Verwerkersovereenkomst

Versie: 28 september 2026

elari

elari

Verwerkersovereenkomst

Versie: 28 september 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, bepaalde per datum ondertekening van de Mantelovereenkomst 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 schetst hoe de Verwerker zal bijdragen aan het waarborgen van de privacy namens de Verwerkingsverantwoordelijke en zijn geregistreerde Betrokkenen, door middel van technische en organisatorische maatregelen in overeenstemming met 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. Deze Overeenkomst is geldig voor de duur zoals overeengekomen in Appendix A.

Artikel 4 Rechten en plichten van de Verwerker

4.1. De Verwerker zal Persoonsgegevens slechts 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) om te voldoen aan alle verplichtingen volgens 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

daarvan op de hoogte is, 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 zal de vertrouwelijkheid, integriteit en beschikbaarheid van Persoonsgegevens waarborgen overeenkomstig de op de Verwerker van toepassing zijnde privacywetgeving. De Verwerker zal systematische, organisatorische en technische 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 de Verwerkingsverantwoordelijke met passende technische en organisatorische maatregelen bijstaan, voor zover mogelijk en rekening houdend met de aard van de Verwerking en de informatie waarover de Verwerker beschikt, bij het nakomen van de verplichtingen van de Verwerkingsverantwoordelijke op grond van de toepasselijke privacywetgeving met betrekking tot het verzoek van Betrokkenen, en de algemene naleving van de privacywetgeving op grond van de AVG artikel 32 t/m 36.

4.6. Indien de Verwerkingsverantwoordelijke informatie of bijstand nodig heeft 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 verstrekt om als Verwerker te voldoen aan de toepasselijke privacywetgeving, kan de Verwerker de Verwerkingsverantwoordelijke voor dit verzoek om aanvullende diensten redelijke kosten in rekening brengen.

4.7. De Verwerker en zijn personeel dragen zorg voor geheimhouding met betrekking tot de Persoonsgegevens die onderwerp zijn van Verwerking in overeenstemming met de Overeenkomst. Deze bepaling is ook van toepassing na beëindiging van de Overeenkomst.

4.8. De Verwerker zal, door de Verwerkingsverantwoordelijke binnen 48 uur in kennis te stellen, de Verwerkingsverantwoordelijke in staat stellen te voldoen aan de wettelijke vereisten inzake kennisgeving aan Autoriteit Persoonsgegevens of Betrokkenen over privacy-incidenten. De Verwerker verstrekt waar van toepassing en noodzakelijk aan de Verwerkingsverantwoordelijke:

- 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.

elari

Voorts zal de Verwerker, voor zover dit passend en rechtmatig is, de Verwerkingsverantwoordelijke in kennis stellen van;

I. van een Betrokkene ontvangen verzoeken om verstrekking van Persoonsgegevens,
II. verzoeken tot openbaarmaking van Persoonsgegevens door overheidsinstanties, zoals maar niet beperkt tot, de politie.

4.9. De Verwerker zal niet rechtstreeks reageren op verzoeken van Betrokkenen, tenzij hij daartoe schriftelijk is gemachtigd door de Verwerkingsverantwoordelijke. De Verwerker zal geen aan deze Overeenkomst verbonden informatie verstrekken aan overheidsinstanties, zoals de politie, waaronder Persoonsgegevens, tenzij daartoe verplicht door de wet, zoals via een gerechtelijk bevel of een soortgelijk bevel.

4.10. De Verwerker heeft geen zeggenschap of en hoe de Verwerkingsverantwoordelijke gebruik maakt van integraties van derden via de API (of vergelijkbaar) van de Verwerker, en de Verwerker aanvaardt in dat verband dus geen aansprakelijkheid. De Verwerkingsverantwoordelijke is als enige verantwoordelijk voor integraties van derden.

4.11. De Verwerker kan Persoonsgegevens over gebruikers en het gebruik van de dienst door de Verwerkingsverantwoordelijke verwerken wanneer dit noodzakelijk is om feedback te verkrijgen en de dienst te verbeteren. De Verwerkingsverantwoordelijke verleent de Verwerker het recht om geaggregeerde gegevens over systeemactiviteiten in verband met uw gebruik van de Diensten te gebruiken en te analyseren met het oog op optimalisering, verbetering of uitbreiden van de wijze waarop wij onze Diensten verlenen en om ons in staat te stellen nieuwe functies en functionaliteit in verband met de Diensten te creëren. Elari wordt beschouwd als de verwerkingsverantwoordelijke voor dergelijke verwerking en de verwerking is derhalve niet onderworpen aan deze Overeenkomst. Dit betreft de volgende groepen gegevens:

Groep	**Grondslag**	**Bewaartermijn**
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
Verwerkingstijd	Gerechtvaardigd belang *Gepseudonimiseerde registratie van verwerkingstijd t.b.v. productverbetering en optimalisatie klant.*	2 jaar

4.12. Bij het gebruik van de dienst zal de Verwerkingsverantwoordelijke gegevens toevoegen aan de Software ("Klantgegevens"). De Verwerkingsverantwoordelijke erkent en heeft er geen bezwaar tegen dat de Verwerker de Klantgegevens in een geaggregeerd en geanonimiseerd formaat gebruikt voor het verbeteren van de aan klanten geleverde diensten, onderzoek, opleiding, educatieve en/of statistische doeleinden.

