GDPR-PRODUCTBLAD
Legisway Essentials

1. Aard van de verwerking

Legisway is SaaS-software die gegevens opslaat via een clouddienst en die een platformdatabank biedt voor het opslaan en beheren van juridische documenten, met inbegrip van maar niet beperkt tot, contractbeheer en bedrijfshuishouding.

2. Categorieën van Persoonsgegevens die worden verwerkt

De Verwerker verwerkt de volgende categorieën van persoonsgegevens van de Verwerkingsverantwoordelijke, en dat uitsluitend in het kader van de Overeenkomst:

- Identiteitsgegevens (achternaam, voornaam, gebruikersnaam)
- Contactgegevens (adres, e-mail, IP-adres, telefoon, fax)
- Gedragsgegevens (gebruikersgeschiedenis)

Bovendien kan de Verwerker de Persoonsgegevens van de Verwerkingsverantwoordelijke verwerken. De Persoonsgegevens die de Verwerkingsverantwoordelijke in LEgisway aanmaakt, invoert en uploadt, zijn naar eigen goeddunken en op risico van de Verwerkingsverantwoordelijke. De Verwerker heeft geen toegang tot of kan niet wetenge welk type van Persoonsgegevens de Verwerkingsverantwoordelijke heeft aangemaakt. De Verwerker weet dus niet op voorhand welk type van Persoonsgegevens door de Verwerkingsverantwoordelijke in LEgisway zal worden aangemaakt, ingevoerd en geüpload. In het kader van de uitvoering van de Serviceovereenkomst kunnen de gegevens ingevoerd door de Verwerkingsverantwoordelijke, echter de volgende categorieën omvatten:

- Identiteitsgegevens (naam, adres, mobiele telefoon, e-mail, geboortedatum, ...)
- Identiteitsgegevens die door de overheid zijn verstrekt (rijksregisternummer, paspoortnummer, ...)
- Sociale status (gezinssituatie, ...)
- Financiële informatie (bankrekeningnummer, ...)

3. Categorieën van betrokkenen

- Klanten en partners van de Verwerkingsverantwoordelijke
- Aandeelhouders, werknemers en andere personeelsleden van de Verwerkingsverantwoordelijke, met inbegrip van stagiairs, onderzoeksassistenten en ongeschoolde arbeiders;
- Andere personen wier gegevens door de Verwerkingsverantwoordelijke worden verwerkt, zoals tegenpartijen.

4. Doeleinden van de verwerking

De Verwerker bepaalt dat u LEgisway kunt gebruiken voor de onderstaande doeleinden:

- Centraal beheer van dossiers, contactgegevens en documenten
- Linken naar uw interne en externe bronnen
- Uitgebreide zoek- en rapporteringsmogelijkheden

- Informatie exporteren voor verslagen enzovoort

5. Bewaartermijn

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

De Verwerker maakt dagelijks een back-up van alle databases van de Verwerkingsverantwoordelijke. Deze back-up wordt 30 dagen bewaard.

Persoonsgegevens worden verwerkt en bewaard gedurende de volgende perioden:

- Na migratie van uw gegevens uit een ander softwarepakket: we bewaren geen informatie na migratie uit een vorig softwarepakket. De Verwerkingsverantwoordelijke dient deze gegevens zelf te kopiëren/back-uppen en ter beschikking te stellen aan de Verwerker indien nodig.
- Persoonsgegevens via support/helpdesk: de contacten worden zes maanden na de beëindiging van het contract geanonimiseerd. Als Verwerkingsverantwoordelijke moet u ervoor zorgen dat u geen gevoelige gegevens doorgeeft tijdens het oplossen van het ticket (screenshot enz.).
- Kopie van uw gegevens in verband met ondersteuning/helpdesk: om een technisch probleem op te lossen, verplaatsen wij een kopie van een specifiek deel van uw gegevens naar een gecodeerde testomgeving. Bij de overdracht van de productie- naar de testomgeving worden gegevens getransporteerd met gecodeerde back-ups, en ook in de testomgeving zijn zowel het transport als de bestanden versleuteld. Daarvoor wordt vooraf uw toestemming gevraagd. Deze gegevens worden alleen gebruikt om het opgetreden probleem op te lossen en zullen na de procedure uit de testomgeving worden gewist.
- Na het einde van de Overeenkomst: wij verstrekken de Persoonsgegevens in een algemeen en toegankelijk bestandsformaat. De Verwerkingsverantwoordelijke kan gegevens, met inbegrip van Persoonsgegevens, gemakkelijk uit LEgisway halen dankzij het algemene en toegankelijke bestandsformaat dat in het systeem beschikbaar is (bv. Excel, Word, enz.). Vervolgens bewaren wij de gegevens vier maanden op onze servers.

