Privacyverklaring

Versie 1.0 · 25 juni 2026

1. Over deze privacyverklaring

Deze privacyverklaring beschrijft hoe Attic Security B.V. ("Attic", "wij", "ons") persoonsgegevens verwerkt in het kader van onze MDR-dienstverlening en de relatie met onze klanten en gebruikers.

Wij hechten waarde aan uw privacy en behandelen persoonsgegevens conform de Algemene Verordening Gegevensbescherming (AVG) en de Nederlandse Uitvoeringswet AVG.

Deze verklaring is van toepassing op:

- Klantorganisaties die gebruikmaken van onze diensten, inclusief continuous monitoring (DSCM), IVON (onze AI-gedreven response agent) en aanverwante MDR-componenten
- Eindgebruikers binnen klantorganisaties van wie gegevens worden verwerkt
- Bezoekers van onze website en kantoor
- Personen die ons contacteren voor sales, support of andere doeleinden

---

2. Wie wij zijn

Attic Security B.V. Molenstraat 36, 4761 CL Zevenbergen Kamer van Koophandel: 83973206 E-mail: privacy@atticsecurity.com Website: www.atticsecurity.com

Privacy-contactpersoon: Erik Remmelzwaal, CEO privacy@atticsecurity.com

---

3. Welke gegevens wij verwerken

Wij verwerken twee categorieën persoonsgegevens, met elk een eigen verwerkingscontext.

3.1 Servicegegevens — onze MDR-dienstverlening

Voor het uitvoeren van onze MDR-diensten verwerken wij persoonsgegevens uit de Microsoft 365-omgeving (tenant) van onze klanten. Onze dienstverlening omvat meerdere componenten:

- **Continuous monitoring en posture management** — periodieke security-checks op uw Microsoft 365-omgeving om afwijkingen, mis-configuraties en risico's te detecteren
- **IVON** — AI-gedreven triage en remediatie-voorstellen bij beveiligingsincidenten (zie sectie 5 voor AI-specifieke uitleg)
- Aanvullende MDR-componenten zoals overeengekomen in uw Overeenkomst

U blijft als klant te allen tijde verwerkingsverantwoordelijke voor deze gegevens; Attic treedt op als verwerker, conform de tussen ons afgesloten verwerkersovereenkomst (DPA).

Specifieke gegevenscategorieën die wij in opdracht van de klant verwerken:

- **Identiteits- en authenticatiegegevens** uit Microsoft Entra ID — gebruikersnamen, e-mailadressen, rolinformatie, sign-in-historie, risk-events
- **Apparaat- en sessie-informatie** uit Microsoft Defender — endpoint-IDs, IP-adressen, sessie-tokens, threat-signals
- **Beveiligingsincidenten en alerts** uit Microsoft Sentinel en Defender — investigation-data, alert-details, indicators of compromise
- **Audit-log-gegevens** uit Microsoft 365 — gebruikersacties relevant voor security-investigations
- **Configuratie- en posture-gegevens** — security-instellingen, compliance-status, toegangs-configuratie (voor monitoring-componenten)

Wij hebben uitsluitend toegang tot deze gegevens via gedelegeerde OAuth-tokens die u als klant aan ons verstrekt via Microsoft Entra ID. Toegang is per klant-tenant geïsoleerd; ons systeem weigert technisch elke poging tot kruisbestuiving tussen klanten.

U kunt deze toegang op elk moment intrekken via Microsoft Entra ID.

3.2 Klantrelatiegegevens

Voor onze klantrelatie, sales, support en facturatie verwerken wij persoonsgegevens van contactpersonen bij klantorganisaties en prospects:

- **Contactgegevens** — naam, functietitel, zakelijk e-mailadres, telefoonnummer, organisatie
- **Communicatie-geschiedenis** — e-mails, supporttickets, gespreksnotities
- **Facturatiegegevens** — bedrijfsnaam, factuuradres, betalingsinformatie (verwerkt via Chargebee en Stripe)
- **Marketing-interactie** — voor zover toepasselijk en met inachtneming van uw voorkeuren

Voor deze categorie zijn wij verwerkingsverantwoordelijke.

