elari

Verwerkersovereenkomst

Versie: 27 oktober 2026

overeengekomen tussen

Verwerkingsverantwoordelijke:	
KvK registratienummer:	
Land van vestiging:	
Contactgegevens van Verwerkingsverantwoordelijke voor algemene verzoeken over de overeenkomst (bij voorkeur een generiek, niet-persoonsgebonden adres):	
Contactgegevens van Verwerkingsverantwoordelijke voor het melden van onrechtmatige verwerking(en) van persoonsgegevens (bij voorkeur een generiek, niet-persoonsgebonden adres):	
Verwerker:	**Elari B.V.**
KvK registratienummer:	34268115
Land van vestiging:	Nederland
Contactpersoon van Verwerker voor algemene verzoeken over de overeenkomst (naam, functie, contactgegevens):	Data Protection Manager (+31) 23 54 22 299 privacy@elari.nl
Contactpersoon van Verwerker voor het melden van onrechtmatige verwerking(en) van persoonsgegevens (naam, functie, contactgegevens):	Data Protection Manager (+31) 23 54 22 299 privacy@elari.nl

Hierna respectievelijk te noemen “Verwerkingsverantwoordelijke”, “Verwerker”, of “Partij” en gezamenlijk als de “Partijen”.

elari

Artikel 1 Inleiding

1.1. Beide Partijen bevestigen dat de ondergetekenden gevolmachtigd zijn om deze overeenkomst (“Overeenkomst”) namens Partijen aan te gaan. Deze Overeenkomst is van toepassing op Verwerkingen (zoals hieronder gedefinieerd) van Persoonsgegevens (zoals hieronder gedefinieerd) door Verwerker (zoals hieronder gedefinieerd) onder de volgende dienstenovereenkomsten (“Dienstenovereenkomsten”) tussen de Partijen:

- Mantelovereenkomst, bepaald per datum ondertekening met nummer:

1.2. Indien de Verwerkingsverantwoordelijke de in bovenstaande tabel genoemde contactpersoon (-personen) wijzigt, moet de Verwerker daarvan schriftelijk in kennis worden gesteld.

Artikel 2 Definities

2.1. De definities Verwerkingsverantwoordelijke, Betrokkene, Persoonsgegevens, Inbreuk in verband met Persoonsgegevens, Verwerking, Verwerker en Gevoelige Gegevens (Bijzondere Persoonsgegevens categorieën) in deze Overeenkomst hebben dezelfde betekenis zoals gebruikt in EU 2016/679 Algemene Verordening Gegevensbescherming (de ‘AVG’).

Artikel 3 Toepasselijkheid

3.1. De Overeenkomst regelt de Verwerking van Persoonsgegevens door de Verwerker namens de Verwerkingsverantwoordelijke, en beschrijft de technische en organisatorische maatregelen die de Verwerker treft ter bescherming van de Betrokkenen en hun Persoonsgegevens overeenkomstig de toepasselijke privacywetgeving, waaronder de AVG.

3.2. Het doel van de Verwerking van Persoonsgegevens door de Verwerker namens de Verwerkingsverantwoordelijke is de uitvoering van de Dienstenovereenkomst(en) en deze Overeenkomst.

3.3. Deze Overeenkomst heeft voorrang op tegenstrijdige bepalingen met betrekking tot de Verwerking van Persoonsgegevens in de Dienstenovereenkomst of in andere eerdere overeenkomsten of schriftelijke communicatie tussen de Partijen.

Artikel 4 Rechten en plichten van de Verwerker

4.1. De Verwerker zal Persoonsgegevens uitsluitend Verwerken namens en in overeenstemming met de schriftelijke instructies van de Verwerkingsverantwoordelijke. Door het aangaan van deze Overeenkomst draagt de Verwerkingsverantwoordelijke de Verwerker op om Persoonsgegevens op de volgende wijze te verwerken; i) uitsluitend in overeenstemming met de toepasselijke wetgeving, ii) ter nakoming van alle verplichtingen uit hoofde van de Dienstenovereenkomst, iii) zoals nader gespecificeerd via het gewone gebruik door de Verwerkingsverantwoordelijke van de diensten van de Verwerker en iv) zoals gespecificeerd in deze Overeenkomst.

4.2. De Verwerker heeft geen reden om aan te nemen dat wetgeving die op hem van toepassing is, de Verwerker verhindert om de hierboven genoemde instructies uit te voeren. De Verwerker zal, zodra hij hiervan op de hoogte raakt, de Verwerkingsverantwoordelijke in kennis stellen van instructies of andere Verwerkingsactiviteiten door de Verwerkingsverantwoordelijke die naar het oordeel van de Verwerker in strijd zijn met de toepasselijke privacywetgeving.

4.3. De categorieën van Betrokkenen en Persoonsgegevens die op grond van deze Overeenkomst aan Verwerking worden onderworpen, zijn vastgelegd in Appendix A.

4.4. De Verwerker waarborgt de vertrouwelijkheid, integriteit en beschikbaarheid van Persoonsgegevens overeenkomstig de toepasselijke privacywetgeving. De verplichtingen van de Verwerker met betrekking tot technische en organisatorische maatregelen treffen om een passend beveiligingsniveau te waarborgen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging in verhouding tot het risico dat de Verwerking vertegenwoordigt, en de aard van de te beschermen Persoonsgegevens.

