebben op het rectificeren, wissen en blokkeren van de Persoonsgegevens. Instructies worden in het algemeen schriftelijk gegeven, tenzij de urgentie of andere specifieke omstandigheden een andere (bijvoorbeeld mondelinge of elektronische) vorm vereisen. Niet-schriftelijke instructies moeten onverwijld door Verantwoordelijke schriftelijk worden bevestigd. Voor zover de uitvoering van een instructie leidt tot kosten voor Verwerker zal Verwerker Verantwoordelijke eerst in kennis stellen van die kosten. Pas nadat

Verantwoordelijke heeft bevestigd dat de kosten voor de uitvoering van een instructie voor zijn rekening komen, zal Verwerker die instructie uitvoeren.

4. Verplichtingen van Verwerker

Verwerker zal:

(a) de Persoonsgegevens uitsluitend verwerken conform de instructies van Verantwoordelijke en ten behoeve van Verantwoordelijke; die instructies worden gegeven in de Overeenkomst van Dienstverlening, deze GVO en anderszins in gedocumenteerde vorm zoals genoemd in artikel 3 hiervoor. Die verplichting om de instructies van Verantwoordelijke op te volgen geldt ook voor de doorgifte van de Persoonsgegevens aan een Derde Land of een Internationale Organisatie;

(b) Verantwoordelijke onmiddellijk informeren indien Verwerker een instructie van Verantwoordelijke om enigerlei reden niet kan naleven;

(c) ervoor zorgen dat personen die door Verwerker gemachtigd zijn om de Persoonsgegevens ten behoeve van Verantwoordelijke te Verwerken toezeggen geheimhouding te zullen betrachten of dat op die personen een passende geheimhoudingsplicht rust en dat de personen die toegang hebben tot de Persoonsgegevens die Persoonsgegevens zullen Verwerken conform de instructies van Verantwoordelijke;

(d) de Technische en Organisatorische Beveiligingsmaatregelen doorvoeren die voldoen aan de vereisten van de Toepasselijke Gegevensbeschermingswet zoals nader gespecificeerd in Bijlage 2 alvorens de Persoonsgegevens te Verwerken en ervoor zorgen dat hij Verantwoordelijke voldoende garanties biedt voor wat betreft die Technische en Organisatorische Beveiligingsmaatregelen;

(e) Verantwoordelijke assisteren door middel van passende Technische en Organisatorische Maatregelen, voor zover haalbaar, voor de nakoming van de verplichting van Verantwoordelijke om in te gaan op verzoeken voor de uitoefening van de rechten van de Betrokkenen betreffende informatie, toegang, rectificatie en wissing, beperking van verwerking, kennisgeving, gegevensportabiliteit, bezwaar en geautomatiseerde besluitvorming; voor zover die haalbare Technische en Organisatorische Maatregelen veranderingen of wijzigingen in de Technische en Organisatorische Maatregelen vereisen zoals genoemd in Bijlage 2, zal Verwerker Verantwoordelijke informeren over de kosten van doorvoering van die aanvullende of gewijzigde Technische en Organisatorische Maatregelen. Zodra Verantwoordelijke heeft bevestigd dat die kosten voor zijn rekening komen, zal Verwerker die aanvullende of gewijzigde Technische en Organisatorische Maatregelen doorvoeren om Verantwoordelijke te assisteren bij het ingaan op verzoeken van betrokkenen;

(f) alle informatie aan Verantwoordelijke beschikbaar stellen die nodig is om aan te tonen dat de in deze GVO en in Art. 28 AVG genoemde verplichtingen worden nagekomen, en controles, waaronder inspecties door Verantwoordelijke of een andere controleur die daartoe is gemandateerd door Verantwoordelijke, mogelijk maken en daaraan bijdragen.

Verantwoordelijke is zich ervan bewust dat controles in persoon en op locatie de bedrijfsactiviteiten van Verwerker aanzienlijk kunnen verstoren en veel geld en tijd kunnen kosten. Derhalve mag Verantwoordelijke een controle in persoon en op locatie uitsluitend uitvoeren indien Verantwoordelijke de (on)kosten die door Verwerker zijn gemaakt als gevolg van de verstoring van de bedrijfsactiviteiten aan Verwerker vergoedt;

(g) Verantwoordelijke zonder onnodige vertraging in kennis stellen:

(i) van enig juridisch bindend verzoek om verstrekking van de Persoonsgegevens door een wethandhavingsinstantie, tenzij deze kennisgeving anderszins is verboden, zoals een strafrechtelijk verbod dat ten doel heeft de vertrouwelijkheid van een wetshandhavingsonderzoek te bewaren;

