Data Pro Statement — Crimson Owl Technologies B.V.

Crimson Owl Technologies B.V. · Versie 1.1 · Geldig vanaf 16 oktober 2026

Dit Data Pro Statement is **Deel 1** van de verwerkersovereenkomst. **Deel 2** zijn de Standaardclausules voor verwerkingen van NLdigital, versie maart 2025. Beide delen worden samen verstrekt; de verwerkersovereenkomst is niet compleet als één van beide ontbreekt.

Dit Data Pro Statement vormt samen met de Standaardclausules voor verwerkingen de verwerkersovereenkomst voor het product of de dienst van het bedrijf dat dit Data Pro Statement heeft opgesteld.

Algemene informatie

1. Dit Data Pro Statement is opgesteld door de volgende data processor (verwerker):

Crimson Owl Technologies B.V.
Bredestraat-Zuid 33, 6674 LA Herveld, Nederland
KvK 99457377 · BTW NL869000172B01

Voor vragen over dit Data Pro Statement of dataprotectie kan contact opgenomen worden met: Marc Dekeyser, marc.dekeyser@crimsonowl.nl, +31 6 10 10 24 44.

Crimson Owl Technologies B.V. heeft geen functionaris voor de gegevensbescherming aangesteld; de AVG verplicht daar in dit geval niet toe. De bevoegde toezichthouder is de Autoriteit Persoonsgegevens (Nederland).

2. Dit Data Pro Statement geldt vanaf 16 oktober 2026, versie 1.1.

Dit Data Pro Statement en de daarin omschreven beveiligingsmaatregelen passen wij regelmatig aan om ten aanzien van dataprotectie steeds voorbereid en actueel te blijven. Nieuwe versies worden gepubliceerd op trust.crimsonowl.eu en aangekondigd aan de contractcontactpersoon van opdrachtgever; vragen kunnen naar privacy@crimsonowl.eu. Bij een significante aanpassing van dit statement mag opdrachtgever de verwerkersovereenkomst binnen 30 dagen na kennisgeving schriftelijk en gemotiveerd opzeggen, overeenkomstig artikel 2.2 van de Standaardclausules.

3. Dit Data Pro Statement is van toepassing op de volgende producten en diensten van data processor:

- **Platform Architecture Authority (PAA)**, in al zijn afnamevormen, waaronder de Platform Foundation Review.
- **Advies- en consultancyopdrachten**, waaronder Fractional Architect, voor zover daarbij persoonsgegevens van opdrachtgever in de eigen omgeving van data processor terechtkomen.

In de Overeenkomst is bepaald welke producten en diensten opdrachtgever afneemt. Waar een punt of onderdeel alleen voor PAA of alleen voor advies- en consultancyopdrachten geldt, is dat aangegeven.

Omschrijving product/dienst en beoogd gebruik

4. Omschrijving product(en)/dienst(en)

PAA beoordeelt geautomatiseerd de configuratie van de Microsoft Azure- en Microsoft 365 / Entra ID-omgevingen van opdrachtgever tegen beveiligings-, architectuur- en regelgevingscriteria, en genereert daaruit bevindingen, documentatie en remediatie-artefacten. Toegang tot de omgeving van opdrachtgever verloopt uitsluitend via read-only rollen en is door opdrachtgever eenzijdig en op elk moment intrekbaar.

De dienst leest geen inhoud van workloads, databases, mailboxen, bestanden, back-ups of Key Vault-secrets. De verleende rollen staan dat niet toe.

Aflevering in eigen systemen van opdrachtgever, optioneel. Opdrachtgever kan de dienst opdragen output door te zetten naar systemen die hij zelf beheert: documentatie naar een GitHub-repository, bevindingen als tickets of meldingen in Jira, ServiceNow of TopDesk, of gebeurtenismeldingen naar een door hem opgegeven webhook-URL. Opdrachtgever levert daarbij zelf de instantie én de inloggegevens. Standaard staat elk van deze koppelingen uit en gaat er niets heen. Zodra een koppeling aanstaat, verwerkt de ontvangende partij de gegevens in opdracht van opdrachtgever en niet in opdracht van data processor; het is een verstrekking aan de verwerkingsverantwoordelijke en geen sub-verwerking, en die partijen staan daarom niet in de lijst onder punt 9.