4.5. De Verwerker zal, rekening houdend met de aard van de Verwerking en informatie waarover de Verwerker beschikt, de Verwerkingsverantwoordelijke met passende technische en organisatorische maatregelen bijstaan, voor zover mogelijk, bij het nakomen van de verplichtingen van de Verwerkingsverantwoordelijke:

A. om te reageren op verzoeken van Betrokkenen die hun rechten uitoefenen op grond van Hoofdstuk III van de AVG; en
B. om te voldoen aan de verplichtingen zoals vastgelegd in de artikelen 32 tot en met 36 van de AVG, waaronder ten aanzien van de beveiliging van de verwerking, melding van Inbreuken in verband met Persoonsgegevens, gegevensbeschermingseffectbeoordelingen en voorafgaande raadpleging van toezichthoudende autoriteiten.

Indien de door de Verwerkingsverantwoordelijke op grond van dit artikel 4.5 vereiste bijstand verder gaat dan wat redelijkerwijs noodzakelijk is in het kader van de standaard dienstverlening, kan de Verwerker de Verwerkingsverantwoordelijke voor dergelijke aanvullende bijstand kosten in rekening brengen op basis van de dan geldende tarieven, overeenkomstig artikel 4.6.

4.6. Indien de Verwerkingsverantwoordelijke informatie of bijstand verzoekt met betrekking tot beveiligingsmaatregelen, documentatie of andere vormen van informatie over de wijze waarop de Verwerker Persoonsgegevens verwerkt, en dergelijke verzoeken verder gaan dan de standaardinformatie die de Verwerker als Verwerker verstrekt ter naleving van de toepasselijke privacywetgeving, kan de Verwerker de Verwerkingsverantwoordelijke voor dit verzoek om aanvullende dienstverlening kosten in rekening brengen.

4.7. De Verwerker stelt de Verwerkingsverantwoordelijke zonder onredelijke vertraging in kennis, en in ieder geval binnen achtenveertig (48) uur, nadat hij kennis heeft gekregen van een Inbreuk in verband met Persoonsgegevens die betrekking heeft op Persoonsgegevens die in het kader van deze Overeenkomst worden verwerkt. Deze kennisgeving bevat, voor zover de informatie op het moment van kennisgeving beschikbaar is, de onderstaande informatie:

- Welke specifieke persoonsgegevens erbij betrokken zijn (bijv. namen, e-mails, financiële data).
- Hoeveel personen (betrokkenen) er zijn getroffen.

- Wat er precies is gebeurd (bijv. ongeautoriseerde toegang, per ongeluk openbaar gemaakt, dataverlies).
- Wie er precies is getroffen (bijv. medewerkers, klanten of derden).
- Hoe de data gecompromitteerd is (bijv. een systeemfout of een menselijke fout).
- De actuele status: of het incident nog gaande is, of dat het lek inmiddels gedicht is.
- Eventuele logbestanden of ander bewijsmateriaal dat meer details kan verschaffen.
- Welke verbetermaatregelen worden genomen om herhaling te voorkomen.

Indien het niet mogelijk is alle informatie tegelijkertijd te verstrekken, kan deze gefaseerd worden verstrekt zonder onredelijke vertraging, naarmate de informatie beschikbaar komt.

4.8. De Verwerker zal niet rechtstreeks reageren op verzoeken van Betrokkenen met betrekking tot Persoonsgegevens die in het kader van deze Overeenkomst worden verwerkt, tenzij hij daartoe schriftelijk is gemachtigd door de Verwerkingsverantwoordelijke. De Verwerker zal Persoonsgegevens of enige informatie betreffende deze Overeenkomst niet verstrekken aan overheidsinstanties (waaronder, maar niet beperkt tot, wetshandhavingsinstanties, toezichthouders of rechterlijke instanties), behalve wanneer dit op grond van toepasselijk Unierecht of nationaal recht, een rechterlijk bevel of ander juridisch bindend instrument verplicht is. Indien de Verwerker wettelijk verplicht is een dergelijke verstrekking te doen, stelt hij, voor zover toegestaan op grond van het toepasselijke recht, de Verwerkingsverantwoordelijke vooraf in kennis. Partijen zullen in dat geval te goeder trouw samenwerken om de rechtmatigheid van de vordering te toetsen en de impact op de privacy van Betrokkenen tot een minimum te beperken. Wanneer voorafgaande kennisgeving niet mogelijk is, stelt hij de Verwerkingsverantwoordelijke zo spoedig mogelijk na de verstrekking in kennis.

4.9. De Verwerker kan API's en vergelijkbare mechanismen beschikbaar stellen waarmee de Verwerkingsverantwoordelijke zelf applicaties van derden met het platform kan integreren ("**Integraties van Derden**"). Een derde partij die via een Integratie van Derden persoonsgegevens ontvangt, kwalificeert niet als subverwerker van de Verwerker en handelt op basis van haar rechtstreekse overeenkomst met de Verwerkingsverantwoordelijke. De Verwerkingsverantwoordelijke is zelf verantwoordelijk voor de rechtsgrondslag, de overeenkomst met de derde partij en de informatie aan Betrokkenen. De Verwerker is niet aansprakelijk voor verwerkingen door de derde partij, behoudens een gebrek in de API of het platform van de Verwerker.

4.10. Bij het verlenen van de diensten verwerkt de Verwerker gegevens die worden gegenereerd in het kader van de toegang tot en het gebruik van de diensten, alsmede in het kader van de ondersteuning en evaluatie van de dienstverlening ("**Dienstverbeteringsgegevens**"). De Verwerker verwerkt Dienstverbeteringsgegevens als zelfstandig Verwerkingsverantwoordelijke ten behoeve van het optimaliseren van de diensten, het ontwikkelen van nieuwe functionaliteiten, het verlenen van klantondersteuning, het meten van klanttevredenheid en het nakomen van eigen wettelijke en beveiligingsverplichtingen. De categorieën Dienstverbeteringsgegevens, de toepasselijke grondslagen en de bewaartermijnen zijn uitgewerkt in onderstaande tabel. Deze verwerking valt niet onder deze Overeenkomst.

