



Data Processing Agreement

Maatwerk & Consultancy (GCP europe-west4)

Documenttype	Data Processing Agreement
Document nummer	CUSTOM-WORK-DPA-2025-001
Datum	02-02-2026
Versie	1.1
Geldig tot	Looptijd hoofdovereenkomst
Contactpersoon	Mario Beck (Prometheon™)
Bedrijf	Prometheon™ B.V. i.o.

1. Partijen

1.1. Verwerkingsverantwoordelijke

Organisatie	[Naam Klant]
Rol	Verwerkingsverantwoordelijke (Art. 4(7) AVG)
Adres	[Adres Klant]
KvK/BTW	[KvK] / [BTW]
Contactpersoon	[Naam + functie + e-mail]

1.2. Verwerker

Organisatie	Prometheon™ B.V. i.o.
Rol	Verwerker (Art. 4(8) AVG)
Status	B.V. in oprichting; bekrachtiging binnen 60 dagen na inschrijving
Adres	n.t.b., Nederland
KvK/BTW	n.t.b. (B.V. in oprichting) / n.t.b. (wordt vermeld op factuur)
Contactpersoon	Mario Beck (Prometheon™)
E-mail	privacy@prometheon.ai

Context

Deze DPA is van toepassing op alle consultancy-, strategie-, workshop- en maatwerktrajecten waarbij Prometheon persoonsgegevens van Klant en diens cliënten verwerkt. Verwerking vindt plaats in beveiligde projectomgevingen binnen Google Cloud Platform (GCP) regio europe-west4 (Eemshaven, Nederland) en eventueel on-site bij Klant.

2. Definities

Projectdata	Combinatie van Klantdata, analysebestanden, annotaties, AI-artefacten en deliverables die tijdens een project worden aangemaakt.
Subverwerker	Derde partij die in opdracht van Prometheon persoonsgegevens verwerkt.
GCP europe-west4	Google Cloud Platform regio Eemshaven (NL) met zones europe-west4-a/-b/-c. Alle online verwerking vindt hier plaats.
On-site verwerking	Verwerking die plaatsvindt bij Klant op locatie of via door Klant beschikbaar gestelde systemen.
Supportwindow	Periode van maximaal 90 dagen na oplevering waarin Prometheon projectdata beschikbaar houdt voor nazorg/iteraties.

3. Onderwerp, Duur en Relatie

3.1. Doel

3.1. Prometheon verwerkt persoonsgegevens uitsluitend ten behoeve van Klant en conform diens schriftelijke instructies voor:

- Analyse t.b.v. AI Strategy Reports en business cases.
- Voorbereiding en uitvoering van workshops en trainingen.
- Ontwikkeling, testen en implementatie van maatwerkoplossingen.
- Documentatie, QA en hypercare.

3.2. Looptijd

3.2. Deze DPA geldt zolang Prometheon persoonsgegevens verwerkt voor Klant. Na beëindiging gelden de verwijdertermijnen uit Artikel 10.

3.3. Rollen

3.3. Klant is verwerkingsverantwoordelijke. Prometheon is verwerker. Wanneer Prometheon subverwerkers inschakelt, blijft Prometheon verantwoordelijk voor hun handelen.

4. Aard van de Verwerking

4.1. Categorieën Persoonsgegevens

- Persoons- en contactgegevens van medewerkers van Klant.
- Cliëntgegevens van Klant (NAW, contractinformatie, dossierinhoud).
- Juridische en financiële documenten (contracten, memo's, redlines).
- HR- of compliance-documenten (indien onderdeel van use case).
- Workshopregistraties en evaluaties.
- Opnames of transcripten van interviews (alleen met toestemming).

4.2. Betrokkenen

- Werknemers en bestuurders van Klant.
- Klanten, cliënten en andere relaties van Klant.
- Derden (advocaten, leveranciers) die in documentatie voorkomen.

