Verwerkersovereenkomst Kleos

De partijen genoemd in de licentieovereenkomst (onder de kop “Toepasselijke voorwaarden en duur van overeenkomst”), hierna te noemen: de “**Overeenkomst**”, wensen middels deze verwerkersovereenkomst te voldoen aan hun verplichtingen onder de Algemene Verordening Gegevensbescherming 2016/679 van 27 april 2016 (AVG). De hiervoor bedoelde partijen komen daarom overeen als volgt:

Artikel 1. Definities

In het kader van deze verwerkersovereenkomst betekent:

"Algemene Verordening Gegevensbescherming" of "AVG"	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;
"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;
"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, gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid;
"Derde Land"	een land waarvan 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.
"Diensten"	de diensten verleend door Verwerker aan Verantwoordelijke onder de Overeenkomst;
"Datalek"	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;
"Internationale Organisatie"	een organisatie en de daaronder vallende internationaalpubliekrechtelijke 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);
"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 verwerkersvereenkomst en de voorwaarden van een schriftelijke subverwerkingsovereenkomst;
"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;
"Toepasselijke Gegevensbeschermingswet"	Verordening (EU) 2016/679 (Algemene Verordening Gegevensbescherming en overige wet- en regelgeving die betrekking heeft op de bescherming van Persoonsgegevens;
"Toezichthoudende Autoriteit"	een door een Lidstaat ingevolge artikel 51 AVG ingestelde onafhankelijke overheidsinstantie;

"Verantwoordelijke"	de contractspartij aan wie Verwerker de Diensten zal leveren onder de Overeenkomst en die, als natuurlijke of rechtspersoon, alleen of samen met anderen, het doel van en de middelen voor de Verwerking van Persoonsgegevens vaststelt;
"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 B.V., die ten behoeve van Verantwoordelijke Persoonsgegevens verwerkt;

Artikel 2. Details van de Verwerking

De details van de Verwerking van Persoonsgegevens die door Verwerker ten behoeve van Verantwoordelijke worden verricht als gegevensverwerker die daartoe opdracht heeft gekregen zijn vermeld in de AVG Productsheet (Bijlage bij deze verwerkersovereenkomst).

Artikel 3. Rechten en verplichtingen van Verantwoordelijke

Verantwoordelijke blijft verantwoordelijk voor de Verwerking van de Persoonsgegevens conform de instructies aan Verwerker op grond van de Overeenkomst, deze verwerkersovereenkomst 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, deze verwerkersovereenkomst 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 verbeteren, wissen, overdraagbaar maken 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.

Artikel 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, deze verwerkersovereenkomst 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 vertrouwelijk met de Persoonsgegevens omgaan of dat op die personen een passende geheimhoudingsplicht rust en dat de personen die toegang hebben tot de Persoonsgegevens die Persoonsgegevens uitsluitend 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 de AVG Productsheet (Bijlage) 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, verbetering en verwijdering, beperking van verwerking, kennisgeving, overdraagbaarheid van gegevens, bezwaar tegen direct marketing, profiling in het kader van direct marketing en beslissing uitsluitend gebaseerd op geautomatiseerde verwerkingen. Voor zover die haalbare Technische en Organisatorische Maatregelen veranderingen of wijzigingen in de Technische en Organisatorische Maatregelen vereisen zoals genoemd in de AVG Productsheet (Bijlage), 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 verwerkersovereenkomst en de in art. 28 AVG genoemde verplichtingen worden nagekomen, en controles, waaronder audits 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. De specifieke voorwaarden waaronder een audit uitgevoerd mag worden zijn vastgelegd in de AVG Productsheet.

(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, verbetering en verwijdering, beperking van verwerking, kennisgeving, overdraagbaarheid van gegevens, bezwaar tegen direct marketing, profiling in het kader van direct marketing en beslissing uitsluitend gebaseerd op geautomatiseerde verwerkingen) zonder op dat verzoek in te gaan, tenzij hij daartoe anderszins is gemachtigd of verplicht;

  (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 en 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 of andere op de Verwerker toepasselijke regelgeving; 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) van een Datalek zodra Verwerker zich bewust wordt van een Datalek bij Verwerker. In geval van een Datalek 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 het Datalek te documenteren. Contactgegevens met betrekking tot de melding worden vastgelegd in het klantenservice systeem.