Artikel 5 Rechten en plichten van Verwerkingsverantwoordelijke

5.1 De Verwerkingsverantwoordelijke bevestigt door de ondertekening van deze Overeenkomst dat:

- zij wettelijk bevoegd is tot het Verwerken en bekendmaken van de Persoonsgegevens in kwestie aan Verwerker (met inbegrip van door Verwerker ingeschakelde subverwerkers).
- zij verantwoordelijkheid draagt voor de accuraatheid, integriteit, inhoud, betrouwbaarheid en rechtmatigheid van de Verwerkte Persoonsgegevens zoals bekendgemaakt aan Verwerker.
- zij heeft voldaan aan haar verplichtingen om relevante informatie te verstrekken aan Betrokkenen en toezichthoudende autoriteiten omtrent de Verwerkingen van Persoonsgegevens conform dwingend gegevensbeschermingswetgeving.
- zij zal, bij het ontvangen en gebruik van de diensten van Verwerker onder de Dienstenovereenkomsten, geen Gevoelige Gegevens aan Verwerker 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 het leveren van diensten aan Verwerkingsverantwoordelijke conform de Dienstenovereenkomsten en deze Overeenkomst, zal Verwerker derden (subverwerkers) inschakelen bij de uitvoering van deze Overeenkomst en Verwerkingsverantwoordelijke geeft algemene toestemming voor het mogen inschakelen van voornoemde subverwerkers door Verwerker. Deze subverwerkers kunnen bedrijven binnen de Visma groep zijn of externe derde partijen. Verwerker ziet erop toe dat subverwerkers akkoord gaan met het accepteren van de verantwoordelijkheden en daarmee corresponderende verplichtingen zoals neergelegd in deze Overeenkomst.

6.2. Een 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/spend-cloud.

6.3. Indien de subverwerkers buiten de EU of de EER zijn gevestigd, machtigt Verwerkingsverantwoordelijke Verwerker om namens Verwerkingsverantwoordelijke voor de doorgifte van persoonsgegevens buiten de EU/EER te zorgen voor passende rechtsgronden door het aangaan van EU-Standard Contractual Clauses (SCC's).

6.4. De Verwerkingsverantwoordelijke wordt vooraf in kennis gesteld van elke wijziging van subverwerkers die Persoonsgegevens verwerken. Indien de Verwerkingsverantwoordelijke bezwaar maakt tegen een nieuwe subverwerker binnen 30 dagen na de kennisgeving, beoordelen de Verwerker en de Verwerkingsverantwoordelijke de documentatie over de beveiligingsmaatregelen van de subverwerker, teneinde de naleving van de toepasselijke privacywetgeving te waarborgen. Indien de Verwerkingsverantwoordelijke blijvend bezwaren heeft en daarvoor redelijke gronden heeft, kan de Verwerkingsverantwoordelijke zich niet tegen het gebruik van een dergelijke subverwerker verzetten (met

name gezien de aard van online standaardsoftware), maar kan de Verwerkingsverantwoordelijke de Dienstenovereenkomst tegen de datum dat de nieuwe subverwerker wordt ingeschakeld opzeggen.

Artikel 7 Beveiliging

7.1. De Verwerker verbindt zich ertoe een hoog niveau van beveiliging te bieden in zijn producten en diensten. De Verwerker voorziet in zijn beveiligingsniveau door middel van organisatorische, technische en fysieke beveiligingsmaatregelen, overeenkomstig de vereisten inzake informatiebeveiligingsmaatregelen zoals uiteengezet in de AVG, artikel 32.

7.2. In de Dienstenovereenkomsten worden de maatregelen of andere beveiligingsmaatregelen vermeld die de Verwerker bij de verwerking van de Persoonsgegevens toepast. De Verwerkingsverantwoordelijke is verantwoordelijk voor de passende en adequate beveiliging van de apparatuur en de IT-omgeving die onder zijn verantwoordelijkheid valt.

Artikel 8 Inspectie rechten

8.1. De Verwerkingsverantwoordelijke kan maximaal eenmaal per jaar controleren of de Verwerker zich aan deze Overeenkomst houdt. Indien de op de Verwerkingsverantwoordelijke van toepassing zijnde wetgeving zulks vereist, kan de Verwerkingsverantwoordelijke om frequentere audits verzoeken. Om een audit aan te vragen, dient de Verwerkingsverantwoordelijke de Verwerker ten minste vier weken voor de voorgestelde auditdatum een gedetailleerd auditplan voor te leggen, met een beschrijving van de voorgestelde omvang, duur en aanvangsdatum van de audit. Indien een derde partij de audit moet uitvoeren, moet dit onderling tussen de partijen schriftelijk worden overeengekomen. Indien de verwerkingsomgeving echter een "multitenant"-omgeving of een soortgelijke omgeving is, geeft de verantwoordelijke voor de verwerking de Verwerker de bevoegdheid om om veiligheidsredenen te besluiten dat de audits worden uitgevoerd door een neutrale derde-auditor naar keuze van de Verwerker.

