GDPR PRODUCTFICHE
Aliment Verhaal

1. **Aard van de Verwerking**
   Aliment Verhaal is een online softwareprogramma, speciaal ontwikkeld voor gemeenten (Sociale Diensten). Met de applicatie is het mogelijk om complexe alimentatieberekeningen uit te voeren. Tevens kan het ingezet worden om de workflow en het documentbeheer van een verhaalsprocedures te regelen.

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

   - identiteitsgegevens (naam, adres, telefoonnummer, e-mail, geboortedatum, geslacht)
   - identeitsgegevens uitgereikt door de overheid (BSN)
   - contactinformatie (adres, telefoonnummer)
   - sociale status (leefsituatie)
   - financiële informatie (bankrekeningnummer, lening, hypotheek)
   - werkgegevens (huidige en vorige werkgever, salaris)

3. **Categorieën van Betrokkenen**
   - klanten van Verantwoordelijke
   - eigen werknemers Verantwoordelijke

4. **Doeleinden van de verwerking**
   - Financiën (alimentatieberekening)
   - Documentenbeheer

5. **Retentieperiode**

   Persoonsgegevens zullen verwerkt en bijgehouden worden gedurende volgende periodes:
   - Ingevoerde Persoonsgegevens: tot 12 maanden na einde van de Overeenkomst.
   - Persoonsgegevens via helpdesk support: tot 12 maanden na einde van de Overeenkomst.

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:	*Transport* De HTTPS-datatransmissie is versleuteld met een 2048-bit PKI certificaat. *In rust* Data staat encrypted opgeslagen op het platform.
Vermogen om blijvende vertrouwelijkheid, integriteit, beschikbaarheid, en veerkracht van verwerkingssystemen en -diensten te garanderen:	De productieversie van de applicatie draait op een aparte server waarvan periodiek een backup gemaakt wordt. De productie-omgeving is hiermee gescheiden van de testomgeving.
Vermogen om de beschikbaarheid van en toegang tot de Persoonsgegevens tijdig te herstellen in het geval van een fysiek of technisch incident:	De beschikbaarheid van gegevens wordt gecontroleerd door middel van een permanent netwerkmonitoringsysteem. Om gegevensverlies te voorkomen, wordt een dagelijkse gegevensback-up met een bewaartermijn van 30 uitgevoerd. Verdere maatregelen omvatten: • fysiek gescheiden opslag van back-upgegevensdragers; • mirroring van server-harde schijven (RAID); • antivirussystemen / SPAM-filters / firewall / inbraakdetectiesysteem / noodherstelplan; • brand / water beveiligingssystemen (inclusief brandblussysteem, branddeuren, rook / brandmelders)
Proces voor regelmatig testen, beoordelen en evalueren van de doelmatigheid van technische en organisatorische maatregelen om de veiligheid van de verwerking te garanderen:	Ieder kwartaal vindt er een vulnerability scan. Eventuele kwetsbaarheden die hierbij naar voren komen worden met hoge urgentie opgelost.

7. Subverwerkers

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

Naam	Adres	Doel van gebruik
Wise Automatisering	Brunlaan 2, 9321 TH Peize	Onderhoud software

8. Doorgifte van persoonsgegevens

Er vindt geen doorgifte van de persoonsgegevens plaats.