Groep	Grondslag	Bewaartermijn*
Beveiliging en probleemoplossing	Gerechtvaardigd belang *Het verwerken van technische en operationele gegevens (zoals systeemlogbestanden, mutatielogs en foutrapportages) ter waarborging van de beveiliging, integriteit en beschikbaarheid van de dienst, evenals voor probleemoplossing (troubleshooting).*	3 maanden
Support Tickets	Gerechtvaardigd belang *Adequaat verweer bij juridische geschillen, klachten of aansprakelijkheidsclaims. Verbeteren van dienstverlening.*	7 jaar
Klanttevredenheid	Gerechtvaardigd belang *Verbeteren van dienstverlening.*	3 jaar
Gebruikerstelemetrie en platformstatistieken	Gerechtvaardigd belang *Verbeteren en doorontwikkelen van de diensten op basis van geaggregeerde gegevens over gebruikspatronen, waaronder paginaweergaven, klikken, sessies en gebeurtenissen rond het gebruik van functionaliteiten.*	2 jaar

** Verwerker kan (een selectie van) Dienstverbeteringsgegevens langer bewaren dan de in de tabel vermelde termijnen, indien en voor zolang daarvoor gerechtvaardigde redenen bestaan, zoals de afhandeling of het onderzoek van een beveiligingsincident, een onderzoek door of verzoek van een overheidsinstantie (waaronder een opsporings- of toezichthoudende instantie), het vaststellen, uitoefenen of verdedigen van rechtsvorderingen, of het onderzoeken of voorkomen van fraude of ander onrechtmatig handelen. De Verwerker bewaart de aldus aangewezen gegevens niet langer dan noodzakelijk voor het doel van de verlengde bewaring.*

4.11. Bij het gebruik van de dienst voegt de Verwerkingsverantwoordelijke gegevens toe aan de Software ("**Klantgegevens**"). De Verwerker of Subverwerker mag uit Klantgegevens geanonimiseerde en geaggregeerde datasets afleiden ("**Geanonimiseerde Afgeleide Gegevens**") ten behoeve van het verbeteren en ontwikkelen van de diensten, intern onderzoek en statistische analyse, en het genereren van benchmarkrapporten. Voorafgaand aan dergelijk gebruik draagt de Verwerker of Subverwerker er zorg voor dat de gegevens zodanig zijn geanonimiseerd dat zij niet langer kunnen worden herleid tot een geïdentificeerde of identificeerbare natuurlijke persoon, rekening houdend met alle middelen waarvan redelijkerwijs te verwachten is dat zij voor heridentificatie worden ingezet. Geanonimiseerde Afgeleide Gegevens vormen geen Persoonsgegevens en vallen niet onder deze Overeenkomst.

Artikel 5 Rechten en plichten van Verwerkingsverantwoordelijke

5.1 De Verwerkingsverantwoordelijke staat ervoor in dat hij:

- op de datum van ondertekening en doorlopend gedurende de looptijd van deze Overeenkomst, over een geldige en gedocumenteerde rechtsgrondslag op grond van de toepasselijke gegevensbeschermingswetgeving beschikt (waaronder, waar van toepassing, de artikelen 6 en 9 van de AVG) om de betreffende Persoonsgegevens te verwerken en aan de Verwerker te verstrekken.
- als enige verantwoordelijk is voor de juistheid, integriteit, volledigheid, betrouwbaarheid en rechtmatigheid van de aan de Verwerker verstrekte Persoonsgegevens. Indien de Verwerkingsverantwoordelijke constateert dat aan de Verwerker verstrekte Persoonsgegevens onjuist, onvolledig of niet langer actueel zijn, stelt hij de Verwerker hiervan zonder onnodige vertraging in kennis en verstrekt hij gecorrigeerde gegevens of draagt hij de Verwerker schriftelijk op om de betreffende Persoonsgegevens overeenkomstig de AVG te rectificeren, te beperken of te wissen.
- heeft voldaan, en gedurende de gehele looptijd van deze Overeenkomst zal blijven voldoen, aan zijn verplichtingen om relevante informatie te verstrekken aan Betrokkenen en samen te werken met bevoegde toezichthoudende autoriteiten met betrekking tot de Verwerking van Persoonsgegevens overeenkomstig de verplichte gegevensbeschermingswetgeving.
- de privacyverklaringen en registers van verwerkingsactiviteiten zal bijwerken voor zover nodig om de door de Verwerker in het kader van deze Overeenkomst uitgevoerde verwerkingsactiviteiten nauwkeurig weer te geven.
- bij het ontvangen en gebruik van de diensten van Verwerker onder de Dienstenovereenkomsten, geen Gevoelige Gegevens aan Verwerker zal bekendmaken/verstrekken, tenzij expliciet overeengekomen in Appendix A bij deze Overeenkomst.

Artikel 6 Inschakelen derden voor Verwerker en data-overdracht

6.1. Als onderdeel van de dienstverlening aan de Verwerkingsverantwoordelijke op grond van de Dienstenovereenkomsten en deze Overeenkomst, zal Verwerker gebruik maken van subverwerkers en de Verwerkingsverantwoordelijke verleent hiervoor algemene toestemming. Dergelijke subverwerkers kunnen andere bedrijven binnen de Visma groep zijn of externe subverwerkers. De Verwerker waarborgt dat subverwerkers instemmen met het aanvaarden van verantwoordelijkheden die overeenkomen met de verplichtingen zoals neergelegd in deze Overeenkomst.