Vanaf het moment dat opdrachtgever een koppeling inschakelt, valt de verwerking door het ontvangende systeem onder zijn eigen verantwoordelijkheid. Data processor levert de gegevens op zijn instructie af; wat daarna in dat systeem gebeurt — bewaring, toegang, verdere verstrekking — staat buiten deze verwerkersovereenkomst. De koppelingen worden in de productdocumentatie beschreven, zodat opdrachtgever vóór het inschakelen weet waar zijn gegevens heen kunnen gaan.

Advies- en consultancyopdrachten. Bij advies- en consultancyopdrachten — waaronder Fractional Architect — werkt data processor als architect met opdrachtgever samen, grotendeels via PAA en deels daarbuiten. Buiten PAA kunnen ontwerpen, notities, diagrammen, correspondentie en exports uit de omgeving van opdrachtgever persoonsgegevens bevatten. Die worden uitsluitend opgeslagen in de Microsoft 365-omgeving van data processor (e-mail, OneDrive, SharePoint en Teams) en op de door data processor beheerde laptop. Werkt data processor bij een opdracht uitsluitend op systemen en apparaten van opdrachtgever, dan verwerkt hij geen persoonsgegevens in eigen beheer en is dit statement voor die opdracht niet van toepassing.

5. Beoogd gebruik

PAA is ontworpen en ingericht om de volgende soorten persoonsgegevens te verwerken:

Categorie	**Toelichting**
Account- en authenticatiegegevens van geautoriseerde gebruikers	Identificatoren, authenticatiegebeurtenissen
Directory- en identiteitsmetadata	User principal names, rol- en groepstoewijzingen, Conditional Access-toewijzingen, device compliance state
Configuratiemetadata van infrastructuur	Resource-identificatoren, typen, eigenschappen, topologie — geen workload-inhoud
Conversatiegegevens	Tekst die gebruikers van opdrachtgever tijdens een sessie invoeren
Bevindingen en afgeleide documentatie	Ernst, categorie, omschrijving, aanbeveling, scores, resource-namen
Auditlogs	Handelingen binnen de werkomgeving van opdrachtgever

Categorieën betrokkenen: geautoriseerde gebruikers van opdrachtgever, en personen die voorkomen in de gescande omgeving (Entra ID-gebruikers, Intune-deviceeigenaren en Azure IAM-principals).

Bij advies- en consultancyopdrachten gaat het buiten PAA om namen, functies en contactgegevens van medewerkers van opdrachtgever in correspondentie en notities, en om accountnamen, rol- en groepstoewijzingen, IAM-principals en resource-namen in ontwerpen, diagrammen en exports. Categorieën betrokkenen: medewerkers van opdrachtgever en personen die voorkomen in de omgeving van opdrachtgever.

Bij deze producten en diensten is **geen rekening gehouden** met de verwerking van bijzondere persoonsgegevens, of gegevens betreffende strafrechtelijke veroordelingen en strafbare feiten, of door de

overheid uitgegeven persoonsnummers. Waar de omgeving van opdrachtgever zulke gegevens bevat, blijven die binnen de systemen van opdrachtgever en zijn ze voor de dienst niet toegankelijk.

Volledigheidshalve: langs drie incidentele routes kan een persoonsnaam in bevindingen terechtkomen — een resource die naar een persoon is vernoemd of getagd, de vrije waarschuwingstekst van Microsoft zelf, en tekst die een gebruiker van opdrachtgever in een sessie intypt. Daarnaast, structureel: bij Zero Trust-controles op gastaccounts (GUEST-001) staan weergavenamen van gasten als bewijs in de bevinding, en waar een weergavenaam ontbreekt het e-mailadres of de user principal name. De eerste drie zijn incidenteel. Deze gastgegevens worden verwijderd voordat een bevinding aan de AI-sub-processor wordt aangeboden (zie punt 6).

Het verwerken van deze gegevens met het hiervoor omschreven product door opdrachtgever is ter eigen beoordeling door opdrachtgever.

