BIJLAGE 2BIS: LEGISWAY ENTERPRISE AVG PRODUCTINFORMATIEBLAD EN TECHNISCHE EN ORGANISATORISCHE MAATREGELEN

De Leverancier mag als Verwerker gedurende de uitvoering van de Overeenkomst Persoonsgegevens van de Klant verwerken om Softwarediensten en/of Professionele Diensten te verlenen, en bijvoorbeeld om de volgende diensten te verrichten:

- Installatie en configuratie van LEGISWAY ENTERPRISE
- Hosting en supervisie van LEGISWAY ENTERPRISE
- Gegevensmigratie
- Ondersteuning en Onderhoud
- Gebruikersopleidingen

De bepalingen van de Gegevensverwerkingsovereenkomst ('DPA') zijn in dit opzicht van toepassing tussen Leverancier en Klant en worden aangevuld met de volgende voorwaarden.

VERWERKING VAN PERSOONSGEGEVENS

A. Categorieën van Persoonsgegevens die worden verwerkt

De Verwerker zal de volgende categorieën van Persoonsgegevens van de Verwerkingsverantwoordelijke verwerken, en dat uitsluitend in het kader van de Overeenkomst:

- Identiteitsgegevens (familienaam, voornaam, loginnaam)
- Contactgegevens (adres, e-mail, IP-adres, telefoon, fax)
- Gedragsgegevens (gebruikersgeschiedenis)
- IP-adres van Gebruikers (controlespoor)

De Klant mag als Verwerkingsverantwoordelijke Klantgegevens betreffende de identificatie en het beheer van contracten en in bredere zin Klantgegevens betreffende de processen van de Juridische Afdelingen van bedrijven, waaronder Persoonsgegevens, invoeren, opslaan en bewerken in LEGISWAY ENTERPRISE.

De standaardconfiguratie van LEGISWAY ENTERPRISE bevat basisvelden waar de Klant Persoonsgegevens kan invullen en bewerken, zoals naam, adres, telefoonnummer, e-mailadres, geboortedatum, ...

Aanvullende optionele informatie mag ook worden ingevoerd als die noodzakelijk is voor een bepaald bedrijfsproces (adres van het bedrijf, zakelijk telefoonnummer) overeenkomstig het door de Klant bepaalde verwerkingsdoel. De aanwezigheid van dergelijke velden is het resultaat van een bewuste keuze van de Klant tijdens de projectfase (instellingen die de Klant aan de Leverancier heeft gevraagd) of tijdens het beheer van de Software (configuratie/instelling uitgevoerd door de klant of door een derde partij in naam van de Klant), en daarom is alleen de Klant ervoor aansprakelijk.

In de standaardconfiguratie van LEGISWAY ENTERPRISE zijn er geen vrije tekstvelden voor opmerkingen in de directory van natuurlijke personen. De aanwezigheid van dergelijke velden is het resultaat van een bewuste keuze van de Klant tijdens de projectfase (instelling/configuratie die de Klant aan de Leverancier heeft gevraagd) of tijdens het beheer van de Software (configuratie/instelling uitgevoerd door de klant of door een derde partij in naam van de Klant), en daarom is alleen de Klant ervoor aansprakelijk.

Persoonsgegevens worden door de Gebruikers via de Softwarefuncties ingevoerd voor de hier beschreven doeleinden. Persoonsgegevens worden niet rechtstreeks van de Betrokkenen zelf verkregen. De Verwerkingsverantwoordelijke bepaalt zelf en op eigen risico welke Persoonsgegevens hij aanmaakt, invoert en uploadt in LEGISWAY ENTERPRISE.

De subverwerker die LEGISWAY ENTERPRISE Cloud host mag geen gezondheidsgegevens hosten. Daarom beveelt de Leverancier de Klant aan om de configuratie van LEGISWAY ENTERPRISE met betrekking tot gezondheidsgegevens in dit opzicht te beperken.