(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 verwerkersovereenkomst zijn verwerkt te verbeteren, te verwijderen en/of te blokkeren, dit onverwijld doen. Indien en voor zover Persoonsgegevens niet kunnen worden verwijderd op grond van wettelijke vereisten in verband met gegevensbewaring, dient Verwerker, in plaats van de desbetreffende Persoonsgegevens te verwijderen, 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 verwijderen.

Artikel 5. Subverwerking en doorgifte van Persoonsgegevens

5.1 Verantwoordelijke geeft toestemming voor het gebruik van Subverwerker(s) die door Verwerker worden ingeschakeld voor het verlenen van de Diensten en die vermeld staan in de AVG Productsheet (Bijlage).

5.2 In het geval dat Verwerker voornemens is nieuwe of meer Subverwerkers in te schakelen, dient Verwerker Verantwoordelijke voorafgaandelijk te informeren over voorgenomen wijzigingen inzake de toevoeging of vervanging van enige Subverwerker ("**Kennisgeving Subverwerker**"). 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 bezwaar 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 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.

5.3 Verwerker legt dezelfde gegevensbeschermingsverplichting als genoemd in deze verwerkersovereenkomst 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 de AVG Productsheet (Bijlage), voor zover die Technische en Organisatorische Beveiligingsmaatregelen van belang zijn voor de door de Subverwerker verleende diensten.

5.4 Verwerker kiest de Subverwerker met de nodige zorg.

5.5 Indien zo'n Subverwerker zich bevindt in een Derde Land, zal Verwerker op schriftelijk verzoek van Verantwoordelijke, een EU-modelcontract (Verantwoordelijke > Verwerker) aangaan ten behoeve van Verantwoordelijke (op naam van Verantwoordelijke), krachtens Besluit 2010/87/EU of andere gelijkwaardige maatregelen nemen ter bescherming van de Persoonsgegevens. In dit geval instrueert en machtigt Verantwoordelijke Verwerker om Subverwerkers instructies te geven uit naam van Verantwoordelijke en om gebruik te maken van alle rechten van Verantwoordelijke jegens de Subverwerkers op basis van het EU-modelcontract of de andere genomen maatregelen.

5.6 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.

Artikel 6. Beperking aansprakelijkheid

Alle aansprakelijkheid voortvloeiend uit of verband houdend met deze verwerkersovereenkomst volgt, en wordt uitsluitend beheerst door, de aansprakelijkheidsbepalingen uiteengezet in, of anderszins van toepassing op, de Overeenkomst. 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 verwerkersovereenkomst voordoet, geacht zich voor te doen uit hoofde van de desbetreffende Overeenkomst. Bovendien komen Partijen het volgende overeen:

a) Elke partij is volledig aansprakelijk voor eventuele boetes die haar door toezichthoudende autoriteiten worden opgelegd en die bedoeld zijn om die partij te straffen voor schendingen van de wetgeving inzake gegevensbescherming.

b) Elke partij die de toepasselijke gegevensbeschermingswet (de 'Vrijwarende partij') niet naleeft, vrijwaart de andere partij voor alle claims van derden die voortvloeien uit een dergelijke niet-nakoming door de schadeloosstellende partij. Deze vergoeding is niet onderworpen aan enige beperking van aansprakelijkheidsclausule in de Overeenkomst.

Artikel 7. Duur en beëindiging

7.1 De looptijd van deze verwerkersovereenkomst is gelijk aan die van de Overeenkomst. Tenzij in deze verwerkersovereenkomst anders is bepaald zijn rechten en verplichtingen op het gebied van beëindiging dezelfde als de rechten en verplichtingen die zijn opgenomen in de Overeenkomst.

7.2 Verwerker dient, naar keuze van Verantwoordelijke, alle Persoonsgegevens na het einde van de verlening van de Diensten te verwijderen 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.

Artikel 8. Overige

8.1 De overige modaliteiten van de Overeenkomst blijven ongewijzigd van toepassing. In geval van tegenstrijdigheid tussen deze verwerkersovereenkomst en de Overeenkomst wat betreft privacy en gegevensbescherming, zullen de bepalingen van deze verwerkersovereenkomst voorgaan.

8.2 Ongeldigheid of onafdwingbaarheid van enige bepaling in deze verwerkersovereenkomst heeft geen gevolgen voor de geldigheid of afdwingbaarheid van de overige bepalingen van deze verwerkersovereenkomst.
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 voorgaande is ook van toepassing indien deze verwerkersovereenkomst een omissie bevat.

8.3 Op deze verwerkersovereenkomst is Nederlands recht van toepassing. Eventuele geschillen die voortvloeien uit of in verband met deze verwerkersovereenkomst zullen uitsluitend worden voorgelegd aan de bevoegde rechtbank te Amsterdam.

