AVG PRODUCTFICHE

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 noncompliance 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:

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