B. Categorieën van Betrokkenen

LEGISWAY ENTERPRISE mag Persoonsgegevens van de volgende Betrokkenen verwerken:

- De gebruikers van LEGISWAY ENTERPRISE (vaak werknemers van de Verwerkingsverantwoordelijke)
- Ondertekenaars, managers, mensen van procurement, ... met betrekking tot contracten (Contracten-module en Dialoogvenster-module)

- Derde partijen in informatie over processen (Processen-module)
- Contacten, corporate officers, aandeelhouders en andere personen die verbonden zijn aan een bedrijf dat opgeslagen is in Legisway Enterprise (Corporate Housekeeping-module)
- Contacten (ontwerpers, uitvinders, ...) in informatie over merk- en octrooiaanvragen (IE-module)
- Contacten, managers en deelnemers in informatie over sitebeheer (Site-module)
- Derde partijen in informatie over vorderingen (Vorderingen-module)

C. Verwerkingsdoel

Het is de verantwoordelijkheid van de Klant om als Verwerkingsverantwoordelijke de doeleinden vast te leggen van de uitgevoerde Verwerking bij gebruik van LEGISWAY ENTERPRISE.

LEGISWAY ENTERPRISE mag voor de volgende doeleinden worden gebruikt:

- Beheer van een adresboek voor verschillende typen bedrijfsbestanden afhankelijk van de modules van Legisway Enterprise die de Verwerkingsverantwoordelijke heeft aangekocht (Contracten, Processen, Corporate Housekeeping, ...).
- Beheer van een lijst met bedrijven (al dan niet deel uitmakend van de groep van de Verwerkingsverantwoordelijke) die in de beheerde bedrijfsbestanden worden gebruikt.
- Beheer van een lijst met contacten binnen de beheerde bedrijven die in de beheerde bedrijfsbestanden worden gebruikt.
- Vanuit de beheerde gegevens informatie opzoeken en output genereren (grafisch of Excel).

Er is geen onderlinge verbinding met andere systemen vereist als maatstaf voor de goede werking van LEGISWAY ENTERPRISE, en in het bijzonder zal er geen informatie uit de directory van natuurlijke personen naar andere systemen worden geëxporteerd.

Hierbij dient opgemerkt te worden dat onderlinge verbindingen soms op vraag van de Klant worden geïmplementeerd. Ze worden dan onder supervisie van de Klant gerealiseerd tussen LEGISWAY ENTERPRISE en andere, door de Klant beheerde systemen.

D. Bewaartermijn

Als Verwerkingsverantwoordelijke bepaalt de Klant de bewaartermijn van Persoonsgegevens beheerd door/in LEGISWAY ENTERPRISE (contractbestanden, geschillen, informatie over contactidentificatie, bijbehorende documenten, ...).

In Cloudmodus zal de Leverancier back-ups maken en ze bewaren overeenkomstig de bepalingen van de Overeenkomst, inclusief die van de voorliggende Bijlage. In Lokale modus is de Klant verantwoordelijk voor het beveiligen en back-uppen van Klantgegevens.

Als Verwerkingsverantwoordelijke bewaart ook de Leverancier Klantgegevens, waaronder, indien van toepassing, Persoonsgegevens, en dat in de volgende gevallen en voor de volgende bewaartermijn:

- Persoonsgegevens via ondersteuning/helpdesk (informatie die de Klant verstrekt voor Onderhoudstickets): Klantgegevens, waaronder, indien van toepassing, Persoonsgegevens, zullen uit de ondersteuningsdatabanken van de Leverancier worden verwijderd zes (6) maanden na afloop van de Overeenkomst; de Klant zal als Verwerkingsverantwoordelijke er altijd voor zorgen dat geen specifieke Categorieën van Gegevens worden verzonden naar de Verwerker bij melding en verwerking van een Anomalie of gelijk welk incident aan de ondersteuningsdiensten van de Leverancier (in de vorm van screenshots, ...);