(ii) van klachten en verzoeken die direct van Betrokkenen zijn ontvangen (bijvoorbeeld klachten en verzoeken om toegang, rectificatie, wissing, beperking van verwerking, gegevensportabiliteit, bezwaar tegen verwerking van gegevens, geautomatiseerde besluitvorming) zonder op dat verzoek in te gaan, tenzij hij daartoe anderszins is gemachtigd;

(iii) indien Verwerker op grond van EU-wetgeving of de wetgeving van een Lidstaat die op Verwerker van toepassing is verplicht is de Persoonsgegevens te verwerken buiten het kader van de opdracht van Verantwoordelijke, alvorens die verwerking uit te voeren buiten dat kader, tenzij die EU-wetgeving of wetgeving van die Lidstaat die informatie verbiedt om gewichtige redenen van algemeen belang; die kennisgeving moet de wettelijke vereiste uit hoofde van die EU-wetgeving of de wetgeving van de Lidstaat vermelden;

(iv) indien, naar de mening van Verwerker, een instructie in strijd is met de Toepasselijke Gegevensbeschermingswet; bij het verstrekken van die kennisgeving is Verwerker niet verplicht de instructie op te volgen, tenzij en totdat Verantwoordelijke deze heeft bevestigd of gewijzigd; en

(v) zodra Verwerker zich bewust wordt van een Inbreuk in verband met Persoonsgegevens bij Verwerker uiterlijk binnen 24 uur na ontdekking. In geval van zo'n Inbreuk in verband met Persoonsgegevens zal Verwerker Verantwoordelijke, op schriftelijk verzoek van Verantwoordelijke, assisteren bij de verplichting van Verantwoordelijke uit hoofde van Toepasselijke Gegevensbeschermingswet om de betrokkenen respectievelijk de Toezichthoudende Autoriteiten te informeren, en om de Inbreuk in verband met Persoonsgegevens te documenteren. Contactgegevens met betrekking tot de melding worden vastgelegd in het klantenservice systeem. Contactpersonen worden gespecificeerd in bijlage 1;

(h) Verantwoordelijke assisteren bij een Gegevensbeschermingeffectbeoordeling zoals vereist op grond van art. 35 AVG die betrekking heeft op de door Verwerker aan Verantwoordelijke verleende Diensten en de Persoonsgegevens die door Verwerker ten behoeve van Verantwoordelijke worden verwerkt;

(i) alle vragen van Verantwoordelijke met betrekking tot zijn Verwerking van de te verwerken Persoonsgegevens behandelen (bijvoorbeeld door Verantwoordelijke in staat te stellen tijdig te reageren op klachten of verzoeken van Betrokkenen) en gehoor geven aan het advies van de Toezichthoudende Autoriteit betreffende de Verwerking van de doorgegeven gegevens;

(j) voor zover Verwerker verplicht en gevraagd is Persoonsgegevens die op grond van deze GVO zijn verwerkt te rectificeren, te wissen en/of te blokkeren, dit onverwijld doen. Indien en voor zover Persoonsgegevens niet kunnen worden gewist op grond van wettelijke vereisten in verband met gegevensbewaring, dient Verwerker, in plaats van de desbetreffende Persoonsgegevens te wissen, de verdere Verwerking en/of het verdere gebruik van Persoonsgegevens te beperken, of de bijbehorende identiteit uit de Persoonsgegevens te verwijderen (hierna te noemen: "blokkeren"). Indien zo'n blokkeringsverplichting van toepassing is op Verwerker, dient Verwerker de desbetreffende Persoonsgegevens uiterlijk op de laatste dag van het kalenderjaar waarin de bewaartermijn eindigt, te wissen.

5. Subverwerking

(a) Verantwoordelijke geeft toestemming voor het gebruik van Subverwerker(s) die door Verwerker worden ingeschakeld voor het verlenen van de Diensten. Verantwoordelijke verleent zijn goedkeuring voor de Subverwerker(s) zoals gespecifieerd op www.wolterskluwer.nl/algemene-voorwaarden/subverwerkers.

(b) In het geval dat Verwerker voornemens is nieuwe of meer Subverwerkers in te schakelen, zorgt Verwerker ervoor dat de url ge-update wordt en zal Verwerker hierover Verantwoordelijke informeren. Indien Verantwoordelijke redelijke grond heeft om bezwaar te maken tegen het gebruik van nieuwe of meer Subverwerkers, dient Verantwoordelijke Verwerker daarvan onmiddellijk schriftelijk binnen 14 dagen na ontvangst van de Kennisgeving Subverwerker in kennis te stellen. In het geval dat Verantwoordelijke bezwaar maakt tegen een nieuwe of andere Subverwerker, en dat bewaar niet onredelijk is, zal Verwerker redelijke inspanningen verrichten om wijzigingen in de Diensten beschikbaar te stellen aan Verantwoordelijke of een commercieel redelijke wijziging aan te bevelen in de configuratie van Verantwoordelijke of het gebruik door Verantwoordelijke van de Diensten ter voorkoming van Verwerking van Persoonsgegevens door de nieuwe of andere Subverwerker waartegen bezwaar is gemaakt, zonder Verantwoordelijke daarbij onredelijk te belasten. Indien Verwerker die wijziging niet binnen een redelijke termijn beschikbaar kan stellen, welke termijn niet meer zal bedragen dan zestig (60) dagen, mag Verantwoordelijke het getroffen deel van de Overeenkomst van Dienstverlening beëindigen, echter uitsluitend met betrekking tot die Diensten die niet door Verwerker kunnen worden verleend zonder het gebruik van de nieuwe of andere Subverwerker waartegen bezwaar is gemaakt door middel van schriftelijke kennisgeving aan Verwerker.