---

4. Waarom wij gegevens verwerken

Categorie	Doel	Rechtsgrond AVG
Servicegegevens (3.1)	Uitvoeren van de MDR-dienst conform overeenkomst en verwerkersovereenkomst	Art. 6.1.b (uitvoering overeenkomst, in verwerker-rol)
Klantrelatiegegevens (3.2)	Beheer van de zakelijke relatie, dienstverlening, support, facturatie	Art. 6.1.b (overeenkomst) en Art. 6.1.f (gerechtvaardigd belang)
Marketing-communicatie	Informeren over diensten en producten	Art. 6.1.a (toestemming) of Art. 6.1.f (gerechtvaardigd belang, opt-out beschikbaar)
Wettelijke verplichtingen	Bewaarplicht boekhouding, fiscale wetgeving	Art. 6.1.c (wettelijke plicht)

---

5. Hoe wij gegevens verwerken — IVON in detail

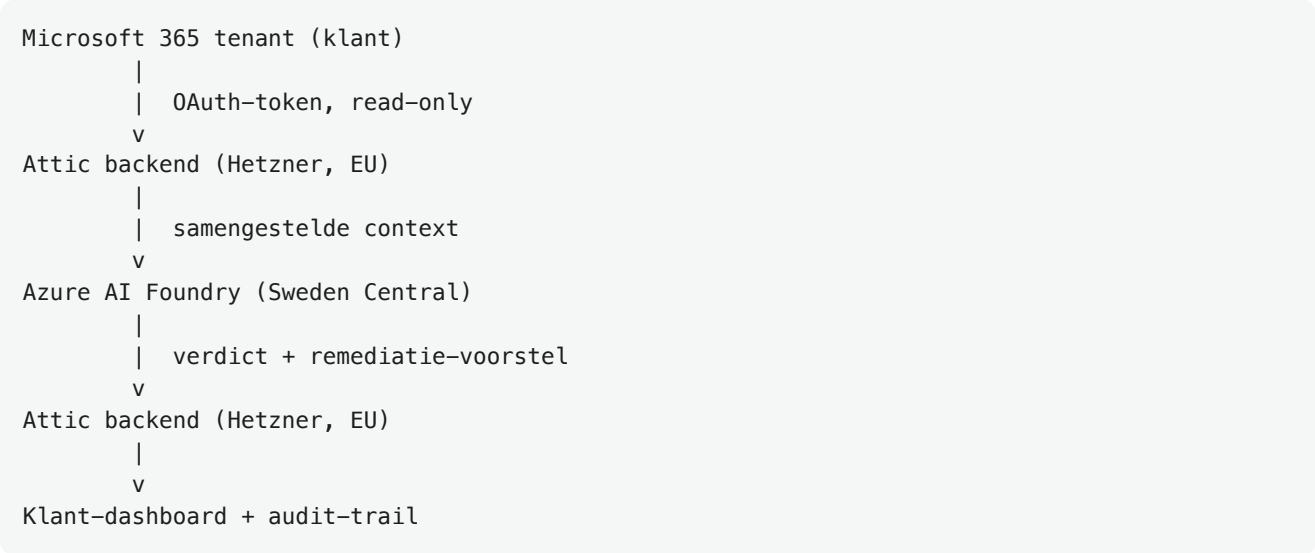
IVON is een geautomatiseerd analyseplatform dat beveiligingsincidenten in uw Microsoft 365-omgeving identificeert, triageert en remediatie-acties voorstelt. Vanwege het AI-component lichten wij hier in detail toe hoe dit werkt.

5.1 Vier waarborgen voor verantwoorde AI-verwerking

Persoonsgegevens van uw eindgebruikers worden voor incident-analyse aan ons taalmodel doorgegeven. Deze gegevens zijn beschermd door vier waarborgen die wij contractueel en technisch hebben ingericht:

1. **Verwerking uitsluitend binnen de EU.** Alle AI-inference vindt plaats binnen Microsoft Azure AI Foundry in regio Sweden Central. Onze eigen backend draait binnen Hetzner-datacenters in Duitsland en Finland. Geen doorgifte buiten de Europese Economische Ruimte.
2. **Het taalmodel wordt niet getraind op uw data.** Microsoft Azure garandeert contractueel dat uw prompts en responses niet worden gebruikt voor training of fine-tuning van welk AI-model dan ook.
3. **Prompts en responses zijn runtime-only.** Het taalmodel verwerkt uw data uitsluitend tijdens de actieve incident-analyse. Er is geen persistente opslag bij het taalmodel, geen geheugen tussen sessies en geen profielopbouw over uw organisatie of eindgebruikers.
4. **Per klant geïsoleerd zonder kruisbestuiving.** Toegang via OAuth-tokens specifiek voor uw tenant; onze systemen weigeren technisch elke poging om data uit andere tenants op te halen. Voor periodieke security-checks hanteren wij daarnaast strikte runtime-scheiding waarbij elke check in een schone omgeving wordt uitgevoerd zonder restanten van eerdere klant-sessies, met centraal beheerde toegangs-credentials.