6. Privacy by design / privacy by default

Privacy by design is toegepast op de volgende punten; de eerste vijf betreffen PAA:

- **Dataminimalisatie aan de bron** — read-only toegang die inhoud van workloads uitsluit, niet door beleid maar doordat de rollen het niet toestaan.
- **Identiteitsgegevens worden in de EU opgeslagen.** Gestructureerde directory- en identiteitsrecords worden niet naar de AI-sub-processor verzonden. De identiteiten die de controles van de dienst als bewijs vastleggen (weergavenamen, user principal names, e-mailadressen en object-ID's van gast- en beheerdersaccounts) worden verwijderd voordat een prompt wordt opgebouwd; in plaats daarvan gaan aantallen mee. Een identiteit die buiten die controles voorkomt, bijvoorbeeld in een resourcenaam of in tekst die een gebruiker intypt, kan wel worden meegezonden. Laat een gebruiker een sectie van een beoordelingsrapport met AI herschrijven, dan gaat de tekst van die sectie ongewijzigd mee (zie punt 5 en 8).
- **Opslagbeperking is geautomatiseerd** — per gegevenscategorie een bewaartermijn die zonder menselijke tussenkomst verwijdert (zie punt 12).
- **Tenantisolatie** — gegevens zijn per tenant gescheiden; toegangscredentials van opdrachtgever staan per tenant in Azure Key Vault.
- **Standaard uit** — alternatieve AI-aanbieders zijn op platformniveau uitgeschakeld (zie punt 9).
- **Advieswerk in één afgebakende omgeving** — persoonsgegevens uit advies- en consultancyopdrachten komen buiten PAA uitsluitend terecht in de Microsoft 365-omgeving van data processor en op een versleutelde, door data processor beheerde laptop, en worden bij het einde van de opdracht verwijderd (zie punt 12).

De verantwoordelijkheid voor de keuze welke omgevingen worden aangesloten en welke gegevens daarmee in scope komen, ligt bij opdrachtgever.

Keuzes onder de Standaardclausules

7. Data processor gebruikt de **Standaardclausules voor verwerkingen**, welke als bijlage bij de Overeenkomst te vinden zijn.

Het betreft de Standaardclausules voor verwerkingen van NLdigital, versie maart 2025. Zij vormen samen met dit Data Pro Statement de verwerkersovereenkomst als bedoeld in artikel 28 lid 3 AVG. Daarnaast zijn op de Overeenkomst de NLdigital Voorwaarden 2025 als algemene voorwaarden van toepassing, gedeponeerd bij de rechtbank Midden-Nederland, locatie Utrecht. Waar hoofdstuk 4 van die voorwaarden een eigen verwerkersregeling bevat, gelden dit Data Pro Statement en de Standaardclausules daarvoor in de plaats, als uitdrukkelijke schriftelijke andersluidende afspraak in de zin van artikel 1.2 van de NLdigital Voorwaarden 2025.

8. Data processor verwerkt de persoonsgegevens **gedeeltelijk buiten de EU/EER**.

Opslag en verwerking vinden plaats binnen de EU, in Microsoft Azure: North Europe (Dublin) als primaire regio; bestandsopslag wordt geo-gerepliceerd naar West Europe (Amsterdam) en databaseback-ups staan in geo-redundante back-upopslag. Eén structurele doorgifte naar buiten de EER vindt plaats: de inhoud van beoordelingen wordt voor inferentie verzonden naar de AI-sub-processor in de Verenigde Staten (contractpartij en werkruimte); de inferentie kan in andere regio's plaatsvinden (global routing), onder de Standaardbepalingen en zonder bewaring van in- en uitvoer (Zero Data Retention). Bij advies- en consultancyopdrachten vindt buiten PAA geen doorgifte buiten de EER plaats: de Microsoft 365-omgeving van data processor valt onder de EU Data Boundary.

Data processor heeft op de volgende manier geborgd dat een passend beschermingsniveau van toepassing is:

> Data processor heeft met de partij in het derde land **standaardbepalingen (Standard Contractual Clauses)** afgesloten, op grond van artikel 46 lid 2 sub c AVG (Module 3, verwerker aan verwerker).