(c) Verwerker legt dezelfde gegevensbeschermingsverplichting als genoemd in deze GVO contractueel op aan alle Subverwerkers. De overeenkomst tussen Verwerker en

Subverwerker biedt met name voldoende garanties voor doorvoering van de Technische en Organisatorische Beveiligingsmaatregelen zoals genoemd in Bijlage 2, voor zover die Technische en Organisatorische Beveiligingsmaatregelen van belang zijn voor de door de Subverwerker verleende diensten.

(d) Verwerker kiest de Subverwerker met de nodige zorg.

(e) Verwerker blijft aansprakelijk jegens Verantwoordelijke voor nakoming van de verplichtingen van Subverwerker, in het geval dat Subverwerker zijn verplichtingen niet nakomt. Verwerker is echter niet aansprakelijk voor schade en vorderingen voortvloeiend uit instructies van Verantwoordelijke aan Subverwerkers.

6. Internationale doorgifte

De Verwerker zal de Persoonsgegevens verwerken binnen de Europese Economische Ruimte ("EER"). De Verwerker zal de Persoonsgegevens niet overdragen aan, of anderszins verwerken in, een Derde Land of Internationale Organisatie, tenzij de Verantwoordelijke daartoe voorafgaande schriftelijke toestemming heeft gegeven aan welke toestemming de Verantwoordelijke aanvullende voorwaarden en vereisten mag stellen, zoals het aangaan van de standaardbepalingen inzake gegevensbescherming zoals bedoeld in artikel 46 lid 2 sub c AVG.

7. Beperking aansprakelijkheid

Alle aansprakelijkheid voortvloeiend uit of verband houdend met deze GVO volgt, en wordt uitsluitend beheerst door, de aansprakelijkheidsbepalingen uiteengezet in, of anderszins van toepassing op, de Overeenkomst van Dienstverlening. Derhalve, en ter berekening van aansprakelijkheidslimieten en/of ter bepaling van de toepassing van andere beperkingen van aansprakelijkheid, wordt elke aansprakelijkheid die zich uit hoofde van deze GVO voordoet, geacht zich voor te doen uit hoofde van de desbetreffende Overeenkomst van Dienstverlening.

8. Duur en beëindiging

(a) De looptijd van deze GVO is gelijk aan die van de desbetreffende Overeenkomst van Dienstverlening. Tenzij in deze overeenkomst anders is bepaald zijn rechten en verplichtingen op het gebied van beëindiging dezelfde als de rechten en verplichtingen die zijn opgenomen in de desbetreffende Overeenkomst van Dienstverlening.

(b) Verwerker dient, naar keuze van Verantwoordelijke, alle Persoonsgegevens na het einde van de verlening van de Diensten te wissen of aan Verantwoordelijke te retourneren, en alle bestaande kopieën te wissen tenzij Verwerker op grond van EU-wetgeving of wetgeving van een Lidstaat verplicht is die Persoonsgegevens te bewaren.

9. Overige

(a) In het geval van strijdigheid tussen het bepaalde in deze GVO en enige andere overeenkomsten tussen Partijen, prevaleert het bepaalde in deze GVO met betrekking tot de gegevensbeschermingsverplichtingen van Partijen. In geval van twijfel over de vraag of

clausules in die andere overeenkomsten betrekking hebben op de gegevensbeschermingsverplichtingen van Partijen prevaleert deze GVO.

(b) Ongeldigheid of onafdwingbaarheid van enige bepaling in deze GVO heeft geen gevolgen voor de geldigheid of afdwingbaarheid van de overige bepalingen van deze GVO. De ongeldige of onafdwingbare bepaling wordt (i) zo gewijzigd dat de geldigheid of afdwingbaarheid ervan wordt gegarandeerd en tegelijkertijd de intenties van Partijen zo veel mogelijk bewaard blijven of – indien dit niet mogelijk is – (ii) zo uitgelegd alsof het ongeldige of onafdwingbare gedeelte daarin nooit was opgenomen. Het vorenstaande is ook van toepassing indien deze GVO een omissie bevat.