6.2. Een actueel overzicht van de huidige subverwerkers met toegang tot Persoonsgegevens is beschikbaar in het Visma Trust Centre en raadpleegbaar via: https://www.visma.com/trust-centre-products/elari. Deze online lijst is leidend en vervangt eventuele eerdere overzichten in bijlagen. De Verwerkingsverantwoordelijke kan meer gedetailleerde informatie opvragen over subverwerkers, waaronder de aard van de door die subverwerker uitgevoerde verwerking en het toegepaste rechtmatige doorgiftemechanisme indien de subverwerker buiten de EU/EER is gevestigd.

6.3. De Verwerker is gerechtigd de Persoonsgegevens buiten de EU/EER door te geven, mits die doorgifte voldoet aan de relevante bepalingen van Hoofdstuk V van de AVG (zoals een doorgifte op basis

van een adequaatheidsbesluit (artikel 45 van de AVG) of een doorgifte op basis van passende waarborgen (artikel 46 van de AVG), of een doorgifte op basis van bindende bedrijfsvoorschriften (artikel 47 AVG)).

6.4. De Verwerker stelt de Verwerkingsverantwoordelijke met een redelijke voorafgaande schriftelijke kennisgeving in kennis van elke beoogde toevoeging of vervanging van een subverwerker. Deze kennisgeving wordt gedaan met een minimale kennisgevingstermijn van dertig (30) dagen voordat de wijziging van kracht wordt, tenzij onmiddellijke vervanging noodzakelijk is om de beveiliging of beschikbaarheid van de dienstverlening te garanderen. In dat geval geschiedt de melding onverwijld na de aanstelling. Indien daar geen sprake van is, kan Verwerkingsverantwoordelijke bezwaar maken door de Verwerker binnen dertig (30) dagen na ontvangst van de kennisgeving schriftelijk van zijn bezwaar in kennis te stellen, met opgave van de redenen voor zijn bezwaar. Indien de Verwerkingsverantwoordelijke bezwaar maakt, zullen de Partijen te goeder trouw samenwerken om de bezwaren van de Verwerkingsverantwoordelijke op te lossen, onder meer doordat de Verwerker nadere informatie verstrekt over de nalevingsmaatregelen van de subverwerker. Indien de Verwerkingsverantwoordelijke zijn bezwaar handhaaft en Partijen de bezwaren van de Verwerkingsverantwoordelijke niet kunnen oplossen, kan de Verwerkingsverantwoordelijke de specifieke Dienstenovereenkomst(en) waarvoor de betreffende subverwerker wordt ingeschakeld, opzeggen door de Verwerker schriftelijk in kennis te stellen. Indien de Verwerkingsverantwoordelijke niet binnen de kennisgevingstermijn bezwaar maakt, wordt hij geacht de wijziging van de subverwerker te hebben aanvaard.

Artikel 7 Beveiliging

7.1. De Verwerker treft en handhaaft passende technische en organisatorische beveiligingsmaatregelen ter bescherming van Persoonsgegevens die in het kader van deze Overeenkomst worden verwerkt. Dergelijke maatregelen zijn passend voor het risico dat de verwerking met zich meebrengt, rekening houdend met de stand van de techniek, de kosten van de tenuitvoerlegging en de aard, omvang, context en doeleinden van de verwerking, zoals vereist op grond van artikel 32 van de AVG.

7.2. Onverminderd het bepaalde in artikel 7.1 omvatten dergelijke maatregelen de maatregelen zoals opgenomen in Appendix C. De Verwerker kan zijn beveiligingsmaatregelen van tijd tot tijd bijwerken of aanpassen, met dien verstande dat dergelijke bijwerkingen het algehele beschermingsniveau van Persoonsgegevens op grond van deze Overeenkomst niet leiden tot een lager beveiligingsniveau dan bij aanvang was afgesproken. Indien een voorgenomen wijziging de beveiligingspositie met betrekking tot de Persoonsgegevens van de Verwerkingsverantwoordelijke wezenlijk zou beïnvloeden, stelt de Verwerker de Verwerkingsverantwoordelijke hiervan met een redelijke voorafgaande kennisgeving in kennis.

7.3. De Verwerkingsverantwoordelijke is verantwoordelijk voor het treffen en handhaven van beveiligingsmaatregelen die passen bij zijn eigen verwerkingsomgeving, waaronder de beveiliging van de apparatuur, systemen en IT-infrastructuur die onder de zeggenschap van de Verwerkingsverantwoordelijke vallen en waarmee Persoonsgegevens worden benaderd of doorgegeven.

Artikel 8 Auditrechten

8.1. De Verwerkingsverantwoordelijke kan de naleving van deze Overeenkomst door de Verwerker maximaal eenmaal per jaar controleren. Indien de op de Verwerkingsverantwoordelijke van toepassing zijnde wetgeving dit vereist, kan de Verwerkingsverantwoordelijke om frequentere audits verzoeken. Om

een audit aan te vragen, dient de Verwerkingsverantwoordelijke ten minste vier (4) weken voor de voorgestelde auditdatum een gedetailleerd auditplan in bij de Verwerker, waarinde voorgestelde omvang, duur en aanvangsdatum van de audit worden beschreven. Audits worden te allen tijde uitgevoerd door een neutrale derde-auditor.

8.2. Voordat de Verwerkingsverantwoordelijke overgaat tot een directe audit, verzoekt de Verwerkingsverantwoordelijke eerst om eventuele bestaande auditrapporten, certificeringen of assurance-documentatie waarover de Verwerker beschikt en die betrekking kunnen hebben op de voorgestelde auditomvang (zoals ISAE 3402- of ISO 27001-rapporten) die zijn afgegeven in de voorafgaande twaalf (12) maanden ("**Bestaande Assurance-rapporten**"). Indien een Bestaand Assurance-rapport de voorgestelde auditomvang afdoende dekt, aanvaardt de Verwerkingsverantwoordelijke dit in plaats van een directe audit. Indien het de omvang slechts gedeeltelijk dekt, mag de Verwerkingsverantwoordelijke uitsluitend de resterende onderwerpen auditen. De Verwerker stelt Bestaande Assurance-rapporten beschikbaar met inachtneming van de geheimhoudingsverplichtingen in deze Overeenkomst en eventuele toepasselijke beperkingen van derden.

