

GDPR PRODUCTFICHE**InvoiceOne****1. Aard van de Verwerking**

Online facturatie applicatie.

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

4. Doeleinden van de verwerking

- financiën

5. Retentieperiode

Persoonsgegevens zullen verwerkt en bijgehouden worden gedurende volgende periodes:

Ingevoerde Persoonsgegevens: Zolang de klant niet vraagt om zijn gegevens te verwijderen blijven deze in het systeem.

Wolters Kluwer werkt aan een continue verbetering van haar dienstverlening en zal dan ook deze retentieperiodes in lijn met de geldende wetgeving brengen.

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: 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 historiek van gebruik, toegang en wissing.
Pseudonimisering van gegevens:	Geen pseudonimisering
Encryptie van gegevens:	Gegevens worden 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 wordt voorzien door Azure.
Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen:	We doen op regelmatige en systematische basis security audits.

7. Subverwerkers

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

Naam	Adres	Doel van gebruik
Microsoft Corporation (Azure) - Microsoft NV	Da Vincilaan 3 1930 Zaventem	Uitvoering van de gebruiksovereenkomst, onderhoud en ontwikkeling van het platform
Sendgrid	41 Corsham St London N1 6DR	Email service provider

8. Doorgifte van persoonsgegevens

De Persoonsgegevens zoals opgenomen in deze productfiche kunnen mogelijk door Microsoft doorgegeven worden naar de US onder het EU-US Privacy Shield programma, met bescherming door middel van een EU Model Contract dat gesloten werd. <https://privacy.microsoft.com/en-us/PrivacyStatement>