De doorgifte is onderdeel van de dienstverlening aan opdrachtgever en heeft geen daarvan te onderscheiden eigen doel. Data processor is daarbij verwerker en de AI-aanbieder sub-verwerker. Er wordt niet vertrouwd op een adequaatheidsbesluit. Aanvullende maatregelen: geen training op klantgegevens, Zero Data Retention bij de AI-aanbieder, en het verwijderen van de identiteiten die de controles van de dienst vastleggen voordat een prompt wordt opgebouwd (zie punt 6). De onderbouwing staat in een Transfer Impact Assessment, die op verzoek beschikbaar is.

9. Data processor maakt gebruik van de volgende sub-processors:

Deze lijst is gelijk aan het gepubliceerde sub-processorregister in § 7.6 van het privacybeleid op https://www.crimsonowl.eu/privacy/.

Standaard ingeschakeld — deze verwerken gegevens voor elke opdrachtgever:

Sub-processor	Rol	Locatie	Doorgiftemechanisme
Microsoft (Azure)	Hosting, opslag, authenticatie, sleutelbeheer	EU — North Europe (Dublin) primair; bestandsopslag geo-gerepliceerd naar West Europe (Amsterdam)	Niet vereist; EU Data Boundary
Microsoft (Microsoft 365)	E-mail, bestandsopslag en samenwerking bij advies- en consultancyopdrachten	EU	Niet vereist; EU Data Boundary
Cloudflare	CDN, DDoS-bescherming, netwerkbeveiliging	EU	Standaardbepalingen voor niet-EER-nodes
Anthropic	AI-inferentie op beoordelingsinhoud — de aanbieder die voor alle beoordelingen wordt gebruikt	Verenigde Staten (contractpartij en werkruimte); inferentie kan in andere regio's plaatsvinden (global routing)	Standaardbepalingen, art. 46 lid 2 sub c AVG. Geen training op klantgegevens. Zero Data Retention
Mollie	Betalingsverwerking voor abonnementen. Mollie is verwerker voor de in zijn verwerkersovereenkomst	EU (Nederland)	Niet vereist

Sub-processor	Rol	Locatie	Doorgiftemechanisme
	omschreven verwerkingen en zelfstandig verwerkingsverantwoordelijke voor betaaltransactiegegevens, fraudebestrijding, de op hem als financiële instelling rustende wettelijke verplichtingen (waaronder AML/KYC) en de verbetering van zijn eigen producten en diensten		
Vanta	Monitoring van beveiligingscontroles	EU	Niet vereist

Niet standaard ingeschakeld — alleen op expliciete instructie van opdrachtgever:

Sub-processor	Rol	Locatie	Doorgiftemechanisme
OpenAI	AI-inferentie (GPT)	Verenigde Staten	Standaardbepalingen
Google	AI-inferentie (Gemini)	VS/EU	Standaardbepalingen
Mistral AI	AI-inferentie (Mistral)	EU (Frankrijk)	Niet vereist

De alternatieve AI-aanbieders zijn op platformniveau uitgeschakeld en uitsluitend bereikbaar wanneer opdrachtgever er expliciet één kiest en een eigen API-sleutel aanlevert. Dat is een instructie van opdrachtgever en voegt voor die opdrachtgever een sub-processor aan deze lijst toe. Zonder die instructie verwerken zij geen gegevens van opdrachtgever. De koppelingen naar systemen die opdrachtgever zelf beheert (punt 4) zijn geen sub-processors.

Het informeren over wijzigingen in sub-processors en het recht van opdrachtgever daartegen bezwaar te maken volgen uit artikel 8.3 van de Standaardclausules, dat tevens bepaalt dat data processor ervoor zorgt dat ingeschakelde derde partijen zich committeren aan eenzelfde beveiligingsniveau als waaraan data processor jegens opdrachtgever gebonden is. Data processor voegt daaraan toe dat wijzigingen in de lijst hierboven ten minste **14 dagen** vooraf worden aangekondigd, met gelegenheid tot bezwaar voordat de wijziging ingaat. Het beschikbaar komen van een nieuwe koppeling naar een systeem dat opdrachtgever zelf beheert is geen wijziging in deze lijst; zo'n koppeling staat uit tot opdrachtgever haar zelf inschakelt.