8.2. Indien de gevraagde reikwijdte van de audit wordt behandeld in een ISAE-, ISO- of vergelijkbaar assurance-rapport dat binnen de voorafgaande twaalf maanden door een gekwalificeerde derde auditor is uitgevoerd, en de Verwerker bevestigt dat er geen bekende materiële wijzigingen zijn in de gecontroleerde maatregelen, stemt Verwerkingsverantwoordelijke ermee in die bevindingen te aanvaarden in plaats van een nieuwe audit aan te vragen van de maatregelen waarop het rapport betrekking heeft.

8.3. In elk geval moeten de audits worden uitgevoerd tijdens de gewone kantooruren in de desbetreffende vestiging, met inachtneming van het beleid van de verwerker, en mogen zij de bedrijfsactiviteiten van de verwerker niet op onredelijke wijze hinderen.

8.4. Verwerkingsverantwoordelijke is verantwoordelijk voor alle kosten die voortvloeien uit de door de Verwerkingsverantwoordelijke gevraagde controles. Voor verzoeken om bijstand van de Verwerker kunnen kosten in rekening worden gebracht.

Artikel 9 Duur en beëindiging

9.1. 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.

elari

9.2. Deze Overeenkomst wordt automatisch beëindigd bij beëindiging van de Dienstenovereenkomsten. Bij beëindiging 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, plaatsvinden. De Verwerker heeft geen plicht om te onderzoeken of aan te nemen dat er gronden zijn om de Persoonsgegevens langer dan deze termijn 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 10 Wijzigingen en amendementen

10.1. Wijzigingen aan de Overeenkomst zullen in een nieuwe Appendix bij deze Overeenkomst worden opgenomen en treden in werking nadat beide Partijen deze hebben ondertekend.

10.2. Indien enige bepaling van deze overeenkomst nietig is, laat zulks de overige bepalingen onverlet. De partijen zullen de nietige bepaling vervangen door een rechtmatige bepaling die het doel van de nietige bepaling weergeeft.

Artikel 11 Aansprakelijkheid

11.1. Ter voorkoming van misverstanden, Partijen komen hierbij overeen en erkennen dat iedere Partij aansprakelijk zal zijn en verantwoordelijk is voor de betaling van administratieve boetes en schadevergoedingen aan Betrokkenen indien deze betalingsplicht aan deze Partij is opgelegd door de relevante autoriteit persoonsgegevens of een bevoegde rechtbank in overeenstemming met toepasselijke wetgeving. Aansprakelijkheidskwesties tussen de Partijen zullen worden beheerst door de relevante bepalingen aangaande aansprakelijkheid zoals overeengekomen in de Dienstenovereenkomst.

elari

Artikel 12 Toepasselijk recht en forumkeuze

12.1. 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 is opgemaakt in tweevoud, waarbij partijen ieder één kopie behouden.

Gegevens Verwerkingsverantwoordelijke:	
Handtekening:	
Door:	
Plaats en datum:	

Gegevens Verwerker:	
Handtekening:	
Door:	
Plaats en datum:	

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 de Spend Cloud.

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

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 de Spend Cloud). 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 zolang de Dienstenovereenkomst van toepassing is.

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	De Spend Cloud wordt in de cloud gehost, de software is gebonden aan de diensten van de service provider.	Nee	Ja
Adyen N.V. Simon Carmiggeltstraat 6-50, 1011 DJ, Amsterdam Nederland	Adyen is de leverancier waar een bankrekening en betaalkaarten in de Kas & Pas module in de Spend Cloud.	Nee	Ja
84codes A.B. Torsgatan 26, 113 21 Stockholm Zweden	Message broker for Spend Cloud mail system	Nee	Ja
Orca Security Ltd 3 Tushia St., Tel Aviv Israel	Vulnerability scanning of cloud infrastructure.	Nee	Ja
Functional Software GmbH Rothschildplatz 3, Top 3.02.AB 1020 Vienna, Austria	Error log beheer.	Nee	Ja
ChurnZero, Inc. 717 D St NW 2nd floor, Washington, DC 20004, USA	Integrated analytics tool for users	Nee	Ja
Visma Software International AS Karenslyst allé 56 0277 Oslo Norway	Moederbedrijf van Visma 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 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 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.

elari

- Wijzigings- en Releasemanagement:
    - Elari gebruikt de agile ontwikkelingsproductiemanagementmethoden 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 Spend Cloud 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 Spend Cloud 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.