Wolters Kluwer

GDPR PRODUCTFICHE

Basecone

1. **Aard van de Verwerking**
   Integratie met onze boekhoudproducten Adsolut, Expert/M, Vero en Top Account.
   Geautomatiseerde verwerking en archivering van documenten waarna deze naar de boekhoudsoftware worden doorgestuurd en boekhoudkundig wordt verwerkt.

2. **Categorieën van Persoonsgegevens die verwerkt worden**
   Verwerker zal uitsluitend volgende categorieën van Persoonsgegevens verwerken in het kader van dit Addendum:

   ☒ identiteitsgegevens (naam, adres, gsm, e-mail, geboortedatum, nummerplaat, IP-adres, …)
   ☒ contactinformatie (adres, e-mail, IP-adres, IMEI, …)
   ☒ financiële informatie (bankrekeningnummer, lening, hypotheek, belegging, betaalgedrag, rating, …)

3. **Categorieën van Betrokkenen**

   ☒ klanten van Verantwoordelijke
   ☒ eigen werknemers Verantwoordelijke

4. **Doeleinden van de verwerking**

   ☒ financiën (verwerking en archivering van boekhoudkundige documenten)

   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:

   - Identificeren en oplossen van technische problemen en bugs
   - Optimaliseren van de gebruikservaring en interface
   - Ontwikkelen van nieuwe functies en verbeteringen die zijn afgestemd op de behoeften en voorkeuren van de gebruiker
   - Uitvoeren van algemene productanalyse om de efficiëntie en effectiviteit van de software te verbeteren

5. **Retentieperiode**
   Persoonsgegevens zullen verwerkt en bijgehouden worden gedurende volgende periodes:

   Ingevoerde Persoonsgegevens: tot onbepaalde tijd na einde van de overeenkomst indien gebruiker beslist (betaald) om archief te blijven consulteren.

   Persoonsgegevens via helpdesk support:onbekend hoelang persoonsgegevens na einde van de overeenkomst behouden blijven, maar kunnen op vraag wel worden verwijderd.

   Andere: een ongelimiteerde periode – overeenkomstig de wettelijke termijn voor boekhoudkundige stukken

6. **Beveiligingsmaatregelen**

   Technische en organisatorische maatregelen kunnen worden beschouwd als de stand der techniek op het moment van sluiten van de Overeenkomst van Dienstverlening. Verwerker zal technische en organisatorische 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:	
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.
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.
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.
Encryptie van gegevens:	in transit: https in rust: Data-opslag wordt transparant geëncrypteerd
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:	Scheiding van productie- en testomgeving, scheiding van specifieke gevoelige gegevens, automatische back-up, geavanceerde paswoordprocedures, specifieke gebruiksrechten, bijhouden van historiek.
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:	Ononderbroken stroomvoorziening, back-up datacenters op verschillende locaties, beveiligingssystemen in geval van brand of waterschade (blussystemen, vuurbestendige deuren, branddetectoren
Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen:	- Software scans op code en third party libraries - Thread modeling - Pen tests - Disaster Recovery - Security audits cf. Global WK Security
Beschikbare certificering:	- ISO/IEC/ 27001 certification

7. Subverwerkers

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

Naam	Adres	Doel van gebruik

Support	WKBE	Ondersteuning gebruiker bij werking Basecone
Dienst facturatie	WKBE	Aanrekenen gebruik

8. Doorgifte van persoonsgegevens

Alle Persoonsgegevens zoals opgenomen in deze productfiche worden doorgegeven aan volgende voorwaarden:
De Persoonsgegevens worden doorgegeven aan:

☒ doorgifte naar land in de Europese Economische Regio (= EU + Ijsland + Liechtenstein + Noorwegen)