Rechten van betrokkenen en DPIA

10. Data processor ondersteunt opdrachtgever op de volgende manier bij verzoeken van betrokkenen; de eerste vijf onderdelen betreffen PAA:

- **Inzage en dataportabiliteit** — opdrachtgever kan beoordelingen, bevindingen en gegenereerde documentatie zelf exporteren via de dienst, in een gestructureerd formaat.
- **Verwijdering** — de dienst kent een verwijderroute per gebruiker die het bijbehorende bestandsobject vóór de metadata verwijdert, met een afkoelperiode van 30 dagen voordat de verwerking definitief wordt.
- **Correctie** — gegevens zijn afgeleid van de bronomgeving van opdrachtgever; correctie vindt aan de bron plaats en werkt door bij de eerstvolgende verzameling.
- **Bezwaar** — data processor verricht geen profilering en geen geautomatiseerde besluitvorming ten aanzien van betrokkenen; geen van de AI-agents van het product beoordeelt, scoort of classificeert individuele natuurlijke personen. Een bezwaar richt zich daarom op de verwerking door opdrachtgever. Data processor voert op diens instructie uit wat uit de honorering van een bezwaar volgt — in de praktijk het uitsluiten van een omgeving, een abonnement of een gegevensgebied uit verdere verzameling, zoals hieronder beschreven.

- **Beperking van de verwerking** — opdrachtgever kan verdere verzameling zelf stopzetten, zonder tussenkomst van data processor: een gekoppelde Azure-omgeving in haar geheel of een afzonderlijk abonnement uitschakelen; de Microsoft 365-koppeling uitschakelen of daarbinnen een afzonderlijk gegevensgebied uitzetten — waaronder Entra ID-directorygegevens, Intune, Defender en identiteitsbeveiliging; of een koppeling geheel verwijderen, waarbij de opgeslagen inloggegevens worden gewist. Zodra een koppeling of gegevensgebied uitstaat, slaan ingeplande en handmatige scans die omgeving over. Reeds verzamelde gegevens blijven daarbij bestaan; voor verwijdering geldt de route hierboven en punt 12. De fijnmazigheid is per abonnement voor Azure en per gegevensgebied voor Microsoft 365; uitsluiting per afzonderlijke controle bestaat niet.
- **Advies- en consultancyopdrachten** — voor persoonsgegevens buiten PAA voert data processor inzage, correctie, beperking en verwijdering op instructie van opdrachtgever handmatig uit in zijn Microsoft 365-omgeving en op zijn laptop.
- Een verzoek dat data processor rechtstreeks bereikt, wordt onverwijld doorgestuurd naar opdrachtgever, met bevestiging aan de verzoeker dat dit is gebeurd. Data processor beantwoordt zo'n verzoek niet inhoudelijk zelf.

11. Data processor zal op de volgende wijze medewerking verlenen aan Data Protection Impact Assessments (DPIA):

Indien opdrachtgever daartoe verplicht is, verleent data processor na een daartoe redelijk gegeven verzoek zijn medewerking aan een DPIA en aan een eventuele voorafgaande raadpleging van de toezichthouder. Beschikbaar gesteld worden in ieder geval: de omschrijving van de verwerking in dit statement, de beveiligingsmaatregelen (punt 14), de Transfer Impact Assessment, de bewaartermijnen (punt 12) en de meest recente samenvatting van de onafhankelijke penetratietest. Data processor kan hiervoor redelijke kosten in rekening brengen conform artikel 7.7 van de Standaardclausules.

Beëindiging

12. Na beëindiging van de Overeenkomst met een opdrachtgever verwijdert data processor de persoonsgegevens die hij voor opdrachtgever verwerkt in principe binnen **3 maanden** op zodanige wijze dat deze niet langer kunnen worden gebruikt en niet langer toegankelijk zijn (*render inaccessible*).

Drie maanden is een bovengrens, geen streefwaarde; binnen PAA is de feitelijke uitvoering onmiddellijk.

