GDPR PRODUCTFICHE

TopRouting

1. **Aard van de Verwerking**
   Leveranciersfacturen voorbereiden registratie, goedkeuring door budgethouders.

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

   ☒ identeitsgegevens uitgereikt door de overheid (rijksregisternummer, paspoort nummer, …)
   ☒ financiële informatie (bankrekeningnummer, …)

3. **Categorieën van Betrokkenen**
   ☒ eigen klanten van de Verwerker
   ☒ leveranciers, consultants, dienstverleners, auteurs, …

4. **Doeleinden van de verwerking**
   ☒ financiën

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

   Ingevoerde Persoonsgegevens: een ongelimiteerde periode

   Persoonsgegevens via helpdesk support: een 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. Verdere instructies over hoe de Verantwoordelijke zelf toegangscontrole manueel kan uitoefenen kunnen teruggevonden wordenin het het bestand “Doma_GDPR_DataRegister_Elements_Arco_v2”
Encryptie van gegevens:	De applicatiesoftware zorgt bij een niet geëncrypteerde file server niet voor encryptie. De keuze voor een alternatieve configuratie “gencrypteerde fileserver” is wel mogelijk voor de Verantwoordelijke. Deze kan zelf ook kiezen voor encryptie via andere methodes (via hardware, via harde schijf, via virtualisatie, via MS Server en SQL Server, ...)
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:	Instructies over hoe de Verantwoordelijke zelf paswoordprotocollen en gebruikshistoriek manueel kan beheren kunnen teruggevonden worden in het bestand “Doma_GDPR_DataRegister_Elements_Arco_v2”
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 bij Wolters Kluwer zelf.

7. Subverwerkers

Wolters Kluwer laat geen gegevens verwerken door Subverwerkers voor deze applicatie.

8. Doorgifte van persoonsgegevens

Er vindt geen doorgifte van de persoonsgegevens plaats.