4.3. Verwerkingen

- Opslag/versleuteling van documenten in GCP-projecten.
- Annotatie, tagging en modellering van data.
- Analyse en rapportage.
- Beheer van taken, backlog, roadmap-items.
- Trainingen (deelnemerslijsten, aanwezigheid, feedback).

5. Verplichtingen van Prometheon

5.1. Prometheon verwerkt persoonsgegevens uitsluitend op gedocumenteerde instructies van Klant. Afwijkingen (bijv. hergebruik voor demonstraties) vereisen expliciete schriftelijke toestemming.

5.2. Prometheon waarborgt vertrouwelijkheid via NDA's, rolgebaseerde toegang en "need-to-know" principes. Hardware wordt versleuteld (FDE) en MFA is verplicht.

5.3. Technische maatregelen:

- Projectomgevingen in GCP europe-west4; dedicated per klant of project, logisch gescheiden.
- Encryptie at rest (AES-256) en in transit (TLS 1.3); optioneel CMEK.
- IAM policies met tijdelijke toegang; geen gedeelde accounts.
- Back-ups binnen dezelfde regio; geen export buiten EU.
- Device management: full disk encryption, automatische lock, remote wipe.

5.4. Organisatorische maatregelen:

- Privacy & security awareness programma.
- Logging van toegang, wijziging en export.
- Jaarlijkse pentest/assurance; resultaten op aanvraag.
- Background checks voor vaste medewerkers; freelancers tekenen NDA.

5.5. Assistentie bij privacyrechten (Art. 12-23 AVG) en DPIA's is beschikbaar op basis van consultancytarief.

6. On-site Verwerking

6.1. Wanneer Prometheon op locatie bij Klant werkt, gelden aanvullende spelregels:

- Gebruik bij voorkeur apparatuur en accounts van Klant. Indien eigen laptops gebruikt worden, gebeurt verwerking uitsluitend via versleutelde containers of VDI.
- Geen documenten worden lokaal opgeslagen buiten GCP of door Klant goedgekeurde systemen.
- Fysieke documenten worden niet buiten locatie meegenomen zonder toestemming; vernietiging volgens afspraken.

6.2. Klant faciliteert veilige werkplekken, netwerktoegang en begeleidt bezoekers conform interne policies.

7. Onderverwerkers

7.1. Toestemming

7.1. Klant verleent algemene toestemming voor de onderverwerkers in onderstaande tabel.

Wijzigingen worden minimaal 30 dagen vooraf aangekondigd; Klant kan bezwaar maken.

7.2. Huidige onderverwerkers

Onderverwerker	Dienst	Locatie
Google Cloud Platform (Google Ireland Ltd.)	Hosting van projectomgevingen, opslag, AI tooling.	europa-west4 (Eemshaven, NL)
Google Workspace (Google Ireland Ltd.)	E-mail, Drive, Meet (EU data residency ingeschakeld).	EU datacenters
Atlassian (EU)	Projecttracking en ticketing (Jira/Confluence).	EU (Dublin/Frankfurt)
Miro EU	Workshop whiteboards; data blijft binnen EU cluster.	EU (Frankfurt)
Notion EU data region	Documentatie; alleen metadata, geen vertrouwelijke dossiers.	EU (Dublin)

8. Internationale Doorgifte

8.1. Prometheon verwerkt persoonsgegevens uitsluitend binnen de EU/EER. Voor digitale opslag geldt: GCP europe-west4 is primair; replicatie binnen EU-regio's (bijv. europe-west1) kan voorkomen voor disaster recovery, maar nooit buiten de EU.

8.2. Alleen indien Klant dat expliciet verzoekt (bijv. voor samenwerking met niet-EU advocaten) vindt doorgifte naar derde landen plaats. In dat geval gebruikt Prometheon SCC's en aanvullende maatregelen (pseudonimisering, encryptie, access controls).

9. Meldingsplicht en Incidentrespons

9.1. Prometheon meldt een inbreuk op persoonsgegevens zonder onnodige vertraging, uiterlijk binnen 24 uur na ontdekking, met alle relevante informatie voor een melding aan de toezichthouder (Art. 33 AVG).