(c) Deze GVO wordt beheerst door dezelfde wetgeving als de Overeenkomst van Dienstverlening behalve voor zover dwingend Toepasselijke Gegevensbeschermingswet van toepassing is.

Ten behoeve van Verantwoordelijke:

(Volledige) Naam: ……

Functie: ……

Datum: ……

Handtekening: ……

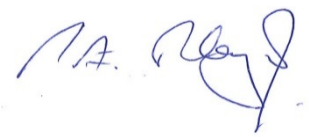
Namens Verwerker:

Naam: Martin O'Malley

Functie: Managing Director BeNeLux

Adres: Zuidpoolsingel 2, Alphen aan den Rijn

Datum: 10-01-2019



Bijlage 1 - Productfiche Avanzer Aangifte

1. **Aard van de Verwerking**
   Online aangiftesoftware voor fiscale professionals. In de aangiftesoftware worden gegevens van de klanten van Wolters Kluwer klanten verwerkt.

2. **Categorieën van Persoonsgegevens die verwerkt worden**
   Wolters Kluwer zal uitsluitend van u als gebruiker de volgende categorieën van Persoonsgegevens verwerken in het kader van dit Addendum:
   - Identiteitsgegevens (naam, voornaam, loginnaam)
   - Contactinformatie (adres, email, IPadres, telefoon)
   - Gedragsgegevens (gebruikershistoriek)

   Als Verwerkingsverantwoordelijke heeft u de mogelijkheid om bijkomende persoonlijke informatie van uw klanten (natuurlijke personen en organisaties) in Avanzer Aangifte in te geven. Dit betreft alle velden die noodzakelijk zijn voor het volledig invullen van de aangifte. De basisvelden die door u in Avanzer Aangifte worden ingevuld zijn o.a.:

   - Identiteitsgegevens (naam, adres, gsm, e-mail, geboortedatum, etc.)
   - Identiteitsgegevens uitgereikt door de overheid (BSN-nummer, paspoortnummer, etc.)
   - Sociale status (gezinssituatie, etc.)
   - Financiële informatie (bankrekeningnummer, inkomen, etc.)

   Belangrijk om te vermelden is dat u als Verwerker hoofdverantwoordelijk bent voor deze gegevens. Wolters Kluwer is alleen technisch aansprakelijk voor het verantwoord bewaren en beheren van deze gegevens. Hier is een uitgebreid veiligheidsprotocol van toepassing, waarin o.a. onderhoud, back-ups en veiligheidsmaatregelen (zoals ISO-certificering en server huisvesting) beschreven worden. Dit veiligheidsdocument vindt u in het document Beveiligingsmaatregelen.
   Daarnaast heeft uw eigen klant het recht om 'vergeten' te worden. Wanneer uw klant dit aangeeft, dient u zelf alle documentatie in Avanzer Aangifte verwijderen en Wolters Kluwer vragen om ook de back-ups van deze klant te verwijderen.

3. **Categorieën van Betrokkenen bij de verwerking van persoonsgegevens in** Avanzer Aangifte

   - klanten en partners van Verwerkingsverantwoordelijke
   - aandeelhouders, medewerkers en andere personeelsleden van de Verwerkingsverantwoordelijke, waaronder stagiairs, onderzoeksassistenten, etc.
   - andere personen waarvan de gegevens door de Verwerkingsverantwoordelijke worden verwerkt, zoals tegenpartijen.

4. Doeleinden van de verwerking

Wolters Kluwer voorziet dat u Avanzer Aangifte voor onderstaande doeleinden kan gebruiken:

- Het invullen en het versturen van aangiften
- Het afdrukken van rapportages over de aangiften
- Het maken van selecties over uw eigen klantdata
- Het centraal beheren van dossiers, contactgegevens en documenten
- Het gebruikmaken van data van gekoppelde systemen, zoals Twinfield en Exact.
- Wanneer u ook Avanzer Advies heeft aangeschaft: het identificeren van advieskansen op uw eigen klanten in Avanzer Aangifte.
- Wanneer u ook de module KvK Opstellen & Deponeren heeft aangeschaft: het gebruiken van de door de verwerker ingevulde CRM- en financiële data t.b.v. het deponeren van de jaarrekening.

5. Retentieperiode

Als Verwerkingsverantwoordelijke bepaalt u zelf de bewaartermijn van de informatie van uw klanten (dossiers, identiteitsgegevens, documenten, enz.), rekening houdend met de opslagbeperking binnen de AVG.

Wolters Kluwer maakt van alle klantendatabases dagelijks een back-up. Deze back-up wordt gedurende 60 dagen bewaard en daarna vernietigd.

