Wolters Kluwer

GDPR PRODUCTFICHE

Legisway Essentials

1. Aard van de verwerking

Legisway Essentials is een SaaS software dat gegevens opslaat via een cloud service en een platform-based database aanbiedt om juridische documenten te bewaren en de beheren. Hierin zit onder meer inbegrepen, zonder dat dit limitatief is: contract management en corporate housekeeping.

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)

Daarenboven kan Verwerker andere Persoonsgegevens verwerken die afkomstig zijn van Verantwoordelijke. Persoonsgegevens die afkomstig zijn van Verantwoordelijke en door Verantwoordelijke ingegeven en geüploaded worden in Legisway Essentials zullen volledig onder de verantwoordelijkheid van Verantwoordelijke vallen. Verwerker heeft geen mogelijkheden om kennis te nemen van de aard van de Persoonsgegevens die afkomstig zijn van Verantwoordelijke, noch hier toegang tot hebben en kan bijgevolg hier vooraf geen kennis van hebben. Niettemin kunnen volgende Persoonsgegevens die afkomstig zijn van Verantwoordelijke ingegeven worden in het kader van de uitvoering van de Overeenkomst:

- Identiteitsgegevens (naam, adres, gsm, e-mail, geboortedatum, …)
- Identiteitsgegevens uitgereikt door de overheid (rijksregisternummer, paspoortnummer, …)
- Sociale status (gezinssituatie, …)
- Financiële informatie (bankrekeningnummer, …)

3. Categorieën van Betrokkenen

- 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

Verwerker stelt dat Legisway Essentials voor volgende doeleinden gebruikt kan worden:

- Dossiers, contactgegevens en documenten centraal beheren
- Linken leggen naar uw interne en externe bronnen
- Uitgebreide zoek- en rapportagemogelijkheden
- Exporteren van informatie in functie van rapportages etc…

5. Retentieperiode

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

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

Persoonsgegevens zullen verwerkt en bijgehouden worden door Verwerker gedurende volgende periodes:

- Na migratie van uw gegevens uit een ander softwarepakket: Verwerker bewaart geen informatie na migratie uit het vroegere softwarepakket. Verwerkingsverantwoordelijke staat zelf in voor kopie/back-up van deze informatie en stelt deze indien nodig ter beschikking van Verwerker.
- Persoonsgegevens via support/helpdesk: contactinfo wordt 6 maanden na de beëindiging van de Overeenkomst geanonimiseerd. Verantwoordelijke zorgt ervoor dat er geen gevoelige informatie doorgestuurd wordt voor de oplossing van een vraag (screenshot etc…).
- Kopie van Persoonsgegevens in functie van support/helpdesk: om een technisch probleem op te lossen verplaatst Verwerker een kopie van een bepaald deel van de gegevens naar een testomgeving. Gegevens worden van de productieomgeving naar de testomgeving getransporteerd via geëncrypteerde back-ups. Binnen de testomgeving worden de gegevens zowel tijdens het transport als in rust geëncrypteerd. Hiervoor wordt vooraf 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: Verwerker bezorgt de gegevens in een algemeen en toegankelijk bestandsformaat. Daarnaast heeft Verantwoordelijke zelf de mogelijkheid om op een eenvoudige manier gegevens, inclusief Persoonsgegevens, uit Legisway Essentials te halen in een algemeen en toegankelijk bestandsformaat (bijvoorbeeld Excel, World, etc…). Aansluitend bewaart Verwerker de gegevens gedurende 4 maanden op de server.

6. Support/helpdesk/consultants

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

- Verantwoordelijke kan de medewerker van Verwerker toegang geven tot Legisway Essentials door zijn toestemming te verlenen voor toegang voor een welbepaald doeleinde. In sommige systemen kan Verantwoordelijke toegang geven aan een medewerker van Verwerker door de Support Access te activeren in de database. Verwerkingsverantwoordelijke kan te allen tijde deze optie uitschakelen.
- Indien toegang tot de technische systemen van Verwerkingsverantwoordelijke vereist is, zal Verwerker vanop afstand toegang krijgen tot de computer van Verantwoordelijke. Voor toegang op afstand is activering door Verantwoordelijke vereist door een code in te voeren die wordt verstrekt door Verwerker. Verantwoordelijke is verantwoordelijk voor het afsluiten/afschermen van alle vertrouwelijke informatie voordat hij toegang verleent.