- Kopie van Klantgegevens (DUMP) aan ondersteuning/helpdesk: het is mogelijk dat de Leverancier om een technisch probleem op te lossen een gedeelte van de Klantgegevens, inclusief persoonsgegevens indien van toepassing, nodig heeft of moet kopiëren naar een testomgeving na eerst de toestemming van de Klant te hebben gevraagd. Deze Klantgegevens worden alleen gebruikt om het opgetreden probleem op te lossen en worden uit de testomgeving verwijderd zodra het incident aangepakt is;

- Na Gegevensmigratie: de Leverancier bewaart de gemigreerde Gegevens twee (2) maanden om indien nodig tijdens die periode de correcties af te ronden. De Klant is verantwoordelijk voor het kopiëren/back-uppen van de Gegevens en ze na die periode zo nodig ter beschikking te stellen van de Leverancier;

- Na beëindiging/afloop van de Overeenkomst: als onderdeel van de Omkeerbaarheidsdiensten, die opgenomen zijn in de Overeenkomst, worden Klantgegevens aan de Klant overgemaakt in het overeengekomen bestandsformaat. De Leverancier zal vervolgens de overeenkomstige databanken twee (2) maanden (of een andere periode zoals vastgelegd in de Overeenkomst) bewaren op de eigen servers alvorens ze volledig te vernietigen.

TECHNISCHE EN ORGANISATORISCHE BEVEILIGINGSMAATREGELEN

Overeenkomstig de Toepasselijke Wetgeving inzake Gegevensbescherming zal de Leverancier passende Technische en Organisatorische Beveiligingsmaatregelen ('TOMs') nemen, die beoordeeld zullen worden aan de hand van de stand van de techniek op het ogenblik van het afsluiten van de Overeenkomst, en na verloop van tijd deze TOMs evalueren, rekening houdend met de

implementatiekosten, aard, omvang, context en doeleinden van de Verwerking, alsook met de kans dat deze resulteert in een hoog risico voor de rechten en vrijheden van de Betrokkenen.

A. Toegangscontrole: Gebouwen

Sites van de Leverancier/Verwerker: de toegang tot de gebouwen van de Verwerker wordt gecontroleerd door zowel technische als organisatorische maatregelen: toegangscontrole met gepersonaliseerde badges, vergrendeling van deuren, ontvangstprocedures voor bezoekers. Als Verwerkingsverantwoordelijke moet ook de Klant ervoor zorgen dat adequate beveiligingsmaatregelen om toegang tot de eigen gebouwen te voorkomen worden geïmplementeerd.

Sites van de onderaannemer/Subverwerkers van de Leverancier (alleen Cloudmodus): bij uitvoering van de Overeenkomst is CLARANET de Subverwerker die hosting aanbiedt: zijn servers en platform bevinden zich in Frankrijk, in het Equinix Data Center, in een privéruimte voor CLARANET. De server met gerepliceerde databanken bevindt zich ook in Frankrijk, in een privéruimte voor CLARANET.

B. Toegangscontrole: systemen

Toegang tot netwerken, besturingssystemen, gebruikersbeheer en applicaties van de Leverancier vereist de nodige machtigingen: geavanceerde wachtwoordprocedures, automatische time-out en blokkering bij een onjuist wachtwoord, individuele accounts met geschiedenis, versleuteling, hardware- en softwarefirewalls.

De Klant moet als Verwerkingsverantwoordelijke ook ervoor zorgen dat adequate maatregelen voor beveiliging van de eigen wachtwoorden en andere elektronische toegangsgegevens worden geïmplementeerd.

C. Toegangscontrole: Gegevens

De Leverancier, die als Verwerker optreedt, treft de volgende maatregelen: gebruikersbeheer en gebruikersaccounts met specifieke toegang, opgeleid personeel voor gegevensverwerking en -beveiliging, scheiding tussen besturingssystemen en testomgevingen, toekenning van specifieke rechten en het bewaren van loggegevens over gebruik, toegang en verwijdering.