8.3. In ieder geval moeten audits worden uitgevoerd tijdens de reguliere kantooruren van de betreffende vestiging, met inachtneming van het beleid van de Verwerker, en mogen zij de bedrijfsactiviteiten van de Verwerker niet op onredelijke wijze hinderen. De Verwerker is niet verplicht toegang te verlenen tot: (i) informatie over andere klanten van de Verwerker; (ii) informatie die de Verwerker op grond van het toepasselijke recht of bindende vertrouwelijkheidsverplichtingen jegens derden niet mag openbaren; of (iii) systemen of locaties die buiten de reikwijdte van het overeengekomen auditplan vallen.

8.4. Alle bevindingen, observaties of documentatie die in het kader van een audit worden verkregen, worden behandeld als Vertrouwelijke Informatie van de Verwerker overeenkomstig artikel 9 van deze Overeenkomst en worden door de Verwerkingsverantwoordelijke uitsluitend gebruikt voor het beoordelen van de naleving van deze Overeenkomst door de Verwerker.

8.5. De Verwerkingsverantwoordelijke is verantwoordelijk voor alle kosten die voortvloeien uit de door de Verwerkingsverantwoordelijke gevraagde audits, inclusief de kosten van een derde auditor. De redelijke kosten van de Verwerker voor het faciliteren van een audit komen voor rekening van de Verwerkingsverantwoordelijke, tenzij de audit een wezenlijke schending door de Verwerker van zijn verplichtingen op grond van deze Overeenkomst of de toepasselijke privacywetgeving aan het licht brengt, in welk geval de Verwerker zijn eigen kosten draagt.

Artikel 9 Vertrouwelijkheid

9.1. Iedere Partij behandelt alle Vertrouwelijke Informatie die zij in verband met deze Overeenkomst van de andere Partij ontvangt als vertrouwelijk en maakt deze niet openbaar aan derden zonder voorafgaande schriftelijke toestemming van de openbarende Partij. "**Vertrouwelijke Informatie**" betekent alle informatie die door een Partij aan de andere wordt verstrekt die als vertrouwelijk is aangemerkt of die redelijkerwijs als vertrouwelijk moet worden aangemerkt in de gegeven omstandigheden, waaronder Persoonsgegevens die in het kader van deze Overeenkomst worden verwerkt, de bepalingen van deze Overeenkomst en de technische systemen en beveiligingsmaatregelen van iedere Partij.

9.2. De ontvangende Partij kan Vertrouwelijke Informatie openbaar maken: (i) aan medewerkers, aannemers, subverwerkers en professionele adviseurs die deze informatie nodig hebben voor de doeleinden van deze Overeenkomst en gebonden zijn door gelijkwaardige vertrouwelijkheidsverplichtingen; of (ii) voor zover vereist door het toepasselijke recht of een bevoegde autoriteit, op voorwaarde dat de ontvangende Partij, voor zover wettelijk toegestaan, de openbarende Partij vooraf schriftelijk in kennis stelt en de openbaarmaking beperkt tot wat strikt noodzakelijk is.

9.3. De Verwerker waarborgt dat al het personeel en alle subverwerkers die op grond van deze Overeenkomst bevoegd zijn tot toegang tot Persoonsgegevens, gebonden zijn aan bindende vertrouwelijkheidsverplichtingen, hetzij door schriftelijke verbintenis hetzij door wettelijke verplichting.

9.4. De verplichtingen in dit artikel 9 zijn niet van toepassing op informatie die: (i) openbaar is of wordt zonder dat de ontvangende Partij daarvoor verantwoordelijk is; (ii) reeds rechtmatig bij de ontvangende Partij bekend was vóór de openbaarmaking; (iii) is ontvangen van een derde partij zonder beperkingen; of (iv) onafhankelijk is ontwikkeld zonder gebruik te maken van de Vertrouwelijke Informatie van de openbarende Partij.

9.5. Niets in dit artikel 9 beperkt de verplichtingen van een van de Partijen op grond van de toepasselijke privacywetgeving. In geval van strijdigheid prevaleert de strengere verplichting.

Artikel 10 Duur en beëindiging

10.1. Deze Overeenkomst is geldig zolang de Verwerker Persoonsgegevens verwerkt namens de Verwerkingsverantwoordelijke in het kader van de Dienstenovereenkomsten of zoals anderszins overeengekomen in Appendix A.

10.2. Deze Overeenkomst wordt automatisch beëindigd bij beëindiging van de Dienstenovereenkomsten. Bij beëindiging of afloop van deze Overeenkomst zal de Verwerker Persoonsgegevens die namens de Verwerkingsverantwoordelijke zijn verwerkt, wissen. Deze verwijdering zal zo spoedig als redelijkerwijs mogelijk is, maar uiterlijk binnen 6 maanden na de datum van beëindiging of afloop van deze Overeenkomst, plaatsvinden, tenzij het toepasselijke EU-recht of nationaal recht de Verwerker verplicht een deel of alle Persoonsgegevens langer te bewaren. Wanneer de Verwerkingsverantwoordelijke de plicht heeft of het voor de Verwerkingsverantwoordelijke anderzijds noodzakelijk is om de Persoonsgegevens langer te bewaren, dan zal de Verwerkingsverantwoordelijke voorafgaand aan beëdiging van de Dienstenovereenkomsten een overeenkomst sluiten met de Verwerker om toegang tot de Persoonsgegevens te behouden of afspraken maken om de Persoonsgegevens over te dragen.