7. Beveiligingsmaatregelen

Verwerker 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 Verwerker wordt door zowel technische als organisatorische maatregelen gecontroleerd: toegangscontrole met gepersonaliseerde badges, elektronische vergrendeling van deuren, receptieprocedures voor bezoekers.

Als verwerkingsverantwoordelijke zorgt Verantwoordelijke ervoor dat er adequate beveiligings- en toegangsmaatregelen worden genomen voor de eigen gebouwen.

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.

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 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.

Voor Verantwoordelijke moet de gebruiker van Legisway Essentials een wachtwoord invoeren om toegang te krijgen tot het Legisway Essentials systeem, wat de vertrouwelijkheid van alle gegevens die in het beheersysteem worden ingevoerd garandeert. Legisway Essentials biedt ook de mogelijkheid om gebruikersrechten te beheren om de informatie die toegankelijk is binnen het Legisway Essentials systeem, indien u dat wenst.

Verantwoordelijke dient derhalve op eigen initiatief geheimhoudingsregels binnen de eigen onderneming 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:

- 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

7.7.1 Monitoring

Het Legisway Essentials system wordt ononderbroken gemonitord:

- 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 real-time waarschuwingen.
- De Legisway Essentials website is ook gecertificeerd:
- McAfee security controleert Legisway Essentials elke dag nauwkeurig: zij certificeren dat de website veilig, resistent tegen virussen en pogingen tot indringing is en dat deze beschermd is tegen aanvallen van hackers op de servers of datatransmissies.
- Norton Symantec controleert ononderbroken onze versleutelde datatransmissie via het SSL-certificaat
- 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.
- Maandelijks vindt een kwetsbaarheidsscan plaats en ontvangen wij het bijbehorende rapport.

7.7.2 Audits

Verwerker zal alle informatie die noodzakelijk is om de naleving van de verplichtingen zoals opgenomen in de DPA en in artikel 28 van de GDPR aan te tonen aan Verantwoordelijke, inclusief de mogelijkheid om audit rapporten ter plekke bij Verwerker in te kijken in het door de Verwerker aangeduide kantoor. Verantwoordelijke is zich ervan bewust dat persoonlijke audits ter plekke bij Verwerker de dagelijkse bedrijfsactiviteiten aanzienlijk kunnen verstoren en dat deze zowel tijd- als geldrovend zijn. Daarom komen Partijen overeen dat:

i. Verwerker Verantwoordelijke in staat zal stellen om de naleving van deze overeenkomst door Verwerker door audit rapporten die reeds in Verwerkers bezit zijn ter beschikking te stellen op aanvraag van Verantwoordelijke.
ii. Indien er enig bewijs is dat het vermoeden wekt dat Verwerker de verplichtingen onder deze overeenkomst niet naleeft, zal Verantwoordelijke, na toestemming van Verwerker, een bijkomende audit kunnen organiseren. De kosten hiervoor zullen door Verantwoordelijke gedragen worden tenzij uit de audit blijkt dat Verwerker haar verplichtingen niet naleeft, waarbij Verwerker in dat geval proportioneel de redelijke kosten van de audit zal dragen. Bovendien zal Verwerker in dat geval zonder uitstel de nodige maatregelen nemen om haar verplichtingen na te komen.

8. Subverwerkers

Volgende Subverwerkers voeren in opdracht van Verwerker dienstverlening met betrekking tot Persoonsgegevens uit:

Naam	Adres	Doel van gebruik
Wolters Kluwer Global Business Services	Zuidpoolsingel 2 2408 ZE Alphen aan den Rijn, The Netherlands	2nd level support en software ontwikkeling
Teleperformance Portugal	Cais dos Argonautas Lote 2.34.01 Lisbon – Portugal	1st level support
Wolters Kluwer Italia	Centro Direzoniale Milanoflori Strada 1, Palazzo 6, 20090 Assago - Italy	2nd & 3rd level support en software ontwikkeling
Salesforce.com EMEA	Floor 26 Salesforce Tower 110 Bishopsgate, London EC2NB 4AY, UK	Tool om support tickets op te volgen
Capgemini Nederland	Reykjavikplein 1 3543 KA Utrecht, The Netherlands	Consultancy services voor de implementatie en de ontwikkeling van Salesforce
NTT Europe	Frankfurt Data Center, Russelsheim, Frankfurt, Germany	Data center

9. Doorgifte van Persoonsgegevens

Geen van de Persoonsgegevens zoals opgenomen in deze productfiche worden doorgegeven tenzij aan de bovenvermelde subverwerkers en enkel in kader van de uitvoering van deze overeenkomst.