# Security Whitepaper

Enterprise Security Overview - AI Interview Analyzer

| | |
|---|---|
| **Aanbieder:** | AI Interview Analyzer Sp. z o.o. |
| **Adres:** | ul. Jedrusik 6/53, 01-748 Warszawa, Poland |
| **NIP:** | 5253079974 |
| **REGON:** | 54402118500000 |
| **Classificatie:** | PUBLIC |
| **Datum:** | 24.06.2026 |

# Contents

# Security Whitepaper

**Aanbieder:** AI Interview Analyzer Sp. z o.o., Warszawa, Poland

**Doelgroep:** Enterprise security-, IT- en inkoopteams

**Classificatie:** Openbaar

## 1. Samenvatting voor directie

AI Interview Analyzer is een enterprise recruitmentplatform dat interviews opneemt met expliciete toestemming van de kandidaat, deze transcribeert en structureert, en op bewijs gebaseerde evaluatieondersteuning voor recruiters produceert. Omdat het platform persoonsgegevens van kandidaten verwerkt en wervingsprocessen ondersteunt, worden security en privacy behandeld als primaire ontwerpbeperkingen, niet als functies die later worden toegevoegd.

Dit whitepaper beschrijft in concrete en verifieerbare termen hoe wij klant- en kandidaatgegevens beschermen. Het is geschreven voor de mensen die leveranciers beoordelen: security engineers, IT-beheerders, functionarissen voor gegevensbescherming en inkoop. Elk cijfer in dit document is rechtstreeks ontleend aan onze eigen engineering-systemen en niet aan marketingmateriaal.

De centrale boodschap is eenvoudig: **wij stellen niet slechts dat het platform veilig is, wij testen dit continu.** Onze codebase bevat **3,171 geautomatiseerde tests**, waaronder een specifieke security-suite die authenticatie, autorisatie, isolatie tussen organisaties, bescherming tegen injecties en gegevensverwijdering test. Daarnaast voeren wij een herhaalbare harness voor penetratietests uit tegen live deployments en produceren wij schriftelijke auditrapporten. Over zeven interne security-audits in maart en april 2026 registreerden wij **zero critical findings**, waarbij onze meest recente audit werd afgesloten met het oordeel **PASS**. (Formele certificering door derden van deze beheersmaatregelen staat op onze roadmap; zie Sectie 18.)

| Security-kenmerk | Samenvatting |
|---|---|
| Hosting | Microsoft Azure, alleen EU-regio's |
| Netwerkmodel | Private endpoints, standaard netwerksegmentatie met default-deny, geen openbare database |
| Encryptie | AES-256 at rest, TLS 1.2 of hoger in transit |
| Identiteit | Kortlevende ondertekende tokens, bcrypt password hashing, SSO-ondersteuning |
| Toegangsbeheer | Role-based access control met strikte isolatie per organisatie |
| Secrets | Gecentraliseerde secrets vault met toegang via managed identity |
| Privacy | Expliciete toestemming, configureerbare retentie, wissen per eenheid |
| Responsible AI | Alleen beslissingsondersteuning, mens altijd in the loop |
| Assurance | 3,171 geautomatiseerde tests plus terugkerende penetratietests en audits |

### 1.1 Hoe dit document te lezen

Secties 3 tot en met 11 beschrijven de beheersmaatregelen die gegevens beschermen: architectuur, netwerk, identiteit, applicatie, gegevensbescherming, privacy en de secure development lifecycle. Secties 12 en 13 behandelen ons onderscheidende programma voor continue tests en onze auditgeschiedenis. Secties 14 tot en met 17 behandelen operations, threat modeling, vulnerability management en compliance-mapping. De appendices bevatten een control catalog, een FAQ voor reviewers en een glossary die een securityteam direct tijdens een beoordeling kan gebruiken.