5.2 Gegevensstroom op hoofdlijnen



5.3 Verwerkingsstappen

1. **Inlezen.** Wij lezen incidenten, alerts en relevante context uit uw Microsoft 365-omgeving via Microsoft Graph en aanverwante API's. Wij wijzigen niets in uw data.
2. **Voorbereiden.** Op onze backend (Hetzner, EU) stellen wij een relevante context samen voor de specifieke incident-analyse. Dit context-pakket bevat de alert-data, betrokken gebruikersnamen, IP-

adressen, indicators of compromise en de specifieke vraag aan het taalmodel.

3. **Analyseren.** De samengestelde context wordt naar het taalmodel gestuurd. Het model produceert een verdict (true positive, false positive, benign of inconclusive) en eventuele remediatie-voorstellen. Het taalmodel ziet uitsluitend deze ene incident-context — geen historie, geen andere klanten, geen toegang tot de bredere tenant.
4. **Terugkoppelen.** Het resultaat komt terug op onze backend en wordt voor u beschikbaar gesteld in het Attic-dashboard, inclusief audit-trail.
5. **Uitvoeren** (optioneel). Door u goedgekeurde remediatie-acties worden via Microsoft Graph uitgevoerd in uw eigen tenant. Zonder uw goedkeuring vinden geen wijzigingen plaats in uw omgeving.

5.4 Technische transparantie — welk taalmodel

Het door ons gebruikte taalmodel is Claude, ontwikkeld door Anthropic en gehost door Microsoft binnen Azure AI Foundry in regio Sweden Central. Microsoft is in deze opzet verantwoordelijk voor de hosting, data-handling en bijbehorende contractuele waarborgen — Anthropic ontvangt zelf geen klantdata via deze route. Om die reden is Anthropic geen sub-verwerker van Attic; Microsoft Corporation (Azure AI Foundry) is dat wel en is opgenomen in onze sub-verwerkerlijst (Bijlage A).

5.5 AI-verwerking — aanvullende kenmerken

Naast de vier hoofdwaarborgen uit sectie 5.1 zijn de volgende technische kenmerken relevant:

- **Abuse monitoring door Microsoft.** Microsoft past content-filtering toe op AI-input en -output. Content die door classifiers wordt gevlagd kan tot maximaal 30 dagen in-region (Sweden Central) worden bewaard voor menselijke review door Microsoft, logisch gescheiden per resource, en wordt niet gebruikt voor model-training. Deze maatregel is bedoeld om misbruik van AI-diensten — zoals het genereren van malware of schadelijke content — tegen te gaan.
- **Transient caching.** Voor performance hanteert Azure een transiënte prompt-caching met een maximum van 24 uur, GPU-lokaal en gescheiden per Azure-subscription.
- **Geen stateful AI-functies.** Wij gebruiken geen Azure-functies die persistente AI-state opbouwen zoals Assistants-threads, fine-tuning of vector-indexes.

5.6 Audit-trail

Wij bewaren een audit-trail van elke uitgevoerde analyse op onze eigen backend (Hetzner, EU). Deze audit-trail bevat metadata zoals het tijdstip van alarm-ontvangst, doorlooptijd tot oppakken, verrijking-stappen, uitgevoerde acties door IVON, conclusie en advies aan u. Deze audit-trail is uitsluitend zichtbaar voor u en voor Attic-medewerkers die in opdracht van u investigation-werk uitvoeren.

5.7 Toekomstige privacy-opties en maatwerk

Wij blijven werken aan aanvullende privacy-controles. Eén optie die wij voor toekomstige releases overwegen is pseudonimisering voorafgaand aan AI-verwerking, waarmee bepaalde persoonsgegevens (zoals gebruikersnamen en e-mailadressen) zouden worden vervangen door pseudoniemen vóór verzending naar het taalmodel. Deze functionaliteit is **bij launch nog niet beschikbaar** — wij beoordelen het samen met klantfeedback voor introductie in een latere release.

Heeft u specifieke verhoogde privacy-eisen vanuit uw sector of regelgeving (bijvoorbeeld zorg, overheid, juridische dienstverlening)? Neem contact op met privacy@atticsecurity.com om de mogelijkheden voor maatwerk-afspraken te bespreken.