6. Ondersteuning/helpdesk/consultants

Om een probleem op te lossen of extra configuratie uit te voeren, heeft de Verwerker toegang nodig tot de database van de Verwerkingsverantwoordelijke.

- De Verwerkingsverantwoordelijke kan de werknemer van de Verwerker toegang geven tot LEgisway door toestemming te geven voor een bepaald doel. Voor sommige systemen kan de Verwerkingsverantwoordelijke de werknemer van de Verwerker toegang geven tot LEgisway door de optie Support Access in de database te activeren. De Verwerkingsverantwoordelijke kan deze optie te allen tijde uitschakelen.
- Indien toegang tot de technische systemen van de Verwerkingsverantwoordelijke nodig is, zal de Verwerker via PC-sharing toegang krijgen tot de computer van de Verwerkingsverantwoordelijke. De activering door de Verwerkingsverantwoordelijke is vereist voor toegang vanop afstand. Dit gebeurt door een code in te voeren die door de Verwerker werd verstrekt door middel van een pop-up die uw toestemming vraagt. De Verwerkingsverantwoordelijke is verantwoordelijk voor het blokkeren/beschermen van alle vertrouwelijke informatie alvorens toegang te verlenen.

7. Veiligheidsmaatregelen

Conform de GDPR-verordeningen zal de Verwerker passende technische en organisationele maatregelen nemen, te beoordelen op basis van de stand van de techniek op het moment dat de Overeenkomst wordt gesloten, en zal hij deze maatregelen in de loop van de tijd evalueren, rekening houdend met de kosten van de uitvoering, de aard, de reikwijdte, de context en de doelstellingen van de

verwerking, evenals het risico van verschillen in de mate van waarschijnlijkheid en ernst voor de rechten en vrijheden van natuurlijke personen.

GEDETAILLEERDE TECHNISCHE EN ORGANISATIONELE MAATREGELEN

7.1 Toegangscontrole: gebouwen

De toegang tot de gebouwen van de Verwerker wordt gecontroleerd door zowel technische als organisatorische maatregelen: toegangscontrole met gepersonaliseerde badges, elektronische vergrendeling van deuren, ontvangstprocedures voor bezoekers.

De Verwerkingsverantwoordelijke moet ook zorgen voor adequate maatregelen om de veiligheid en de toegang tot hun gebouwen te verzekeren.

7.2 Toegangscontrole: systemen

Als Verwerker vereist elke toegang tot netwerken, operationele systemen, gebruikersadministratie en applicaties de nodige machtigingen: geavanceerde wachtwoordprocedures, automatische time-out en blokkering van onjuiste wachtwoorden, individuele accounts met geschiedenissen, codering, hardware- en softwarefirewalls.

De Verwerkingsverantwoordelijke moet ook zorgen voor adequate veiligheidsmaatregelen voor de wachtwoorden en andere elektronische toegangsgegevens.

7.3 Toegangscontrole: gegevens

De toegang tot de gegevens door de Verwerker zelf wordt gecontroleerd door organisationele maatregelen: gebruikersadministratie en gebruikersaccounts met specifieke toegang, personeel dat is opgeleid met betrekking tot gegevensverwerking en -beveiliging, scheiding van de operationele systemen en de testomgevingen, toekenning van specifieke rechten en bijhouden van gebruiks-, toegangs- en verwijderingsgeschiedenissen.

7.4 Gegevenscodering

De HTTPS-gegevensoverdracht wordt versleuteld met een PKI-certificaat van 2048 bits en is gecertificeerd door Norton.

7.5 Het vermogen om de permanente vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten te garanderen

De toegangscontrole voor Persoonsgegevens volgt de richtlijnen voor interne controle, met inbegrip van het beleid voor de toegang tot informatie van de organisatie, de implementatie van een systeem voor gebruikersadministratie en toegangsrechten, de bewustmaking van werknemers rond de omgang met informatie en wachtwoorden, de controle op de netwerktoegang, met inbegrip van de scheiding van gevoelige netwerken, en de controle op de toegang tot het besturingssysteem en de onderliggende applicaties. De maatregelen omvatten met name:

- schriftelijke/geprogrammeerde machtigingsstructuur;
- gedifferentieerde toegangsrechten (o.a. voor lezen, wijzigen, verwijderen);
- definitie van rollen;
- loggen/auditeren.

Persoonsgegevens worden afgezonderd. De maatregelen omvatten:

- scheiding van functies (productie-/testgegevens);
- scheiding van zeer gevoelige gegevens;
- doelbeperking/compartimentering;
- beleid/maatregelen om te zorgen voor gescheiden opslag, wijziging, verwijdering en overdracht van gegevens.