Uitleg op welke wijze gegevens verwijderd worden — PAA. De verwijdering bestaat uit twee helften:

1. **Toegang wordt onmiddellijk ingetrokken.** Bij het verwijderverzoek worden de lidmaatschappen verwijderd en de toegangscache geïnvalideerd. Toegang wordt uitsluitend op een actief lidmaatschap verleend, zodat op dat moment is voldaan aan "niet langer toegankelijk" in de zin van artikel 6.3 van de Standaardclausules — niet pas wanneer het wissen klaar is.
2. **Het wissen loopt daarna op de achtergrond en herhaalt zichzelf** tot elke stap als voltooid is vastgelegd. Bestandsobjecten gaan eerst, over alle opslaglocaties, daarna de gegevensverzamelingen, daarna verweesde gebruikersaccounts en als laatste het tenantrecord. Het wissen is daarmee niet afhankelijk van een beheerder die een mislukte poging opnieuw start.

Welke gegevens worden gewist en welke worden bewaard, is in de broncode van de dienst per gegevensverzameling vastgelegd; een geautomatiseerde test faalt wanneer een nieuwe verzameling zonder beslissing wordt toegevoegd.

Op de hoofdregel van drie maanden bestaan binnen PAA twee uitzonderingen.

a. Wettelijk verplichte bewaring — toegestaan op grond van artikel 6.5 van de Standaardclausules:

Categorie	Termijn	Grondslag
AI-kwaliteitsfeedback en AI-incidentregistraties	3 jaar vanaf aanmaak	EU AI Act art. 25

b. Eigen, gemotiveerde termijn:

Categorie	Termijn	Motivering
Auditlogs van de werkomgeving van opdrachtgever	365 dagen vanaf aanmaak	Vastlegging van handelingen is een beveiligingsmaatregel binnen de dienstverlening aan opdrachtgever, ingericht conform ISO/IEC 27001:2022 A.8.15. Een auditlog die bij beëindiging meteen verdwijnt, kan een incident dat vóór de beëindiging plaatsvond niet meer reconstrueren. Twaalf maanden is de termijn die het beveiligingsstelsel van data processor hanteert

Beide categorieën blijven onder dezelfde beveiligingsmaatregelen vallen en worden voor geen ander doel verwerkt. De auditlogs worden uitsluitend gebruikt voor de beveiliging van de dienst aan opdrachtgever.

Binnen PAA worden gegevens tijdens de looptijd automatisch verwijderd bij het verstrijken van de bewaartermijn per categorie: sessiegegevens 7 dagen, operationele registraties 30 dagen, beoordelingen 90 dagen, directory- en identiteitsmomentopnamen 90 dagen, resultaten van beveiligingscontroles 90 dagen.

Advies- en consultancyopdrachten. Persoonsgegevens van opdrachtgever buiten PAA — in de Microsoft 365-omgeving van data processor en op zijn laptop — worden bij het einde van de opdracht verwijderd, en in elk geval binnen dezelfde termijn van 3 maanden. Die verwijdering is handmatig en omvat ook het legen van de prullenbakken, waaronder die van OneDrive en SharePoint, die verwijderde items anders tot 93 dagen bewaren.

13. Retourneren van persoonsgegevens na beëindiging van de Overeenkomst

Er zijn met opdrachtgever geen afzonderlijke afspraken over teruggave gemaakt, omdat de dienst opdrachtgever gedurende de looptijd doorlopend in staat stelt zijn beoordelingen, bevindingen en gegenereerde documentatie zelf te exporteren. Opdrachtgever wordt geadviseerd dat vóór beëindiging te doen. Op verzoek en tegen redelijke kosten kan alsnog een export worden verstrekt, mits het verzoek vóór het verstrijken van de bewaartermijnen wordt gedaan. Bij advies- en consultancyopdrachten worden de opgeleverde stukken tijdens de opdracht aan opdrachtgever verstrekt.

Beveiligingsbeleid

14. Data processor heeft de volgende beveiligingsmaatregelen genomen ter beveiliging van zijn producten en diensten. Waar niet anders vermeld, betreffen de maatregelen PAA. De regels Incidentrespons en Personeel gelden ook voor advies- en consultancyopdrachten, net als de regels die dat zelf vermelden.