# 2. Reikwijdte en aanpak van het document

## 2.1 Wat dit document behandelt

Dit whitepaper behandelt de security-architectuur en -praktijken van de AI Interview Analyzer-dienst: de hostingomgeving, het netwerkontwerp, identity and access management, applicatiecontroles, gegevensbescherming, privacy en afstemming op regelgeving, de secure development lifecycle en ons programma voor continue security-tests.

## 2.2 Wat het verifieerbaar maakt

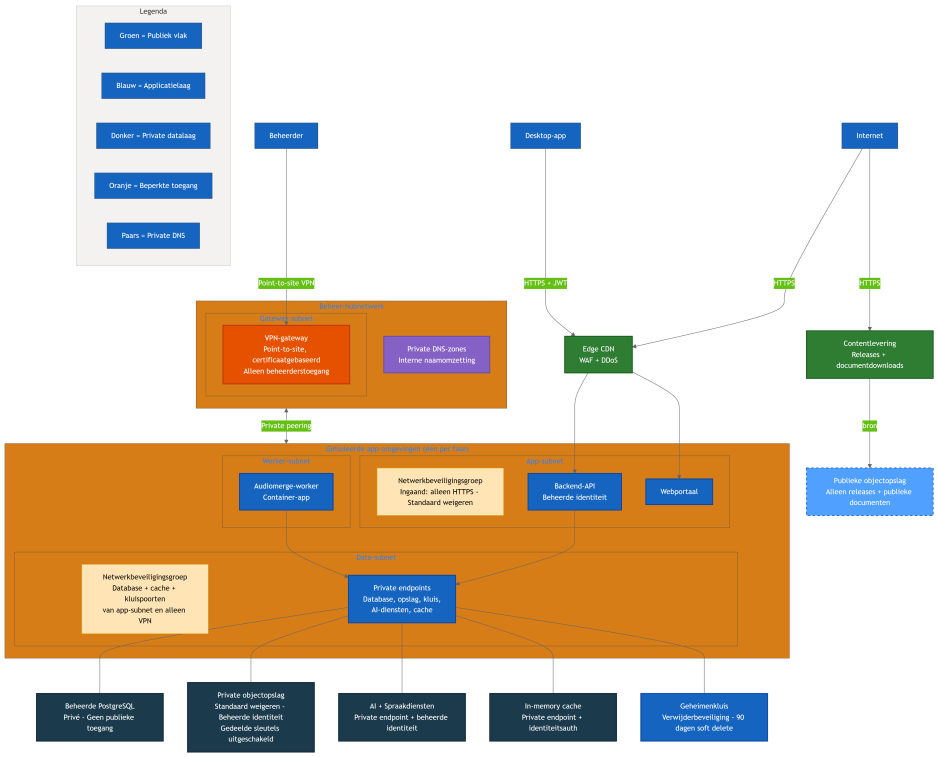
Security-claims van leveranciers zijn eenvoudig op te schrijven en moeilijk te vertrouwen. Daarom hebben wij elke belangrijke claim in dit document gekoppeld aan iets concreets en telbaars binnen onze engineering-systemen: een control die in code is geïmplementeerd, een test die aantoont dat de control werkt, een infrastructuurdefinitie die deze afdwingt, of een auditrapport dat een gedocumenteerde controle vastlegt. Waar een control deel uitmaakt van onze toekomstige roadmap en vandaag nog niet is uitgerold, vermelden wij dat expliciet. Wij doen liever te weinig claims en worden vertrouwd, dan te veel claims en worden betrapt.

## 2.3 Gedeelde verantwoordelijkheid

Het platform wordt geleverd als software as a service. Wij beheren de infrastructuur, applicatie, AI-pipeline en gegevensverwerking. De klant is verantwoordelijk voor het beheren van de eigen gebruikersaccounts en rollen, het configureren van data-retentietermijnen zodat deze aansluiten op het interne beleid, en het waarborgen dat toestemming van kandidaten wordt verkregen via de toestemmingsworkflow die het platform biedt. Sectie 14 beschrijft deze verdeling in meer detail.