9.2. Prometheon treft onmiddellijk maatregelen om de impact te beperken en verstrekt een follow-up rapport met root cause en preventieve acties.

9.3. Klant is verantwoordelijk voor melding aan Autoriteit Persoonsgegevens en betrokkenen; Prometheon ondersteunt waar redelijk.

10. Audits

10.1. Klant mag audits uitvoeren met een waarschuwing van 30 dagen (tenzij er een incident is).

Audits kunnen bestaan uit documentreviews, interviews en (indien noodzakelijk) locatiebezoeken.

10.2. Prometheon mag aantonen dat zij voldoet via externe rapporten (ISO 27001 roadmap, SOC 2-in-progress, pentestresultaten). Wanneer deze rapporten toereikend zijn, is een aanvullende audit niet noodzakelijk.

10.3. Kosten van audits komen voor rekening van Klant, tenzij een wezenlijke tekortkoming wordt geconstateerd.

11. Bewaartermijnen en Verwijdering

11.1. Projectdata wordt 90 dagen na oplevering verwijderd (standaard). Klant kan:

- onmiddellijke verwijdering verzoeken (binnen 10 werkdagen),
- langere retentie afspreken (tegen aanvullende beveiliging/prijs).

11.2. Back-ups worden na 120 dagen automatisch overschreven. Auditlogs met persoonsgegevens worden 12 maanden bewaard (instelbaar 6-24 maanden).

11.3. Klant ontvangt op verzoek een verwijderlog of certificaat.

12. Aansprakelijkheid

12.1. Aansprakelijkheid van Prometheon onder deze DPA volgt de limieten van de hoofdovereenkomst (standaard €100.000 per contractjaar). Deze beperking geldt niet bij opzet of bewuste roekeloosheid.

12.2. Prometheon is niet aansprakelijk voor boetes of claims die voortkomen uit instructies of nalatigheid van Klant (bijv. wanneer Klant onrechtmatige data aanlevert).

13. Toepasselijk Recht

13.1. Nederlands recht is van toepassing; geschillen worden voorgelegd aan de bevoegde rechter te Amsterdam, nadat partijen overleg of mediation hebben geprobeerd.

14. Normenkader & Referenties

Norm / Richtlijn

AVG/GDPR (EU) 2016/679

EDPB Guidelines for Controllers &
Processors

ISO/IEC 27001:2022 & 27701:2019

ISO/IEC 27017:2021 (Cloud
Security)Autoriteit Persoonsgegevens –
Beveiligingsrichtsnoeren**Bron**<https://eur-lex.europa.eu/eli/reg/2016/679/oj>https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_en<https://www.iso.org/isoiec-27701-information-security.html><https://www.iso.org/standard/43757.html><https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/beveiliging-van-persoonsgegevens>

15. Contact en Escalatie

Klant DPO / privacy contact

[Naam / e-mail / telefoon]

Prometheon DPO

Mario Beck (Interim DPO)

e: privacy@prometheon.ai

t: +31 (0)6 161 661 05

Security Hotline (24/7)

security@prometheon.ai • +31 (0)6 161 661 05 (Signal/WhatsApp beschikbaar)

16. Ondertekening

Deze DPA treedt in werking op de datum van de laatste handtekening en vormt samen met de hoofdovereenkomst en NDA één geheel. Door te ondertekenen bevestigen partijen dat zij wettelijke verplichtingen onder de AVG zullen naleven.

Verwerkingsverantwoordelijke

[Naam Klant]

Naam:

Functie:

Datum:

Handtekening:

line(length: 100%)

Verwerker

Prometheon™ B.V. i.o.

Naam: Mario Beck

Functie: Oprichter (B.V. i.o.)

Datum:

Handtekening:

line(length: 100%)

The logo for Prometheon, featuring the word "prometheon" in a lowercase, sans-serif font. The letter 'p' is stylized with a circular element around it.

CUSTOM-WORK-DPA-2025-001 • v1.1 • 02-02-2026 • Hosting: GCP europe-west4 (Eemshaven, NL)