Wolters Kluwer

GDPR PRODUCTFICHE

Kleos

1 Aard van de Verwerking

Online beheersoftware voor advocaten, bedrijfsjuristen, andere juridische beroepen en departementen met een dossier-gebaseerde organisatie.

2 Categorieën van Persoonsgegevens die verwerkt worden

Wolters Kluwer, als verwerker zal uitsluitend van de gebruikers volgende categorieën van Persoonsgegevens verwerken in het kader van dit Addendum:

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

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

- Identiteitsgegevens (naam, adres, gsm, e-mail, geboortedatum, …)
- Identiteitsgegevens uitgereikt door de overheid (rijksregisternummer, paspoortnummer, …)
- Sociale status (gezinssituatie, …)
- 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, enz,…;
- 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
- Gecertificeerde connectie met het DPA, Digitaal Platform Advocaten
- Kleos Connect: beveiligde uitwisseling van uw bestanden met uw klanten en andere partijen
- Boekhouding en facturatie: Op basis van de geregistreerde prestaties en kosten maakt u met Kleos automatisch uw ereloonstaten en facturen op, verstuurt u rappels, doet u de btw-aangifte en maakt u klantenlistings aan.
- Linken leggen naar uw interne en externe bronnen
- Uitgebreide zoek- en rapportagemogelijkheden
- In het kader van onze voortdurende inspanningen om de kwaliteit en functionaliteit van onze software/product te verbeteren, verzamelen en analyseren wij gegevens over het gebruik van onze producten. De verzamelde gegevens worden uitsluitend gebruikt voor de volgende doeleinden: (i) Identificeren en oplossen van technische problemen en bugs (ii) Optimaliseren van de gebruikservaring en interface (iii) Ontwikkelen van nieuwe functies en verbeteringen die zijn afgestemd op de behoeften en voorkeuren van de gebruiker (iv) Uitvoeren van algemene productanalyse om de efficiëntie en effectiviteit van de software te verbeteren.
- Exporteren van informatie ifv rapportages edm.

©Legal Office WKB

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 (screenshot etc)
- Kopie van uw gegevens ifv 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. 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 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 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 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:

7.1 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.

©Legal Office WKB

7.2 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.

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

7.3 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.

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

7.4 Encryptie van gegevens

7.4.1 Transport

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

7.4.2 In rust

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

7.5 Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:

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 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.

Als verwerkingsverantwoordelijke moet de Kleosgbruiker 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.

7.6 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:

©Legal Office WKB

- 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).

7.7 Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking 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.

7.8 Beschikbare certificering

Kleos heeft een ISO/IEC 27001 certification

8 Subverwerkers

Volgende Subverwerker(s) voeren in opdracht van Wolters Kluwer dienstverlening met betrekking tot persoonsgegevens uit:

Naam	Adres	Doel van gebruik
Teleperformance Portugal	Cais dos Argonautas Lote 2.34.01 Lisbonne – Portugal	Support Level 1
Sendinblue	55 rue de Madrid Paris (75008)	Verzenden van facturen en reminders via e-mail.
Capgemini Nederland B.V.	Reykjavikplein 1 3543 KA Utrecht - Nederland	Consultancy voor implementatie en ontwikkeling van Salesforce
Salesforce EMEA Limited	Floor 26 Salesforce Tover 110 Bishophsgate London EC2N 4AY - United Kingdom	Tool voor supporttickets
Wolters Kluwer Global Business Services	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 & 3 th level support en software development

©Legal Office WKB

T systems International GmbH	Data centre Munich/Allach Dauchauer Strasse 665 80995 München, Germany Data Centre Munich/Eip Elisabeth Selbert Strasse 1 80939 München	Hosting servers
Wolters Kluwer Global Business Services Italia	Via dei Missaglia 97 20142 Milano Italy	Backup & Gegevensresidentie
TeamViewer	TeamViewer GmbH Jahnstr. 30 73037 Göppingen, Germany	Remote support
Salesforce.com	Floor 26 Salesforce Tower, 110 Bishopsgate, EC2N 4AY London, United Kingdom	Support ticket Management
Microsoft Azure	Allemagne / Germany / Duitsland Frankfurt am Main	Datacenters

©Legal Office WKB

9 Doorgifte van persoonsgegevens

Alle Persoonsgegevens zoals opgenomen in deze productfiche worden niet doorgegeven tenzij aan de boven vermelde subverwerkwers en enkel in kader van de uitvoering van deze overeenkomst.

©Legal Office WKB