Wolters Kluwer

GDPR PRODUCTFICHE

DLEX

1 Aard van de Verwerking

Beheerssoftware voor advocaten

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, telefoon, fax)
- Gedragsgegevens (gebruikershistoriek)

Als Verwerkingsverantwoordelijke heeft u de mogelijkheid om bijkomende persoonlijke informatie van uw klanten in DLex in te geven. Basisvelden dewelke in DLex 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”, De titel, de inrichting en de inhoud van deze velden zijn ude verantwoordelijkheid van de Verwerkingsverantwoordelijke

3 Categorieën van Betrokkenen bij de verwerking van persoonsgegevens in DLex

- Klanten en partners van Verwerkingsverantwoordelijke
- Aandeelhouders, medewerkers en andere personeelsleden van de Verwerkingsverantwoordelijke, waaronder stagiairs, assistenten, enz,…;
- Andere personen waarvan de gegevens door de Verwerkingsverantwoordelijke worden verwerkt, zoals bijv. tegenpartijen.

4 Doeleinden van de verwerking

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

- Dossiers, contactgegevens en documenten centraal beheren
- Gecertificeerde connectie met het DPA, Digitaal Platform Advocaten
- Extranet/CWA: 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 DLex 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
- Exporteren van informatie ifv rapportages edm.

5 Retentieperiode

Als Verwerkingsverantwoordelijke bepaalt u zelf de bewaartermijn van de informatie van uw klanten (dossiers, identiteitsgegevens, documenten, enz.). U bent tevens verantwoordelijk voor de beveiliging en back up van de informatie op uw server

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.

6 Support/helpdesk

Om een probleem op te lossen of een bijkomende configuratie uit te voeren, moet Wolters Kluwer toegang hebben tot de DLex interface en/of de PC van de Vzerwerkingsverantwoordelijke, of soms rechtstreeks tot de database en de DLex server in complexere gevallen.

- 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.
- Indien toegang tot de server of database noodzakelijk is, kan de Verwerkingsverantwoordelijke onder bepaalde voorwaarden toegang verlenen aan de medewerker van Wolters Kluwer:
    - De toegang mag niet permanent zijn, maar moet op verzoek geactiveerd kunnen worden.
    - Voor een snellere oplossing is het te verkiezen dat de verbindingsinformatie statisch is, bekend is bij de IT-manager en DLex en indien nodig kan worden geactiveerd. Deze verbindingsinformatie moet door IT-onderaannemers en DLex worden opgeslagen in beveiligde omgevingen en mag alleen toegankelijk zijn voor degenen die de informatie nodig hebben.
    - Om het afhandelingsproces niet te vertragen, moeten alle ondersteuningsaanvragers op de hoogte zijn van de activerings-/deactiveringsprocedure.
- Wolters Kluwer zal geen wijzigingen aanbrengen aan de database zonder toezicht van de Verwerkingsverantwoordelijke of de IT van de Verwerkingsverantwoordelijke (indien de Verwerkingsverantwoordelijke dit recht schriftelijk verleent).
- Wolters Kluwer zal geen wijzigingen aanbrengen aan de server van de Verwerkingsverantwoordelijke, dit recht is voorbehouden aan de Verwerkingsverantwoordelijk of de IT-dienstverlener.

! Belangrijk! De Dlex ondersteuning mag in geen geval een Microsoft patch installeren of handmatig een nieuwe DLex versie downloaden en installeren in plaats van de Verwerkingsverantwoordelijke of zijn IT partner. Voor een DLex-update worden enkel de volgende 2 methodes toegestaan:

- activering rechtstreeks door de Verwerkingsverantwoordelijke of zijn IT-provider via de DLex-upgraderfunctie (controle door IT aanbevolen)
- activering via een automatische batchfunctie op vooraf bepaalde data en enkel als de ervaring heeft aangetoond dat deze methode betrouwbaar was voor de IT-omgeving van de Verwerkingsverantwoordelijk. In geval van problemen kan DLex-support de IT-partner van de Verwerkingsverantwoordelijke, in zijn aanwezigheid, helpen bij dit soort operaties als de hierboven vermelde methoden niet effectief zijn.

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

Als verwerker wordt de toegang tot de gebouwen van Wolters Kluwer 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.

7.2 Toegangscontrole: systemen

Als Verwerker wordt voor toegang tot netwerken, operationele systemen, user administratie en applicaties de nodige autorisaties vereist: 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 elektronische toegangsinformatie te beveiligen

7.3 Toegangscontrole: gegevens

Toegang tot gegevens beheerd door Wolters Kluwer 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 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 DLexgbruiker een wachtwoord invoeren, wat de vertrouwelijkheid van alle gegevens die in het beheersysteem worden ingevoerd garandeert. DLex biedt ook de mogelijkheid om gebruikersrechten te beheren om de informatie die toegankelijk is binnen uw kantoor te segmenteren, indien u dat wenst. Het is dan de verantwoordelijkheid van de Verwerkingsverantwoordelijke zelf om de toegang tot de gegevens tot de server en databases te beveiligen, aangezien DLex gehost wordt op het netwerk van de Verwerkingsverantwoordelijke.

De Verwerkingsverantwoordelijke dient derhalve op eigen initiatief geheimhoudingsregels binnen kantoor vast te leggen.

7.5 Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:

Data wordt opgeslagen op server van Verwerkingsverantwoordelijke en valt onder diens verantwoordelijkheid

7.6 Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen:

De verwerker zorgt er voor dat er regressietesten worden uitgevoerd om de compatibiliteit met de GDPR-regels te behouden vóór de levering van elke nieuwe versie van DLex.

Door de technologie die gebruikt wordt voor DLex (d.w.z. client-server), is de verantwoordelijkheid voor het technisch en organisatorisch onderhoud volledig de verantwoordelijkheid van de Verwerkingsverantwoordelijke, die de technische en organisatorische maatregelen die genomen zijn voortdurend moet testen en evalueren.

8 Subverwerkers

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

Naam	Adres	Doel van gebruik
CAPTEL	Rue Grétry 50/096 4020 Liège Belgium	'Overflow support' – opvang van support en andere meldingen in eerste lijn bij overflow of onbeschikbaarheid
Capgemini	Capgemini Nederland B.V. Reykjavikplein 1 3543 KA Utrecht - Nederland	Consultancy voor implementatie en ontwikkeling van Salesforce
Salesforce	Salesforce EMEA Limited Floor 26 Salesforce Tover 110 Bishophsgate London EC2N 4AY - United Kingdom	Tool voor supporttickets
Pluritech	Franklin Rooseveltlaan 26a – 1800 Vilvoorde - Belgium	Testservers geleverd voor testen in TS-clientconfiguratie.
Qlik	France Headquarters Office 93 avenue Charles de Gaulle 92200 Neuilly sur Seine - FRANCE	Partner voor module rapporten

1. **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.