Artikel 11 Wijzigingen en amendementen

11.1. Geen enkele wijziging of aanpassing van deze Overeenkomst is geldig of bindend tenzij deze schriftelijk is gedaan en ondertekend door een naar behoren gemachtigde vertegenwoordiger van iedere Partij. Onverminderd het voorgaande kan de Verwerker Appendix B (Subverwerkers) en Appendix C (Beveiligingsmaatregelen) bijwerken overeenkomstig de kennisgevingsprocedure in artikel 6.4, zonder dat een formele schriftelijke wijziging door beide Partijen ondertekend hoeft te worden.

11.2. Indien enige bepaling van deze Overeenkomst nietig, onwettig of niet-afdwingbaar is of wordt op grond van het toepasselijke recht, wordt die bepaling geacht te zijn gewijzigd tot de minimale mate die nodig is om haar geldig, wettig en afdwingbaar te maken. Indien een dergelijke wijziging niet mogelijk is, wordt de betreffende bepaling geacht te zijn geschrapt. In beide gevallen worden de geldigheid, wettigheid en afdwingbaarheid van de overige bepalingen van deze Overeenkomst niet aangetast. Indien een bepaling wordt gewijzigd of geschrapt, onderhandelen de Partijen te goeder trouw over een vervangende bepaling die, voor zover mogelijk, hetzelfde juridische en commerciële doel bereikt als de oorspronkelijke bepaling.

Artikel 12 Aansprakelijkheid

12.1. Alle aansprakelijkheid tussen de Partijen die voortvloeit uit of verband houdt met deze Overeenkomst wordt uitsluitend beheerst door de aansprakelijkheidsbepalingen van de toepasselijke Dienstenovereenkomst. Voor zover een vordering op grond van deze Overeenkomst ontstaat in plaats van rechtstreeks op grond van de Dienstenovereenkomst, zijn dezelfde beperkingen en uitsluitingen van aansprakelijkheid van toepassing als ware de vordering ingesteld op grond van de Dienstenovereenkomst.

elari

Artikel 13 Toepasselijk recht en forumkeuze

13.1. Deze Overeenkomst wordt beheerst door het toepasselijke recht van de Dienstenovereenkomsten. De in de Dienstenovereenkomsten genoemde bevoegde rechter is mutatis mutandis bevoegd kennis te nemen van geschillen rondom deze Overeenkomst.

Deze Overeenkomst wordt digitaal ondertekend.

Gegevens Verwerkingsverantwoordelijke:	
Handtekening:	
Door:	
Plaats en datum:	

Gegevens Verwerker:	
Handtekening:	
Door:	
Plaats en datum:	

Elari B.V.

een handelsnaam van Visma
Richard Holkade 9
2033 PZ Haarlem

Contact
T 023 – 5422299
E administratie@elari.nl
W www.elari.nl

Bedrijfsinformatie
IBAN NL17RABO0384422292
Btw NL8258.50.320B01
KvK 34268115

elari

Appendix A – Betrokkenen, Soorten persoonsgegevens, Doel, Aard, Duur

A.1 Categorieën van Betrokkenen

- Eindgebruikers van de klant
- Klantmedewerkers
- Contactpersonen voor de klant

A.2 Categorieën van Persoonsgegevens

- Contactgegevens, zoals naam, telefoon, adres, e-mail
- Functie-informatie, zoals functie, bedrijf
- Financiële informatie ten aanzien van zakelijke inkomsten en uitgaven via Elari.

A.3 Bijzondere categorieën Persoonsgegevens (Gevoelige Persoonsgegevens)

Indien de Verwerker dergelijke gegevens namens de Verwerkingsverantwoordelijke mag verwerken, moeten de betrokken soorten Gevoelige Persoonsgegevens hieronder door de Verwerkingsverantwoordelijke worden gespecificeerd.

De verantwoordelijke voor de verwerking is tevens verantwoordelijk voor het informeren van de Verwerker over, en het hieronder specificeren van, eventuele aanvullende soorten Gevoelige Persoonsgegevens overeenkomstig de toepasselijke privacywetgeving.

Verwerker zal, ten behoeve van Verwerkingsverantwoordelijke, informatie verwerken over:	***Ja***	***Nee***
ras of etnische afstamming, of politieke, filosofische of religieuze overtuigingen,		
dat een persoon verdacht wordt van een strafbaar feit, een strafbaar feit ten laste wordt gelegd en/of voor een strafbaar feit is veroordeeld,		
gezondheidsinformatie,		
seksuele geaardheid,		
lidmaatschap vakbond,		
genetische of biometrische gegevens.		

Elari B.V.
een handelsnaam van Visma
Richard Holkade 9
2033 PZ Haarlem

Contact
T 023 – 5422299
E administratie@elari.nl
W www.elari.nl

Bedrijfsinformatie
IBAN NL17RABO0384422292
Btw NL8258.50.320B01
KvK 34268115

elari

A.4 Doel van de Verwerking

Het doel van de verwerking van persoonsgegevens door de gegevensverwerker ten behoeve van de verantwoordelijke voor de verwerking zijn:

- Het leveren van diensten in overeenstemming met de Dienstenovereenkomst (gebruik van Elari). Afhankelijk van de afgenomen modules is dat bijvoorbeeld:
    - Het verwerken van inkoopfacturen.
    - Beheer van contracten.
    - Het plaatsen en beheren van bestellingen.
    - Het beheren en uitgaven doen met zakelijke betaalpassen.
    - Het voeren van een cliëntgelden administratie.
    - Administratie van contact- en contractgegevens van de Verwerkingsverantwoordelijke