AVG PRODUCTSHEET
Kleos

1. Aard van de Verwerking

Online beheersoftware voor advocaten.

2. Categorieën Persoonsgegevens

Wolters Kluwer, als Verwerker zal uitsluitend van de gebruikers volgende categorieën van Persoonsgegevens verwerken in het kader van deze Bijlage:

- Identiteitsgegevens (naam, voornaam, loginnaam)
- Contactinformatie (adres, email, IP-adres, telefoon, fax)
- Gedragsgegevens (gebruikershistoriek)

Als Verwerkingsverantwoordelijke heeft u de mogelijkheid om bijkomende persoonlijke informatie van uw klanten in Kleos in te geven. Basisvelden welke in Kleos worden voorzien en door u eventueel kunnen worden ingevuld zijn:

- Identiteitsgegevens (naam, adres, telefoonnummer, e-mail, geboortedatum, …)
- Zakelijke gegevens (bedrijfsnaam, telefoonnummer, e-mail, …)
- Financiële informatie (bankrekeningnummer, …)
- Andere bijkomende persoonsgegevens kan u steeds toevoegen via de functie “extra velden”

3. Categorieën van Betrokkenen bij de verwerking van persoonsgegevens in Kleos

- 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 bijv. tegenpartijen

4. Doeleinden van de verwerking

Wolters Kluwer voorziet dat u Kleos voor onderstaande doeleinden kan gebruiken:

- Dossiers, contactgegevens en documenten centraal beheren
- Kleos Connect: beveiligde uitwisseling van uw bestanden met uw klanten en andere partijen
- Boekhouding en facturatie: Op basis van de geregistreerde uren en kosten maakt u met Kleos automatisch uw urenstaten en facturen op, verstuurt u aanmaningen, doet u de btw-aangifte en maakt u klantenlijsten aan
- Linken leggen naar uw interne en externe bronnen
- Uitgebreide zoek- en rapportagemogelijkheden
- Exporteren van informatie voor rapportages

5. Retentieperiode

Als Verwerkingsverantwoordelijke bepaalt u zelf de bewaartermijn van de informatie van uw klanten (dossiers, identiteitsgegevens, documenten, enz.).

Wolters Kluwer maakt van alle klantendatabases dagelijks een back-up. Deze back-up wordt gedurende 30 dagen bijgehouden.

Persoonsgegevens zullen verwerkt en bijgehouden worden door Wolters Kluwer 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 en stelt deze indien nodig ter beschikking van Wolters Kluwer.
- Persoonsgegevens via support/helpdesk: contactinfo wordt 6 maanden na de beëindiging van het contract geanonimiseerd. U zorgt ervoor dat u geen gevoelige informatie doorstuurt voor de oplossing van uw vraag (bijvoorbeeld door middel van een screenshot).

- Kopie van uw gegevens voor support/helpdesk: om een technisch probleem op te lossen kan het noodzakelijk zijn dat we een kopie van een bepaald deel van uw gegevens verplaatsen naar een testomgeving. In een dergelijk geval zal u hierover vooraf geïnformeerd worden. 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. Aansluitend bewaren wij de gegevens gedurende 3 maanden op onze server, tenzij partijen anders zijn overeengekomen.

6. Support/helpdesk

Om een issue op te lossen of bijkomende configuratie uit te voeren heeft Wolters Kluwer toegang nodig tot de data van de Verwerkingsverantwoordelijke.

- De Verwerkingsverantwoordelijke kan de medewerker van Wolters Kluwer toegang geven tot Kleos door de Support User te activeren in de database. De Verwerkingsverantwoordelijke kan te allen tijde deze optie uitschakelen.
- Indien toegang tot de technische systemen van de Verwerkingsverantwoordelijke vereist is, zal Wolters Kluwer vanop afstand toegang krijgen tot de computer 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 AVG 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 na verloop van tijd 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.

Als verwerkingsverantwoordelijke zorgt u ervoor dat er adequate beveiligings- en toegangsmaatregelen worden genomen voor uw gebouwen.

Toegangscontrole: systemen

Toegang tot netwerken, operationele systemen, user administratie en applicaties vereisten de nodige autorisaties: geavanceerde wachtwoord procedures, automatische time-out en blokkering bij foutieve wachtwoorden, individuele accounts met gebruikersgeschiedenis, encryptie, hardware en software firewalls.