Gebied	Maatregel
Pseudonimisering	Persoonsgegevens worden in de dienst zelf niet gepseudonimiseerd. De dienst moet resources en identiteiten bij naam aan opdrachtgever tonen om bruikbaar te zijn; pseudonimisering zou het product zijn functie ontnemen. In plaats daarvan wordt beperkt bij de bron (read-only, geen workload-inhoud) en in doorgifte: de identiteiten die de controles vastleggen gaan niet mee naar de AI-sub-processor (zie punt 6 en 8)
Versleuteling in opslag	Ja, platformversleuteling op alle opslag, met door Microsoft beheerde sleutels. Door de klant beheerde sleutels (BYOK) worden niet aangeboden
Versleuteling in transport	TLS 1.2 minimaal
Vertrouwelijkheid	Tenantisolatie; credentials per tenant in Azure Key Vault; geheimhoudingsplicht voor al wie onder verantwoordelijkheid van data processor gegevens verwerkt

Gebied	Maatregel
Toegang tot de omgeving van opdrachtgever	**PAA:** uitsluitend read-only; eenzijdig en op elk moment intrekbaar door opdrachtgever. **Advies- en consultancyopdrachten:** via accounts en apparaten die opdrachtgever verstrekt en beheert, met een door opdrachtgever bepaald toegangsniveau dat hij op elk moment kan intrekken
Bevoorrechte toegang	Entra Privileged Identity Management, just-in-time activatie, MFA en motivering vereist; geen permanente rechten
Credentialbeheer	Kortlevende bootstrapsecrets, vervangen door zelfroterende certificaten
Integriteit en onweerlegbaarheid	Entra sign-in- en auditlogs, Azure Activity Log, Log Analytics
Transparantie van uitgaand verkeer	Elke aanroep die het platform tegen de omgeving van opdrachtgever doet, wordt per scan gelogd en geclassificeerd als lezend of schrijvend, 90 dagen bewaard en opvraagbaar door opdrachtgever
Netwerkbescherming	Azure Front Door (Standard) WAF in preventiemodus met eigen regels, waaronder rate limiting; validatie van de Front Door-ID op applicatieniveau tegen het omzeilen van de WAF; alerting naar een bewaakt adres. Een door Microsoft beheerde OWASP-regelset (Premium) is nog niet ingericht
Veilige ontwikkeling	Verplichte code review; CI-poorten voor statische analyse, dependency scanning, secret scanning en DAST
Kwetsbaarhedenbeheer	Scanning van container images en dependencies, gedocumenteerd remediatieproces, onafhankelijke penetratietest (meest recent juni 2026)
Beschikbaarheid en veerkracht	Zone-redundante compute in North Europe; bestandsopslag geo-redundant (North Europe naar West Europe); databaseback-ups geo-redundant. De database zelf draait in één regio, zonder tweede schrijf- of leesregio
Herstel na incident	Doorlopende point-in-time restore, RPO onder 1 seconde, RTO onder 2 uur, jaarlijks getest. Bij uitval van de volledige regio North Europe wordt de database uit de geo-redundante back-up in een andere EU-regio hersteld, met een geschatte extra hersteltijd van twee tot vier uur
Scheiding productie/non-productie	Productiegegevens worden nooit in niet-productieomgevingen gebruikt
Opslagbeperking	Geautomatiseerde verwijdering per gegevenscategorie, zonder menselijke tussenkomst
Incidentrespons	Gedocumenteerde procedure met classificatie, containment-playbooks en de verplichtingen uit artikel 33 AVG
Personeel	Geheimhoudingsplicht, bewustwordingstraining, gedocumenteerd acceptabel gebruik
Werkplek bij advies- en consultancyopdrachten	Eén door data processor beheerde laptop (Windows 11) met volledige schijfversleuteling (BitLocker), Microsoft Defender Antivirus, automatische schermvergrendeling en een wachtwoordbeheerder. Meervoudige authenticatie is verplicht op alle accounts. Buiten de ISMS-eigenaar heeft niemand toegang tot persoonsgegevens van opdrachtgever

Data processor staat er niet voor in dat deze maatregelen onder alle omstandigheden doeltreffend zijn (artikel 4.1 van de Standaardclausules).