6. Geautomatiseerde besluitvorming

IVON voert geautomatiseerde analyse uit, maar geen geautomatiseerde besluitvorming met rechtsgevolgen of vergelijkbaar significante impact in de zin van Art. 22 AVG. Concreet:

- IVON triageert en stelt acties voor; uitvoering van remediatie-acties vindt alleen plaats na expliciete goedkeuring door u of een door u gemachtigde persoon
- Geen automatische sanctie of weigering jegens betrokkenen vindt plaats op basis van AI-analyse

7. Met wie delen wij gegevens

Voor de uitvoering van onze dienstverlening maken wij gebruik van zorgvuldig geselecteerde sub-verwerkers, met elk van wie een verwerkersovereenkomst is afgesloten. De volledige sub-verwerker lijst is te vinden in Bijlage A van dit document en wordt periodiek bijgewerkt op onze website.

Wij delen uw persoonsgegevens uitsluitend met:

- **Sub-verwerkers** die noodzakelijk zijn voor onze dienstverlening (zie Bijlage A)
- **Bevoegde autoriteiten** indien een wettelijke verplichting daartoe bestaat
- **Adviseurs en accountants** voor zover noodzakelijk voor onze bedrijfsvoering, onder geheimhoudingsplicht

Wij verkopen geen persoonsgegevens aan derden voor marketing- of andere commerciële doeleinden.

8. Waar wij gegevens verwerken — geen doorgifte buiten de EU

Onze verwerking vindt volledig binnen de Europese Unie plaats:

- **Backend en opslag:** Hetzner Online datacenters in Duitsland (primair) en Finland (secundair)
- **AI-inference:** Microsoft Azure AI Foundry in Sweden Central
- **Continuous monitoring infrastructure:** Microsoft Azure regio West Europe
- **Klantrelatiegegevens (CRM, support, billing):** EU-regio's van onze sub-verwerkers — zie Bijlage A

Wij dragen geen persoonsgegevens over naar landen buiten de Europese Economische Ruimte (EER). Mocht in de toekomst een dergelijke doorgifte alsnog noodzakelijk worden, dan zal dit uitsluitend gebeuren onder de toepasselijke waarborgen uit hoofdstuk V AVG (zoals modelcontractbepalingen) en wordt deze privacyverklaring vooraf aangepast.

9. Hoe lang wij gegevens bewaren

Categorie	Bewaartermijn	Toelichting
Servicegegevens — IVON incident-investigation-data	**30 dagen** in IVON-systeem	Stelt ons in staat snel onderzoek te doen op uw verzoek. Doorgegeven aan continuous monitoring-systemen voor langere bewaring waar relevant
Servicegegevens — continuous monitoring (door checks geselecteerde data)	**1 jaar**	Voor historisch overzicht en posture-trend-analyse
Servicegegevens — open alarmen en openstaande tickets	Tot afhandeling + 1 jaar	Tot werkstroom is afgerond
Servicegegevens — bij beëindiging klant-abonnement	7 dagen soft-delete + 30 dagen daarna purge	Volledige verwijdering binnen 37 dagen na beëindiging abonnement
Servicegegevens — LLM-prompts/responses	Runtime-only	Zie sectie 5.5
Servicegegevens — Microsoft abuse monitoring gevlagde content	Maximaal 30 dagen bij Microsoft	Zie sectie 5.5
Klantrelatiegegevens — facturatie-gerelateerd	7 jaar	Fiscale bewaarplicht
Klantrelatiegegevens — overige (CRM, contacten)	Duur klantrelatie + 24 maanden	Voor relatiebeheer
Support-tickets	Duur klantrelatie + 24 maanden	Voor lopende issues
Marketing-gegevens	Tot intrekking toestemming of opt-out	Zie sectie 11
Website-bezoekersinformatie	Conform ons cookiebeleid	atticsecurity.com/cookies

De oorspronkelijke data waar Attic doorheen werkt (de incidenten, alerts en log-data in uw Microsoft 365-omgeving) blijft altijd eigendom van u en in uw omgeving. Attic verwijdert na de bovenstaande termijnen uitsluitend de eigen kopieën en bewerkingen.