Wolters Kluwer zal persoonsgegevens verwerken en bijhouden worden gedurende volgende periodes:

- Na migratie van uw gegevens uit een ander softwarepakket: wij bewaren geen informatie na migratie uit het vroegere softwarepakket. De Verwerkingsverantwoordelijke staat zelf in voor kopie/back-up van deze informatie.
- Persoonsgegevens via support/helpdesk: tickets kunnen 3 maanden na het beëindiging van het contract worden geanonimiseerd. Wanneer u dit graag wilt, kunt u dit aangeven bij de helpdesk.
- Kopie van uw gegevens t.b.v. support/helpdesk: om een technisch probleem op te lossen verplaatsen we een kopie van een bepaald deel van uw gegevens naar een testomgeving. Hiervoor wordt vooraf uw toestemming gevraagd. Deze gegevens worden alleen gebruikt om het probleem op te lossen dat zich heeft voorgedaan en zullen na de interventie uit de testomgeving worden verwijderd.
- Na einde van de Overeenkomst: bezorgen wij de gegevens in een algemeen en toegankelijk bestandsformaat (MS-SQL). Aansluitend bewaren wij de gegevens gedurende 6 maanden op onze server tenzij partijen anders zijn overeengekomen. De Klant kan echter bij beëindiging van de Overeenkomst een inkijklicentie afnemen voor Avanzer Aangifte. Wolters Kluwer verleent deze inkijklicentie onder dezelfde voorwaarden als die van de volledige licentie.

6. Support/helpdesk

Om een issue op te lossen of bijkomende configuratie uit te voeren heeft de helpdesk toegang nodig tot de database van de Verwerkingsverantwoordelijke.

- De Verwerkingsverantwoordelijke kan de medewerker van de helpdesk toegang verlenen tot een specifieke aangifte in Avanzer Aangifte. Dit doet hij door deze via de exportknop te exporteren en te versturen naar de helpdesk.
- Indien toegang tot de technische systemen van de Verantwoordelijke vereist is, zal Wolters Kluwer vanop afstand toegang krijgen tot de computer van de Verwerkingsverantwoordelijke, met toestemming van de Verwerkingsverantwoordelijke. Voor toegang op afstand is activering door de klant vereist door een code in te voeren die wordt verstrekt door Wolters Kluwer. De Verwerkingsverantwoordelijke is verantwoordelijk voor het afsluiten/afschermen van alle vertrouwelijke informatie voordat hij toegang verleent.

7. Beveiligingsmaatregelen

Wolters Kluwer zal conform de voorschriften van de GDPR passende technische en organisatorische maatregelen nemen, te beoordelen naar de stand der techniek op het moment van sluiten van de Overeenkomst van Dienstverlening, en zal deze maatregelen gedurende de contractperiode regelmatig evalueren, daarbij rekening houdend met kosten voor doorvoering, aard, omvang, context en doelstellingen van verwerking, en het risico van verschillen in de mate van waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen.

Gedetailleerde technische en organisatorische maatregelen:	
Toegangscontrole: gebouwen	Toegang tot de gebouwen van Wolters Kluwer wordt door zowel technische als organisatorische maatregelen gecontroleerd: toegangscontrole met gepersonaliseerde badges, elektronische vergrendeling van deuren, receptieprocedures voor bezoekers.
Toegangscontrole: systemen	Toegang tot netwerken, operationele systemen, user administratie en applicaties vereisten de nodige autorisaties: geavanceerde paswoord procedures, automatische time-out en blokkering bij foutieve paswoorden, individuele accounts met historieken, encryptie, hardware en software firewalls.
Toegangscontrole: gegevens	Toegang tot gegevens zelf wordt beheerst door organisatorische maatregelen: user administratie en user accounts met specifieke toegang, opgeleid personeel omtrent gegevensverwerking en veiligheid, scheiding van de operationele systemen en de testomgevingen, toekennen van specifieke rechten en bijhouden van historieken van gebruik, toegang en wissing.
Encryptie van gegevens:	De HTTPS-datatransmissie is versleuteld met een 2048-bit PKI certificaat en is gecertificeerd door Comodo.
Vermogen om blijvende vertrouwelijkheid, integriteit,	Toegangscontrole voor persoonlijke gegevens volgt de richtlijnen voor interne controle, inclusief toegangsbeleid tot informatie van de organisatie, implementatie van een gebruikersadministratiesysteem en toegangsrechten, het creëren van bewustzijn bij medewerkers over het