A.5 Aard van de Verwerking

De verwerking van persoonsgegevens door de Verwerker ten behoeve van de verantwoordelijke voor de verwerking heeft voornamelijk betrekking op (de aard van de verwerking):

- Opslaan/ hosting
- Wijzigen/ bewerken/ wissen
- Rapporteren

A.6 Duur van de Verwerking

De duur van de verwerking van persoonsgegevens is gelijk aan looptijd van de Dienstenovereenkomst, inclusief de termijn voor de definitieve afwikkeling en verwijdering van de data.

elari

Appendix B - Subverwerkers

Subverwerker	Beschrijving dienst en Persoonsgegevens	Gegevens buiten de EER	Verwerkers-overeenkomst
Google Cloud EMEA Ltd 70 Sir John Rogerson's Quay, Dublin 2 Ierland	Hosting provider.	Nee	Ja
Adyen N.V. Simon Carmiggeltstraat 6-50, 1011 DJ, Amsterdam Nederland	Bankrekening en betaalkaarten leverancier voor de Kas & Pas module.	Nee	Ja
84codes A.B. Torsgatan 26, 113 21 Stockholm Zweden	Message broker voor het e-mail systeem.	Nee	Ja
Orca Security Ltd 3 Tushia St., Tel Aviv Israël	Vulnerability scanning van cloud infrastructuur.	Nee	Ja
Functional Software GmbH Rothschildplatz 3, Top 3.02.AB 1020 Vienna, Austria	Beheer van error logs.	Nee	Ja
ChurnZero, Inc. 717 D St NW 2nd floor, Washington, DC 20004, USA	Integrated analytics.	Nee	Ja
Visma Software International AS Karenslyst allé 56 0277 Oslo Norway	Moederbedrijf van Elari. Leverancier van cloud infrastructuur en het authenticatieplatform	Nee	Ja
Visma Machine Learning Gærtorvet 1-5 1799 Copenhagen Denmark	Leverancier Smart scan technologie t.b.v. OCR.	Nee	Ja

elari

Appendix C - Beveiligingsmaatregelen

Elari werkt continu aan beveiliging. Hiervoor worden een groot aantal organisatorische en technische maatregelen genomen waaronder, maar niet beperkt tot:

Organisatorische Maatregelen:

- Beleid en Verantwoordelijkheden:
    - Een informatie- en beveiligingsbeleid is opgesteld, wordt regelmatig gecontroleerd en bijgewerkt. Dit beleid beschrijft hoe Elari en haar medewerkers omgaan met klantgegevens en de IT-infrastructuur.
    - Elari heeft een Security Officer aangesteld om het informatie- en beveiligingsbeleid te onderhouden, te promoten en af te dwingen.
    - Alle medewerkers van Elari hebben getekend om het informatie- en beveiligingsbeleid te lezen en na te leven.
    - De gegevens van klanten worden als vertrouwelijk beschouwd en moeten dienovereenkomstig worden behandeld.
    - Informatiebeveiligingsverantwoordelijkheden zijn gedefinieerd en toegewezen.
- Awareness en Training:
    - Regelmatige verplichte sessies worden georganiseerd om het beveiligingsbewustzijn van het Elari-personeel te vergroten.
    - Visma organiseert een jaarlijks beveiligingsbewustzijnsprogramma voor haar medewerkers om actuele kennis over privacy, beveiliging en de huidige IT-risico's en uitdagingen te waarborgen.
- Supplier Relationship Management:
    - Elari heeft formele verwerkingsovereenkomsten met leveranciers die persoonsgegevens verwerken.
    - Deze leveranciers worden jaarlijks beoordeeld op basis van de door hen beschikbaar gestelde informatie.
    - Relevante informatiebeveiligingsvereisten worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot, gegevens verwerkt, opslaat, communiceert, of IT-infrastructuurcomponenten levert voor de informatie van de organisatie.
    - De Security Officer beoordeelt periodiek de prestaties van IT-leveranciers door middel van tooling en assurance-rapporten van derden.
- Incident Management:
    - Beveiligingsincidenten moeten worden gemeld aan de security officer (security@Elari.nl).
    - Deze incidenten worden binnen 24 uur beoordeeld en passende actie wordt ondernomen door de security officer.
    - Informatiebeveiligingsincidenten worden geregistreerd, gemonitord en opgevolgd volgens de procedure voor beveiligingsincidenten.
    - Een beleid voor het melden van datalekken is beschreven en geïmplementeerd, met procedures voor het melden van datalekken.
- Compliance:
    - Bij niet-naleving van gedrag door medewerkers of leveranciers kunnen disciplinaire maatregelen worden genomen.
    - Naleving van beveiligingsbeleid is een continue inspanning.
    - De beveiligingsfunctionaris beoordeelt jaarlijks de classificatie van verwerkte gegevens en de encryptiestandaarden.

Technische Maatregelen:

- Beveiliging van de IT-infrastructuur:
    - De software wordt in-house ontwikkeld en gehost op Google Cloud Platform.
    - Procedures zijn aanwezig om leveranciers geleverde (beveiligings)patches tijdig op de IT-infrastructuur te installeren.
    - Elari test de IT-infrastructuur op kwetsbaarheden.
    - Elari neemt deel aan het Visma Application Security Program (VASP), dat bestaat uit maatregelen zoals Security Self-Assessment (SSA), Dynamic Application Security Test (DAST), Automated Third-party Vulnerability Service (ATVS), Static Application Security Test (SAST), Software Composition Analysis (SCA) en Manual Application Vulnerability Assessment (MAVA).
    - Voor hun omgeving op Google Cloud Platform worden Google's datacenters in Eemshaven, Nederland, gebruikt. Andere Google datacenters in de EU kunnen worden gebruikt voor back-upopslag.
    - Besturingsprocedures zijn gedocumenteerd en beschikbaar gesteld aan alle gebruikers die ze nodig hebben.
    - Monitoring van Google informatieverwerkingsbronnen wordt uitgevoerd door leden van het infrastructuurteam via geconfigureerde triggers en waarschuwingen.
    - Detectie-, preventie- en herstelcontroles ter bescherming tegen kwetsbaarheden zijn geïmplementeerd. Patches worden volgens beleid geïmplementeerd.
- Encryptie:
    - Alle gegevens die als gevoelig zijn geclassificeerd, worden zowel 'at rest' als 'in transit' versleuteld.
- Toegangsbeheer:
    - Elari heeft toegangscontroleprocedures opgesteld voor zowel fysieke als digitale omgevingen.
    - Medewerkers krijgen beperkte toegang tot de digitale omgeving van Elari, afhankelijk van hun functie.
    - Medewerkers zijn verplicht om sterke wachtwoorden en 2FA te gebruiken volgens het wachtwoordbeleid van Visma.
    - Toegang tot serversystemen wordt verleend via Privileged User-accounts, die tijdelijk met extra rechten kunnen worden verhoogd.
    - De toegangscontroleprocedures worden ten minste elke 6 maanden gecontroleerd en beoordeeld.
    - Een formeel proces voor het toekennen van gebruikerstoegang is geïmplementeerd om toegangsrechten voor alle gebruikerstypen tot alle systemen en services toe te wijzen of in te trekken.
    - De toewijzing en het gebruik van geprivilegieerde toegangsrechten zijn beperkt en goedgekeurd door de Security Officer.
    - De Security Officer beoordeelt de toegangsrechten van gebruikers en geprivilegieerde toegangsrechten elke zes maanden.
    - Toegang tot productiedatabases is beperkt en gecontroleerd. Alleen geautoriseerde gebruikers kunnen toegang tot productiedatabases aanvragen, wat wordt gelogd en slechts voor een beperkte tijd wordt verleend.
    - Toegang tot de broncode-repository van Elari is beperkt tot geautoriseerde gebruikers.
- Monitoring en Logging:
    - Alle systemen van Elari worden, zowel handmatig als automatisch, gemonitord op prestatievermindering, ongeautoriseerde toegang en ander onregelmatig gedrag.
    - Alle systemen loggen toegang, gebruik en algemene systeeminformatie. Het IT-personeel beoordeelt deze logs.
    - Alle werkstations van medewerkers zijn uitgerust met centraal gecontroleerde antivirus- en antimalwaresoftware. Deze software wordt automatisch up-to-date gehouden. Alle gedetecteerde virussen en andere onregelmatigheden worden via een centrale interface gerapporteerd.
    - Waarschuwingen van gebeurtenislogboeken met betrekking tot uitzonderingen worden gemonitord door DevOps-engineers en de Security Officer.
    - Logboeken en loginformatie worden beschermd tegen manipulatie en ongeautoriseerde toegang.

- Wijzigings- en Releasemanagement:
    - Elari gebruikt de agile methoden Scrum en Kanban.
    - Softwarewijzigingen vereisen het 'vierogenprincipe'.
    - Alle wijzigingen worden gedocumenteerd in de releasenotes.
    - Tickets worden ontwikkeld en getest tijdens de sprint.
    - Elari geeft de voorkeur aan automatische testprocedures en testers maken op maat gemaakte automatische testsuites.
    - Nadat een nieuwe release alle testsuites in de testomgeving heeft doorlopen, wordt deze vrijgegeven in de productieomgeving. Dit proces is volledig geautomatiseerd.
    - Een procedure voor wijzigings- en releasemanagement voor de ontwikkeling van de Elari webapplicatie is beschreven.
    - Regels voor de ontwikkeling van software en systemen zijn vastgesteld en toegepast.
    - Wijzigingen worden geregistreerd en gemonitord via een ticketsysteem.
    - Peer-to-peer codereviews worden uitgevoerd voor elke codecommit.
    - Wijzigingen worden getest voordat ze naar de live-omgeving worden geïmplementeerd.
    - Controles zijn aanwezig om ongeautoriseerde implementatie van code naar de live-omgeving te voorkomen. De ontwikkelings- en release-pipeline moet worden gevolgd en kan niet worden afgeweken.
    - Ontwikkel-, test- en live-omgevingen zijn gescheiden om de risico's van ongeautoriseerde toegang of wijzigingen aan de live-omgeving te verminderen.
- Netwerkbeveiliging:
    - Netwerktoegang en -segmentatie zijn geregeld door firewalls. Beheerderstoegang tot de firewalls is beperkt tot geautoriseerde medewerkers.
    - Netwerkverkeermonitoring van het internet naar de Elari webapplicatie wordt continu uitgevoerd.
    - Kwetsbaarheidsscans worden dagelijks uitgevoerd en gevonden kwetsbaarheden worden verholpen via het incidentmanagementproces.
    - Penetratietesten worden frequent uitgevoerd en gevonden kwetsbaarheden worden verholpen via het incidentmanagementproces.
    - Toegang tot de back-end van de Elari webapplicatie en toegang tot bedrijfskritische apps wordt beschermd door versleutelde communicatie en beveiligd met gebruikersnaam, wachtwoord en multifactor-authenticatiemethoden.
    - Draadloze netwerken op de kantoorlocatie zijn wachtwoordbeveiligd met WPA-encryptie.
    - Toegang tot bedrijfskritische apps en informatiesystemen die gevoelige gegevens bevatten, wordt verleend op basis van 'need-to-know'.
    - Communicatie met de Elari webapplicatie is versleuteld volgens de nieuwste veilige TLS-standaarden.