Als verwerkingsverantwoordelijke zorgt u ervoor dat er adequate beveiligings- en toegangsmaatregelen worden genomen om wachtwoorden en andere elektronische toegangsinformatie te beveiligen.

Toegangscontrole: gegevens

Toegang tot gegevens zelf wordt beheerst door organisatorische maatregelen: gebruikersadministratie, gekwalificeerd personeel m.b.t. gegevensverwerking en veiligheid, scheiding van de operationele systemen en de testomgevingen, toekennen van specifieke rechten en bijhouden van gebruikersgeschiedenis, toegang en verwijdering.

Als verwerkingsverantwoordelijke zorgt u ervoor dat er adequate maatregelen worden genomen om gegevens en documenten te beveiligen.

Encryptie van gegevens

Transport
De HTTPS-datatransmissie is versleuteld met een 2048-bit PKI-certificaat en is gecertificeerd door Norton.

Overig
We coderen databases met een specifiek certificaat/ private sleutel, met behulp van het AES-algoritme.

Vertrouwelijkheid, integriteit, beschikbaarheid van verwerkingssystemen

Toegangscontrole voor persoonsgegevens 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 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.

Persoonsgegevens 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.

Als verwerkingsverantwoordelijke moet de Kleos gebruiker een wachtwoord invoeren, wat de vertrouwelijkheid van alle gegevens die in het beheersysteem worden ingevoerd garandeert. Kleos biedt ook de mogelijkheid om gebruikersrechten te beheren om de informatie die toegankelijk is binnen uw kantoor te segmenteren, indien u dat wenst. De Verwerkingsverantwoordelijke dient derhalve op eigen initiatief geheimhoudingsregels binnen kantoor vast te leggen.

Herstellen van beschikbaarheid van en toegang tot Persoonsgegevens in het geval van een 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).

Periodiek testen, beoordelen van technische en efficiënte beveilingsmaatregelen om de veiligheid te garanderen

Het Kleos 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.
- Bovendien is het inbraakdetectiesysteem altijd actief en geeft het realtime-waarschuwingen.
- De Kleos website is ook gecertificeerd:
- McAfee security controleert Kleos 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.

Audit

Verwerker zal alle informatie aan Verantwoordelijke beschikbaar stellen die nodig is om aan te tonen dat de in deze Verwerkersovereenkomst en de in art. 28 AVG genoemde verplichtingen worden nagekomen, en controles, waaronder audits 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 komen Partijen overeen:

i. Verwerker staat Verantwoordelijke toe om de controle uit te voeren door een auditrapport aan te leveren aan Verantwoordelijke op verzoek van Verantwoordelijke.

ii. Indien het auditrapport aantoont dat Verwerker de verplichtingen van deze Overeenkomst niet of niet behoorlijk nakomt, is Verantwoordelijke bevoegd om een tweede audit uit te voeren. De kosten voor een tweede audit worden gedragen door Verantwoordelijke, tenzij de audit aantoont dat er sprake is van non-compliance door Verwerker, in dat geval zal de Verwerker redelijke kosten vergoeden. Indien de tweede audit aantoont dat Verwerker volledig in strijd handelt met de verplichtingen uit deze Overeenkomst, zal Verwerker de tekortkoming zonder onredelijke vertraging ongedaan maken of herstellen. Verantwoordelijke mag een controle op afstand uitvoeren en een controle in persoon en op locatie mag uitsluitend uitgevoerd worden indien Verantwoordelijke de (on)kosten die door Verwerker zijn gemaakt als gevolg van de verstoring van de bedrijfsactiviteiten aan Verwerker vergoedt en het tijdstip en de locatie van de controle in onderling overleg tussen de Partijen vooraf vastgelegd is.

Subverwerkers

De volgende Subverwerker(s) verwerken persoonsgegevens in opdracht van Wolters Kluwer in het kader van de Overeenkomst:

Naam	Adres	Doel van gebruik
Teleperformance Portugal	Cais dos Argonautas Lote 2.34.01 Lissabon, Portugal	Support Level 1
Wolters Kluwer Global Business Services - DXG	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, Nederland	2nd level support en software development
Wolters Kluwer Italia	Centro Direzoniale Milanoflori Strada 1, Palazzo 6 20090 Assago - Italië	2nd & 3th level support en software development
T-systems	Data centre Munich/Allach Dauchauer Strasse 665 80995 München, Germany Data Centre Munich/Eip Elisabeth Selbert Strasse 1 80939 München, Duitsland	Hosting servers