beschikbaarheid en veerkracht van verwerkingssystem en en -diensten te garanderen:	omgaan met informatie en hun wachtwoorden, netwerktoegangscontrole, inclusief scheiding van gevoelige netwerken, en toegangscontrole tot het besturingssysteem en onderliggende applicaties. Concreet omvatten de maatregelen: • schriftelijke / geprogrammeerde autorisatiestructuur; • gedifferentieerde toegangsrechten (inclusief voor lezen, wijzigen, wissen); • definitie van rollen; • logging / auditing. Persoonlijke gegevens worden gescheiden. De maatregelen omvatten: • scheiding van functies (productie- / testgegevens); • scheiding van bijzonder gevoelige gegevens; • doelbeperking / compartimentering; • beleid / maatregelen om afzonderlijke opslag, wijziging, verwijdering en overdracht van gegevens te waarborgen.
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:	De beschikbaarheid van gegevens wordt gecontroleerd door middel van een permanent netwerkmonitoringsysteem. Om gegevensverlies te voorkomen, wordt een dagelijkse gegevensback-up met gedefinieerde bewaartermijnen uitgevoerd. Verdere maatregelen omvatten: • back-upprocedures; • overspanningsbeveiliging; • fysiek gescheiden opslag van back-upgegevensdragers; • mirroring van server-harde schijven (RAID); • antivirussystemen / SPAM-filters / firewall / inbraakdetectiesysteem / noodherstelplan; • brand / water beveiligingssystemen (inclusief brandblussysteem, branddeuren, rook / brandmelders).
Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen:	Het Avanzer Aangifte -systeem wordt ononderbroken bewaakt: • In het kader van de 24/7 monitoring worden zowel de gezondheid van het systeem als de prestaties van de toepassing voor elke cliënt afzonderlijk nauwkeurig gecontroleerd. • Ieder jaar voert een onafhankelijke externe onderneming inbraaktests uit. • De Avanzer Aangifte - website is ook gecertificeerd: • McAfee security controleert Avanzer Aangifte elke dag nauwkeurig. • Certificeert dat de website beveiligd is, bestand is tegen virussen en inbraakpogingen, en beschermd is tegen aanvallen van hackers op servers en datatransmissie. • Wij worden in real time ingelicht over eventuele risico's, zodat wij aanvallen onmiddellijk kunnen blokkeren. • Norton Symantec controleert ononderbroken onze versleutelde datatransmissie via het SSL-certificaat • Maandelijks vindt een kwetsbaarheidsscan plaats en ontvangen wij het bijbehorende rapport.
Beschikbare certificering:	ISO/IEC 27001 certification

8. Subverwerkers

De Subverwerker(s) genoemd op https://www.wolterskluwer.nl/algemene-voorwaarden/subverwerkers onder Avanzer Aangifte, voeren in opdracht van Wolters Kluwer dienstverlening met betrekking tot persoonsgegevens uit.

9. Doorgifte van persoonsgegevens

Alle Persoonsgegevens zoals opgenomen in deze productfiche worden niet doorgegeven tenzij aan de boven vermelde subverwerkers en enkel in kader van de uitvoering van deze overeenkomst.
De data zal worden opgeslagen in de beveiligde Cloud omgeving van Wolters Kluwer.

Contactgegevens in geval van datalekken

Verantwoordelijke: **…….**
Verwerker: Data Privacy Coördinator via Privacy-NL@wolterskluwer.com

Bijlage 2 – Blad Beveiligingsmaatregelen

1 ONLINE TER BESCHIKKING STELLING

1.1 Toegang tot Avanzer Aangifte

Benadering van Avanzer Aangifte wordt gerealiseerd via een door Wolters Kluwer opgegeven webadres, via een zogenaamde Uniform Resource Locator (URL). Autorisatie op de toegang vindt plaats via een gebruikersnaam en wachtwoord. Gebruikersnamen en wachtwoorden zijn strikt voor persoonlijk gebruik en mogen niet gedeeld worden met andere personen.

1.2 Onderhoud van Avanzer Aangifte

Gepland onderhoud	<u>Software:</u> • Gepland onderhoud vindt in principe iedere 2 weken plaats en zal buiten Kantoortijden worden gepland. • Tijdvakken voor gepland onderhoud worden uiterlijk 1 werkdag van te voren gecommuniceerd (via een pop-up scherm in Avanzer Aangifte). • Gedurende dit software onderhoud is Avanzer Aangifte meestal niet beschikbaar. <u>Infrastructuur (servers):</u> • Uitgangspunt is dat dit onderhoud iedere 4e zaterdag van de maand vanaf 23:00 uur tot 03:00 uur CET (4 uur in totaal) kan plaatsvinden. Het is mogelijk dat Avanzer Aangifte dan niet beschikbaar is. Wolters Kluwer kan dit tijdvenster eenzijdig aanpassen maar zal dit altijd buiten Kantoortijden plannen.
Spoed onderhoud	Voor alle Incidenten, zowel op gebied van infrastructuur, applicatie en klantdata geldt dat – afhankelijk van het incidentniveau en de impact daarvan op de Beschikbaarheid van het totale aanbod van Wolters Kluwer – door Wolters Kluwer de keuze gemaakt kan worden om ter bevordering van een zo spoedig mogelijk herstel van de dienstverlening Avanzer Aangifte tijdig minder beschikbaar te doen zijn. Dit betekent dat Avanzer Aangifte dan ook tijdens Kantoortijden tijdelijk niet beschikbaar zou kunnen zijn. Waar mogelijk wordt Spoedonderhoud gecommuniceerd op gelijke wijze als beschreven bij “Gepland onderhoud”.

