Wolters Kluwer

GDPR PRODUCTFICHE

Vero Licentie registratie

1. **Aard van de Verwerking**
   Registratie van de Vero licenties en de daarbij behorende installatiecodes.

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

   ☒ identiteitsgegevens: naam en bedrijfsnaam
   ☒ contactinformatie (adres, e-mail, IP-adres, IMEI, …)

3. **Categorieën van Betrokkenen**
   ☒ eigen klanten van de Verwerker

4. **Doeleinden van de verwerking**
   ☒ levering van goederen of diensten: installatie van software.

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

   Ingevoerde Persoonsgegevens: worden ingegeven en beheerd door de klant, dus zijn verantwoordelijkheid

   Persoonsgegevens via helpdesk support: ongelimiteerde periode.

   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: 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. Deze worden steeds door de Verantwoordelijke zelf beheerd. De Verwerker staat louter in voor het beheer van de initiële paswoorden.
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:	Verantwoordelijkheid van de Verantwoordelijke om back-up te voorzien, alsook voor de historiek. Gebruikersrechten, binnen de aangekochte modules, worden door de Verantwoordelijke beheerd.
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:	Verantwoordelijkheid van de Verantwoordelijke om back-up te voorzien.

7. Subverwerkers

Er wordt niet met subverwerkers gewerkt.

8. Doorgifte van persoonsgegevens

Er vindt geen doorgifte plaats.