D. Gegevensversleuteling en bescherming van uitwisselingen

Toepasselijke gegevensstromen tussen de Klant en de Leverancier worden versleuteld via het HTTPS-protocol.

Voor uitwisselingen met betrekking tot de implementatie van LDAP- of SSO-authenticatie bij Cloud-installaties beveelt de Leverancier het gebruik van een versleutelde IPSEC-tunnel aan.

Als de Klant bij Cloud-installaties interfaces tussen de Software en een eigen systeem wil opzetten, beveelt de Leverancier ook de implementatie van een versleutelde IPSEC-tunnel aan.

Berichten (e-mails) worden door het platform verstuurd om Gebruikers te informeren over bepaalde gebeurtenissen (vervaldata, uit te voeren taken, ...). Deze e-mails worden niet versleuteld, maar ze bevatten absoluut geen kritieke bedrijfsgegevens, en in het bijzonder geen content (contract, bijbehorend document, ...).

Als optie kunnen Leveranciers bepaalde gevoelige gegevensvelden (met gevoelige gegevens) in de databank versleutelen. Als de Klant voor deze optie heeft betaald bepalen de Klant en de Leverancier welke velden versleuteld worden. Deze velden worden door de applicatieserver versleuteld en ontsleuteld als ze worden gebruikt om gelezen of ingevuld te worden.

E. Softwareontwikkeling

Bij de ontwikkeling van de Software past de Leverancier de good practices toe die worden aanbevolen door OWASP (www.owasp.org), en meer specifiek over de aanbevelingen van het 'Top 10'-project: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

Er worden regelmatig veiligheidstests uitgevoerd. De resultaten van die tests worden gebruikt om de restrisico's te blijven beperken.

F. Middelen om de vertrouwelijkheid, integriteit, beschikbaarheid en aanhoudende veerkracht van verwerkingssystemen en -diensten te garanderen

F.1 Bij Leverancier

De toegangscontrole tot Persoonsgegevens volgt de richtlijnen voor interne controle, met inbegrip van het beleid voor de toegang tot informatie van Kluwer, de implementatie van een gebruikersbeheersysteem en toegangsrechten, de bewustmaking van werknemers rond de omgang met informatie en wachtwoorden, de controle op de netwerktoegang en onderliggende applicaties. De maatregelen bestaan uit:

- een schriftelijke/geprogrammeerde machtigingsstructuur;
  gedifferentieerde toegangsrechten, bijv. om gegevens te lezen, wijzigen of verwijderen;

- een definitie van rollen;
- loggegevens over activiteit en audit

Persoonsgegevens worden afgescheiden. De maatregelen omvatten:

- scheiding van functies (productie-/testgegevens);
- afzondering van gevoelige gegevens;
- beperking van verwerkingsdoelen; compartimentering
- regels/maatregelen om te zorgen voor gescheiden opslag, wijziging, verwijdering en overdracht van gegevens.

'Lokale' installatie: specifieke maatregelen

Bij lokale installaties is de Klant verantwoordelijk voor de essentiële processen met betrekking tot gebruik en beveiliging.

Subverwerking: geen in toepassingsfase

Back-uppen en restoren: de Leverancier beveelt de uitvoering van dagelijkse back-ups aan. De uitvoering en verificatie van deze back-ups valt onder de uitsluitende aansprakelijkheid van de Klant.

Test-/acceptatieomgeving: de Leverancier raadt de Klant aan om minstens twee omgevingen op het eigen platform te hebben: een productieomgeving en een test-/acceptatieomgeving.

'Cloud'-installatie: specifieke maatregelen

Subverwerking*:* op de datum van inwerkingtreding van de Overeenkomst worden hosting en outsourcing van de servers van de Leverancier uitbesteed aan CLARANET.
CLARANET is ISO 27001-gecertificeerd voor de verrichte hostingactiviteiten voor de Leverancier.
Back-uppen en restoren: Configuraties van de applicatieservers worden dagelijks opgeslagen op de back-upinfrastructuur van CLARANET op een externe site.
De volledige databank van de Klant wordt dagelijks geback-upt op de back-upinfrastructuur van CLARANET op een externe site. Back-ups worden vier weken bewaard. Back-ups worden niet versleuteld.