Nieuwe release	Het plaatsen van een (uitgebreid geteste) nieuwe release van Avanzer Aangifte zal alleen plaatsvinden buiten Kantoortijden. Wolters Kluwer hanteert een releasekalender die uitgaat van een 2-wekelijkse releasefrequentie. Wolters Kluwer zorgt tijdig voor updates bij fiscale wijzigingen dan wel procedurele wijzigingen van de belastingdienst.

1.3 Beschikbaarheid van Avanzer Aangifte

Wolters Kluwer zal zich ervoor inspannen dat de Klant gedurende vierentwintig uur per dag toegang heeft tot Avanzer Aangifte. Op werkdagen van 08:30 – 17:30 uur bedraagt de Beschikbaarheid op maandbasis minimaal 97%.

Genoemde Beschikbaarheid is niet van toepassing:

- in het geval een probleem of storing is ontstaan als gevolg van handelen door de Klant;
- in het geval Avanzer Aangifte of delen daarbinnen niet beschikbaar zijn (i) op verzoek van de Klant dan wel (ii) vanwege werkzaamheden die op verzoek van de Klant door of namens Wolters Kluwer worden verricht;
- tijdens gepland onderhoud op de Wolters Kluwer infrastructuur en op de momenten van nieuwe releases.

Zowel op niveau van de infrastructuur als op het niveau van de applicatie is monitoring tooling ingericht. Zo kunnen storingen vaak al worden voorkomen of vroegtijdig worden opgelost.

Een deel van deze tooling simuleert, monitort en rapporteert periodiek gebruikershandelingen van een eindgebruiker. Op basis hiervan wordt de Beschikbaarheid (in percentages) vastgesteld door de totale meetperiode te verminderen met de tijd dat de server niet beschikbaar is (met uitzondering van de situaties waarin de Beschikbaarheid niet van toepassing is), gedeeld door de totale meetperiode en vermenigvuldigd met 100.

Lokale aspecten (o.a. internetverbinding, systeeminstellingen, firewall) kunnen van invloed zijn op de daadwerkelijke beschikbaarheid voor de Klant. Ook is het mogelijk dat een door de monitoringtool gesignaleerde niet-beschikbaarheid voor een specifieke Klant geen negatieve gevolgen heeft gehad. Daarom kan de door de monitoring tooling gemeten beschikbaarheid afwijken van de door de Klant ervaren beschikbaarheid.

1.4 Backup & Restore & Klantdata bij beëindiging Overeenkomst

De Klant stemt ermee in dat er backups worden gemaakt van de klantdata. De door Wolters Kluwer Nederland gehanteerde backup procedure is als volgt. Wolters Kluwer Nederland spant zich ervoor in om (a) elk half uur een tussentijdse backup te maken die een dag wordt bewaard en (b) dagelijks een backup te maken die 60 dagen wordt bewaard. De backups worden bewaard in een extern datacentrum in een land dat deel uitmaakt van de Europese Economische Ruimte (EER).

Hierbij is Wolters Kluwer Nederland niet verantwoordelijk voor de (correctheid en kwaliteit van) de in de backup opgeslagen informatie en voor enig dataverlies in de periode tussen het maken van een backup en de terugplaatsing daarvan.

Bij beëindiging van de Overeenkomst worden de klantdata in principe na 6 maanden gewist. De Klant kan echter bij beëindiging van de Overeenkomst een inkijklicentie afnemen voor Avanzer Aangifte. Wolters Kluwer verleent deze inkijklicentie onder dezelfde voorwaarden als die van de volledige licentie.

Ook kan de Klant – voorafgaand aan het aflopen van de volledige licentie - de eigen (beschikbare) klantdata bij Wolters Kluwer opvragen. Deze zullen ter beschikking worden gesteld in een gangbaar formaat.

1.5 Beveiliging

Avanzer Aangifte wordt op verschillende manier beveiligd. In het algemeen zal Wolters Kluwer passende maatregelen treffen ter beveiliging van persoonsgegevens die met Avanzer Aangifte zijn opgeslagen en om te voorkomen dat onbevoegden toegang krijgen tot die gegevens.