15. Data processor heeft zich geconformeerd aan een Information Security Management System (ISMS), geborgd in/via:

> **ISO 27001** — het managementsysteem is ingericht conform ISO/IEC 27001:2022 en de naleving wordt doorlopend geautomatiseerd bewaakt door een onafhankelijk monitoringplatform. De status is inzichtelijk op trust.crimsonowl.eu.

Dit is conformiteit, geen certificering. De certificeringsaudit loopt: fase 1 is op 13 oktober 2026 uitgevoerd door ProCertify B.V. (RvA C 707); fase 2 staat gepland op 30 november en 1 december 2026.

16. Data processor heeft de volgende verificaties en certificeringen:

Geen. Ter voorkoming van misverstanden expliciet vermeld:

	Status
Data Pro Code	Niet opgenomen in het Data Pro register. Crimson Owl Technologies B.V. is lid van NLdigital. Zolang registratie niet rond is, wordt het Data Pro-merk niet gevoerd
ISO 27001 (certificering)	Niet gecertificeerd; wel conform ingericht en doorlopend bewaakt — zie punt 15
SOC 2	Niet van toepassing
NEN 7510	Niet van toepassing — de dienst is niet ingericht voor de zorgsector

Wel is er doorlopende geautomatiseerde controlemonitoring door een extern platform en een onafhankelijke penetratietest, meest recent uitgevoerd in juni 2026, met een gedocumenteerd remediatieplan.

Datalekkenprotocol

17. In geval er toch iets misgaat, hanteert data processor het volgende datalekkenprotocol om ervoor te zorgen dat opdrachtgever op de hoogte is van incidenten:

- **Melding aan opdrachtgever onverwijld en in elk geval binnen 48 uur** nadat data processor bekend is geworden met een inbreuk in verband met persoonsgegevens die opdrachtgever raakt, zodat opdrachtgever zijn eigen termijn van 72 uur uit artikel 33 AVG kan halen.
- **De melding bevat**, voor zover bekend: de aard van de inbreuk, de aard en categorieën van de betrokken persoonsgegevens, de categorieën en het geschatte aantal betrokkenen en registraties, een indicatie van wanneer de inbreuk heeft plaatsgevonden, de waarschijnlijke gevolgen, de getroffen of voorgestelde maatregelen, welke maatregelen opdrachtgever of de betrokkenen zelf zouden kunnen nemen — bijvoorbeeld het wijzigen van wachtwoorden of het letten op ongebruikelijke berichten — en een contactpunt. Wat op dat moment nog niet bekend is, volgt gefaseerd en zonder verdere onnodige vertraging; data processor houdt opdrachtgever op de hoogte van verdere ontwikkelingen totdat het incident is afgesloten.
- **Wijze van melden:** per e-mail aan de bij opdrachtgever bekende contactpersoon voor beveiligingszaken, met telefonische opvolging bij classificatie hoog of kritiek.
- **Beoordeling en melding aan de toezichthouder.** Het is aan de verwerkingsverantwoordelijke — opdrachtgever, of diens klant — om te beoordelen of de inbreuk aan de toezichthouder en/of aan betrokkenen moet worden gemeld. Data processor doet die melding niet namens opdrachtgever, tenzij daartoe schriftelijk geïnstrueerd (artikel 4.2 van de Standaardclausules), en verleent op verzoek medewerking aan de melding (artikel 4.3).
- **Eigen meldroute.** Voor zover data processor zelf verwerkingsverantwoordelijke is, verloopt de melding via het Meldloket datalekken van de Autoriteit Persoonsgegevens.
- De volledige procedure is vastgelegd in een gedocumenteerde incidentresponsprocedure, inclusief classificatie en containment-playbooks.

Ondertekening

	Data processor
Organisatie	Crimson Owl Technologies B.V.
Naam	Marc Dekeyser
Functie	Bestuurder
Datum	16/10/2026
Handtekening	Marc Dekeyser