---

10. Hoe wij gegevens beveiligen

Attic is **in proces tot ISO/IEC 27001:2023-certificering, met onze Stage 2-audit gepland voor Q4 2026.** Wij hanteren passende technische en organisatorische maatregelen om persoonsgegevens te

beschermen, waaronder:

- **Toegangsbeveiliging** — least-privilege access, multi-factor authenticatie voor alle medewerkers met toegang tot klant-relevante systemen
- **Versleuteling** — versleuteling in transit (TLS) en at rest voor alle persoonsgegevens
- **Logging en monitoring** — alle toegang tot klantdata wordt gelogd en gemonitord; afwijkingen worden onderzocht
- **Incidentbeheer** — wij hebben een formeel incidentbeheerproces met meldroutes. Wij melden datalekken die uw persoonsgegevens raken binnen 48 uur aan u; u meldt vervolgens als verwerkingsverantwoordelijke binnen 72 uur aan de Autoriteit Persoonsgegevens conform AVG Art. 33
- **Awareness** — onze medewerkers ontvangen periodieke training over informatiebeveiliging en privacy
- **Sub-verwerker review** — wij beoordelen onze sub-verwerkers op security en privacy bij contract en periodiek daarna

---

11. Uw rechten

Onder de AVG heeft u (of de betrokkenen in uw organisatie) de volgende rechten:

- **Inzage** in de persoonsgegevens die wij verwerken
- **Rectificatie** van onjuiste of onvolledige gegevens
- **Verwijdering** (vergetelheid), voor zover daar geen wettelijke grondslag voor bewaring bestaat
- **Beperking** van verwerking onder bepaalde omstandigheden
- **Overdraagbaarheid** van gegevens
- **Bezwaar** tegen verwerking op grond van gerechtvaardigd belang of voor direct marketing
- **Intrekking van toestemming** wanneer verwerking op toestemming is gebaseerd

Hoe uw rechten uit te oefenen: stuur een e-mail naar privacy@atticsecurity.com. Wij reageren binnen 30 dagen.

Voor servicegegevens (categorie 3.1) waarvoor uw organisatie verwerkingsverantwoordelijke is: verzoeken van betrokkenen worden in eerste instantie via uw eigen organisatie behandeld. Wij ondersteunen u daarbij conform onze verwerkersovereenkomst.

---

12. Klachtrecht

Als u meent dat wij niet zorgvuldig met uw persoonsgegevens omgaan, horen wij dat graag van u via privacy@atticsecurity.com.

U heeft het recht om een klacht in te dienen bij de Autoriteit Persoonsgegevens: **Autoriteit Persoonsgegevens** Postbus 93374 2509 AJ Den Haag www.autoriteitpersoonsgegevens.nl

---

13. Wijzigingen

Wij actualiseren deze privacyverklaring wanneer onze dienstverlening, sub-verwerkers of relevante wet- en regelgeving daartoe aanleiding geeft. De actuele versie is altijd te vinden op www.atticsecurity.com/privacy.

Bij materiele wijzigingen informeren wij u proactief, in ieder geval per e-mail aan de geregistreerde contactpersoon bij uw organisatie.

---

14. Toepasselijk recht en geschillen

Op deze verklaring is Nederlands recht van toepassing.

---

15. Contact

Voor vragen over deze privacyverklaring of de verwerking van uw gegevens:

- **Privacy-vragen:** privacy@atticsecurity.com
- **Privacy-contactpersoon:** privacy@atticsecurity.com (Erik Remmelzwaal)
- **Algemeen:** contact@atticsecurity.com

Bijlage A — Sub-verwerker overzicht

Sub-verwerker	Categorie data	Locatie verwerking	Doel
Hetzner Online GmbH	Servicegegevens (alle, audit-trail), klant-configuratie	Duitsland + Finland (EU)	Hosting backend infrastructure
Microsoft Corporation (Azure + Azure AI Foundry)	Servicegegevens (continuous monitoring, LLM-input/output runtime-only, vault-storage)	West Europe + Sweden Central (EU)	Cloud-infrastructure en AI-inference
Zendesk Inc.	Klantrelatiegegevens (support tickets)	EU-regio	Klantsupport en ticketbeheer (voorgenomen migratie naar HubSpot)
HubSpot Inc.	Klantrelatiegegevens (CRM)	EU-regio	CRM en relatiebeheer
Chargebee Inc.	Klantrelatiegegevens (billing)	EU-regio	Facturatie en abonnementsbeheer
Stripe Inc.	Klantrelatiegegevens (payment)	EU-regio	Betaalverwerking (via Chargebee)

Sub-verwerker	Categorie data	Locatie verwerking	Doel
Functional Software Inc. (Sentry)	Service-metadata (error-tracking, kan PII bevatten in stack traces)	EU-regio	Foutdetectie en debugging (voorgenomen vervanging door het zelf-gehoste GlitchTip)

Technische infrastructure (geen persoonsgegevens, geen AVG sub-verwerker maar opgenomen voor transparantie):

- **Zabbix** — system monitoring, alleen infrastructure-metrics
- **GlitchTip** — error-tracking, zelf-gehoste oplossing op Attic-infrastructure (Hetzner, EU)