Test-/acceptatieomgeving: de Leverancier raadt de Klant aan minstens twee omgevingen op het platform te hebben: een productieomgeving en een test-/acceptatieomgeving.

Toegangsfilter op basis van het IP-adres: onafhankelijk van de voorziene beveiliging door de identiteitsbeheeroplossing installeert de Leverancier voor de Klant een toegangsfilter op basis van een lijst met IP-adressen (witte lijst) overeenkomstig de publieke IP-adressen van de Internetgateways van de Klant.

Isolatie: de fysieke en logische architectuur zorgt ervoor dat de Klant in een omgeving werkt die geïsoleerd en afgescheiden is van andere klanten. Elke klant heeft een specifieke databank en een specifieke versie van de applicatieserver Tomcat.

Beveiligingsupdates: CLARANET controleert beveiligingsgebreken en ermee verbonden updates en geeft de Leverancier regelmatig aanbevelingen over beveiligingsupdates. Deze beveiligingsupdates worden regelmatig uitgevoerd op basis van de aanbevelingen.

Antivirusbescherming: de Software van de Leverancier is uitgerust met een antivirusoplossing, die wordt onderhouden.

Continuïteitsplan (BC)*:* een BCR is van kracht. Dat systeem voorziet in een failover van de dienstverlening naar een tweede datacenter in geval van een dienstonderbreking op de hoofdserver.

Procedure om beveiligingsincident te beheren: de Leverancier implementeert een beheersproces voor beveiligingsincidenten met melding van het Datalek overeenkomstig de Gegevensverwerkingsovereenkomst.

Wissen van gegevens*:* in overeenstemming met de bepalingen van de Overeenkomst.

F.2 Bij de Klant

Toelatingsbeheer: LEGISWAY ENTERPRISE integreert door ontwerp en standaardinstellingen aanpasbare functies voor de bescherming van Klantgegevens, waardoor de Klant het niveau van toegekende rechten om de voor Gebruikers toegankelijke informatie te segmenteren kan beheren en het passende beschermingsniveau kan bepalen overeenkomstig de te verwerken Persoonsgegevens.

Gebruikersprofielen worden door Klantbeheerders aan Gebruikers toegekend zodra ze in de Software vastgesteld/geregistreerd zijn.

De directory-gegevens van natuurlijke personen worden in de databank van de Software op dezelfde manier beschermd als alle bewerkte Gegevens in de Software. Ze zijn alleen via de Software toegankelijk voor Gebruikers die de overeenkomstige

machtigingen bekomen hebben van de Klant. De Klant moet daarom als Verwerkingsverantwoordelijke vertrouwelijkheidsregels opstellen naar eigen inzicht, en het is aan de Klant om de niveaus van Gebruikersmachtiging te bepalen volgens de gebruikersprofielen.

Tracking: LEGISWAY ENTERPRISE heeft een controlespoorfunctie die in de databank van de Klant een reeks gegevens opslaat over toegang en gebruik van elke gebruiker van de Software. Tot deze informatie behoort in het bijzonder de registratie van (geslaagde en mislukte) verbindingen alsook van gebruikte en/of gewijzigde content. Deze informatie is toegankelijk voor een gemachtigde beheerder van de Klant.

Authenticatie: Er zijn verschillende modi voor authenticatiebeheer beschikbaar, afhankelijk van de opties waarop de Verwerkingsverantwoordelijke zich heeft geabonneerd:

- Een 'eenvoudige' authenticatie aan de hand van gebruikersnamen en wachtwoorden, ingesteld/gekozen door de gebruikers en beheerders.
- Authenticatie via een link naar de LDAP-directory van de Verwerkingsverantwoordelijke.
- Authenticatie via integratie in een SSO-oplossing (Single Sign-On).
- Toegangsfilter op basis van het IP-adres. (Een witte lijst die overeenkomt met de publieke IP-adressen van de internetpaden van de Verwerkingsverantwoordelijke).