Voor de Verwerkingsverantwoordelijke vereist LEgisway dat de gebruiker een wachtwoord gebruikt om toegang te krijgen tot het LEgisway-systeem, waardoor de vertrouwelijkheid van alle in het beheersysteem ingevoerde gegevens wordt gegarandeerd. LEgisway biedt ook de mogelijkheid om de gebruikersrechten te beheren om de informatie die in het LEgisway-systeem toegankelijk is, te segmenteren. De Verwerkingsverantwoordelijke moet daartoe geheimhoudingsregels vaststellen binnen de onderneming.

7.6 Mogelijkheid om de beschikbaarheid van en toegang tot de Persoonsgegevens onmiddellijk te herstellen in geval van een fysiek of technisch incident

De beschikbaarheid van de gegevens wordt gecontroleerd door middel van een permanent netwerkbewakingssysteem. Om gegevensverlies te voorkomen, wordt er dagelijks een back-up van de gegevens gemaakt, met vastgestelde bewaarperiodes. Verdere maatregelen omvatten:

- back-upprocedures;
- overspanningsbeveiliging;
- fysiek gescheiden opslag van back-upgegevensdragers;
- spiegelen van harde schijven van servers (RAID);
- antivirussystemen/spamfilters/firewall/intrusiedetectie/herstelplan bij incidenten;
- brand/waterbeveiligingssystemen (met inbegrip van brandblussysteem, branddeuren, rook/brandmelders).

7.7 Proces voor het regelmatig testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisationele maatregelen om de veiligheid van de verwerking te garanderen:

De Verwerker zal de Verwerkingsverantwoordelijke alle informatie ter beschikking stellen die nodig is om aan te tonen dat de verplichtingen uit hoofde van deze DPA en uit hoofde van Art. 28 GDPR zijn vervuld, met inbegrip van de mogelijkheid om auditverslagen ter plaatse op het kantoor van de aangestelde Verwerker te bekijken. De Verwerkingsverantwoordelijke is zich ervan bewust dat eventuele audits ter plaatse de bedrijfsvoering van de Verwerker aanzienlijk kunnen verstoren en hoge uitgaven in termen van kosten en tijd met zich mee kunnen brengen. Derhalve komen de Partijen het volgende overeen:

i. De Verwerker stelt de Verwerkingsverantwoordelijke in staat de naleving van deze overeenkomst door de Verwerker te toetsen door de Verwerkingsverantwoordelijke op diens verzoek auditrapporten ter beschikking te stellen die reeds in het bezit van de Verwerker zijn.

ii. Indien er aanwijzingen zijn dat de Verwerker zijn verplichtingen uit hoofde van deze Overeenkomst niet nakomt, kan de Verwerkingsverantwoordelijke, met toestemming van de Verwerker, een secundaire audit uitvoeren. De kosten van een secundaire audit zullen door de Verwerkingsverantwoordelijke worden gedragen, tenzij de audit aantoont dat de Verwerker zich niet aan de regels houdt (in dat geval zal de Verwerker de redelijke kosten dragen). Indien uit de secundaire evaluatie blijkt dat de Verwerker zijn verplichtingen uit hoofde van deze Overeenkomst niet volledig nakomt, zal de Verwerker de tekortkomingen die uit de evaluatie naar voren zijn gekomen, onverwijld ongedaan maken en/of herstellen.

8. Subverwerkers

De volgende Subverwerker(s) voeren namens de Verwerker diensten uit met betrekking tot persoonsgegevens:

Naam van de subverwerker	Activiteit	Data locatie	Sub-sub verwerker/Activiteit/Locatie
Wolters Kluwer Global Business Services Italia. Via dei Missaglia 97 20142 Milano, Italia	Management van Cloud	Italë	AWS Europe (Amazon EMEA SARL)/Hosting/Duitsland AWS Europe (Amazon EMEA SARL)/Hosting–recovery-Backup /Ierland
DELLA AI UK Ltd. at 5 Countess Road, NW5 2NS, London, UK	Enkel voor Indexing Service*: service aanbieder en tweedelijnsondersteuning	Frankrijk	Orange Business service/ hosting/Frankrijk
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth, Germany	Enkel voor Teamdocs* (optie): dienstverlener	Duitsland	Telekom Deutschland GmbH (Scanplus GmbH)/hosting/Duitsland
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth, Germany	Enkel vor Teamdocs (optie) : tweedelijnsondersteuning	Duitsland	Toppan Merrill GmbH/software editor and support level 3/Duitsland
Claranet SAS 2 Rue Breguet, 75011 Paris, France	Only for Mail to Legisway* (option) : Hosting and datacenter	Frankrijk	Equinix/hosting/ Frankrijk Telecity/hosting / Frankrijk
Wolters Kluwer Global business services B.V. Zuidpoolsingel 2, 2408 ZE Alphen aan den Rijn, The Netherlands	Only for Word2PDF* (option): Hosting and datacenter	Nederland	Azure, Europe/Hosting