Server/database beveiliging:

- De benodigde servers voor Avanzer Aangifte, inclusief de klantdata, zijn gehuisvest in een extern datacentrum in een land dat deel uitmaakt van de Europese Economische Ruimte (EER).
- Het datacentrum is ISO/IEC 27001 gecertificeerd en voldoet daarmee aan dé ISO standaard op het gebied van informatiebeveiliging die tot doel heeft beveiligingsrisico's te verkleinen. Voor het datacentrum is een ISEA 3402 type 2 verklaring afgegeven.
- Met betrekking tot het signaleren van oneigenlijk gebruik van de gebruiksnaam/wachtwoordcombinatie is Avanzer Aangifte uitgerust met de volgende signaleringen:
- Iedere inlogpoging wordt gelogd. Het inlogmechanisme is voorzien van een beveiliging (korte blokkeerperiode) op mislukte inlogpogingen.
- De Klant ontvangt een email in het geval met een gebruikersnaam/wachtwoord combinatie voor het eerst wordt ingelogd vanuit een nieuw IP-adres.
- De klantdata worden binnen een databaseomgeving op een of meerdere servers ondergebracht. Iedere Klant van Wolters Kluwer heeft een eigen database. De verschillende Klanten van Wolters Kluwer hebben uitdrukkelijk geen toegang tot elkaars databases. Het betreft volledig gescheiden databases.
- Wolters Kluwer is zich bewust van het belang van de veiligheid van de klantdata en hanteert daarom een uiterst defensief beleid met betrekking tot toegang door medewerkers van Wolters Kluwer of door medewerkers van leveranciers van Wolters. Als het voor het oplossen van een Incident voor een specifieke Klant (en dus voor een specifieke database) noodzakelijk is om toegang te hebben tot de klantdata, dan zal dat pas plaatsvinden na uitdrukkelijke toestemming van de Klant. Generieke werkzaamheden aan meerdere databases (meerdere Klanten tegelijk) zullen uitsluitend plaatsvinden door middel van geautomatiseerde scripts. In de arbeidsovereenkomst van de medewerkers van Wolters Kluwer alsmede in die van de werknemers van de betrokken leveranciers is een geheimhoudingsclausule opgenomen. Wolters Kluwer houdt technische ontwikkelingen op dit gebied nauwlettend in de gaten en vertaalt dit waar mogelijk in Avanzer Aangifte.

Communicatiebeveiliging:

- Avanzer Aangifte is een SSL- beveiligde website. Met deze SSL-beveiliging is de identiteit van Wolters Kluwer als eigenaar van Avanzer Aangifte gegarandeerd. Daarnaast wordt er een beveiligde verbinding tot stand gebracht. Hierdoor is de informatie tussen pc, laptop etc. van de Klant niet te lezen of te bewerken door anderen omdat deze versleuteld wordt verzonden.

Conform de Overeenkomst worden er eisen gesteld aan het gebruiksrecht van de Klant voor Avanzer Aangifte. De Klant heeft daarnaast ook een verantwoordelijkheid aangaande de beveiliging van specifiek de eigen klantdata. Denk daarbij aan zaken als:

- Geen afgifte van inloggegevens voor werkplek, applicatie etc. door rechtmatige gebruikers aan anderen;
- Treffen van passende maatregelen om ervoor te zorgen dat gebruikers gebruik maken van beveiligingssoftware die gewoonlijk op een computer is geïnstalleerd, zoals antivirus, anti-spam, anti-spyware, anti-malware, anti-fishing, en firewall software.
- Wolters Kluwer is niet aansprakelijk voor misbruik of verlies van gebruikersnamen of wachtwoorden en mag ervan uit gaan dat gebruik daarvan rechtmatig is en met toestemming van de Klant plaatsvindt. Zodra de Klant weet of reden heeft om te vermoeden dat gebruikersnamen of wachtwoorden bekend zijn bij onbevoegden, dient hij de Servicedesk daarvan onverwijld in kennis te stellen.
- Beeldschermvergrendeling bij het verlaten van de werkplek;
- Bij vertrouwelijke/geheime zaken: zorgdragen dat niet over de schouder kan worden meegekeken;
- Eigen verantwoordelijkheid dat de met Avanzer Aangifte opgeslagen gegevens rechtmatig zijn en geen inbreuk maken op rechten van derden.
- De Klant zal ervoor zorgen dat de gebruikers de voorschriften en instructies van Wolters Kluwer nauwgezet nakomen en dat Avanzer Aangifte op een voor een dergelijk online product normale manier gebruiken. Als handelingen hen functioneren van Online Belastingdienst in gevaar brengen, is Wolters Kluwer gerechtigd zonder voorafgaande waarschuwing de toegang tot Avanzer Aangifte te blokkeren.
- Etc.

Wolters Kluwer wordt geacht aan haar verplichtingen op het gebied van beveiliging te hebben voldaan, voor zover zorg wordt gedragen voor de beveiliging zoals beschreven in dit artikel onder server/data beveiliging en communicatiebeveiliging.