Bij eenvoudige authenticatie met gebruikersnaam/wachtwoord moet de Verwerkingsverantwoordelijke een wachtwoordbeleid toepassen. Dit beleid gaat over de volgende aspecten:

- Minimumlengte van het wachtwoord
- Moeilijkheid van het wachtwoord
- Verbod op 'triviale' wachtwoorden
- Regelmatige wijziging van het wachtwoord

Gegevensversleuteling: de Leverancier biedt een betalende optie aan om sommige Gegevensvelden (in de databank) te versleutelen. Het doel hiervan is deze informatie ontoegankelijk te houden, zelfs in geval van een niet-gemachtigde verspreiding van de databank van de Klant. Als de Klant deze optie heeft, worden de bewuste velden door de applicatieserver versleuteld en ontsleuteld als ze worden gebruikt om gelezen of gewijzigd te worden. De codeersleutels worden beheerd op applicatieserverniveau.

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

Het systeem van Legisway Enterprise wordt continu gecontroleerd:

- Claranet, de hostingpartner van de Verwerker, controleert constant beveiligingsfouten en bijbehorende updates en geeft de Verwerker regelmatig aanbevelingen over beveiligingsupdates. Op basis van deze aanbevelingen worden de beveiligingsupdates regelmatig uitgevoerd.
- Een onafhankelijk extern bedrijf voert elk jaar inbraaktests uit.
- Een inbraakdetectiesysteem is altijd actief en geeft realtimewaarschuwingen.
- Er wordt regelmatig een kwetsbaarheidsscan gedaan.

SUBVERWERKERS

Op de datum van inwerkingtreding van de Overeenkomst voeren de volgende Subverwerkers namens de Verwerker diensten uit met betrekking tot Persoonsgegevens.

Naam van de Subverwerker	Activiteit	Gegevenslocatie	Sub-subverwerker/Activiteit/Locatie
VP&White SAS 62 bis avenue André-Morizet, 92100 Boulogne-Billancourt	configuratie	Frankrijk	--
S. Blavet	configuratie	Frankrijk	--
Pharmadvize SARL 37 rue d'Amsterdam, 75008 Parijs	opleiding	Frankrijk	--
Opleiders, natuurlijke personen	opleiding	Frankrijk	--
Claranet SAS* 2 Rue Breguet, 75011 Parijs	Hosting en datacenter voor Cloud ENTERPRISE	Frankrijk	Equinix/hosting/Frankrijk Telecity/hosting/Frankrijk Telehouse/hosting/Frankrijk
DELLA AI UK Ltd.	Leverancier van indexdiensten	Frankrijk	Orange Business service/hosting/Frankrijk

5 Countess Road, NW5 2NS, Londen	en ondersteuning niveau 2		
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1 50354 Hürth, Germany	Leverancier van de dienst TeamDocs (optie)	Duitsland	Telekom Deutschland GmbH (Scanplus GmbH)/hosting/Duitsland
Wolters Kluwer Deutschland GmbH Wolters-Kluwer-Straße 1, 50354 Hürth, Germany	Ondersteuning niveau 2 TeamDocs (optie)	Duitsland	Smartwork Solutions GmnH/software-editor en ondersteuning niveau 3/Duitsland
Claranet SAS 2 Rue Breguet, 75011 Parijs	Hosting en datacenter Mail naar Legisway (optie)	Frankrijk	Equinix/hosting/Frankrijk Telecity/hosting/Frankrijk
Wolters Kluwer Global business services B.V. Zuidpoolsingel 2, 2408 ZE Alphen aan den Rijn, Nederland	Hosting en datacenter Word2PDF (optie)	Nederland	Azure, Europa/Hosting

* CLARANET is ISO 27001-gecertificeerd voor zijn hosting- en outsourcingactiviteiten