# 3. Overzicht van de security-architectuur

Het platform is gebouwd als een klein aantal samenwerkende diensten in plaats van als één monolith. Een desktopapplicatie en een webportal fungeren als clients. Een centrale backend API beheert alle persistentie, authenticatie, facturatie, de AI-pipeline, toestemming, e-mail, bestandsverwerking en dashboards. Een audio merge worker verwerkt opnamen asynchroon. Alle gevoelige status bevindt zich achter de backend API; clients communiceren nooit rechtstreeks met de database, storage of AI-diensten.




Het bovenstaande diagram toont de productietopologie, waarbij resourcenamen opzettelijk zijn gegeneraliseerd. Drie principes zijn hierin zichtbaar:

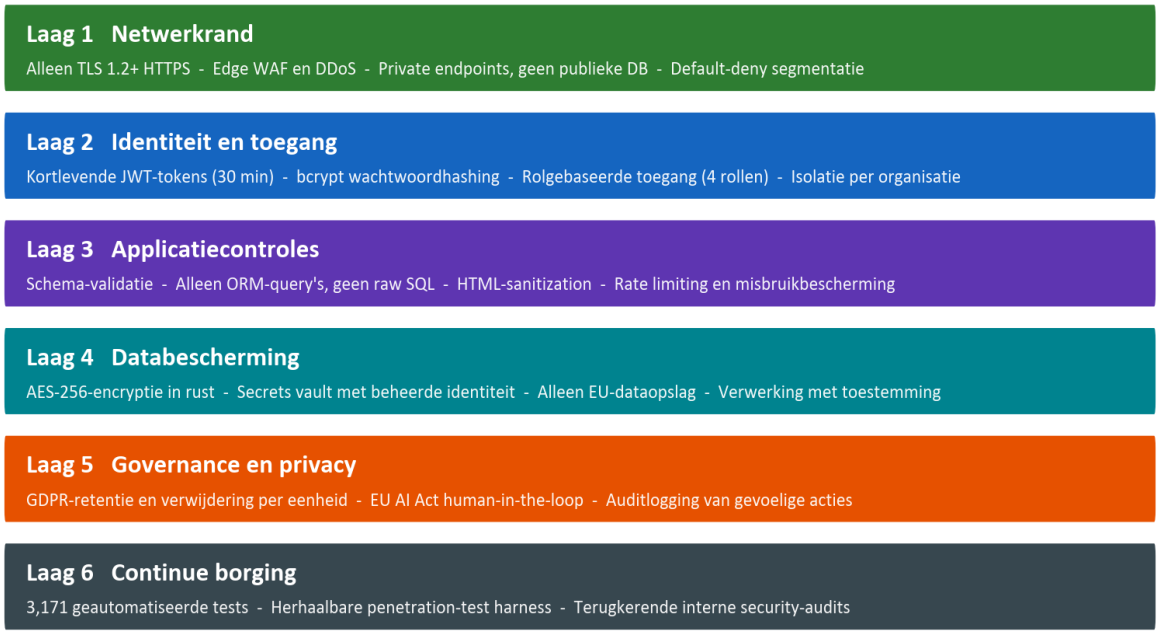
- **Geen directe blootstelling van datadiensten.** De database, private object storage, AI-diensten en cache hebben openbare netwerktoegang uitgeschakeld en zijn alleen bereikbaar via private endpoints binnen een geïsoleerd virtueel netwerk. De secrets vault wordt door de applicatie bereikt via een private endpoint en wordt daarnaast beschermd door platformidentiteitsauthenticatie en least-privilege-toegangsbeleid, zodat voor elke toegang een geldige, geautoriseerde identiteit vereist is, ongeacht het netwerkpad.
- **Een gescheiden publiek oppervlak.** De enige openbare object storage bevat release-downloads en openbare documenten. Deze bevat nooit kandidaatgegevens. Klantgerichte applicatieverkeer loopt via een edge-laag die web application firewall, distributed-denial-of-service-bescherming en content delivery biedt.
- **Administratieve toegang is afgeschermd.** Operators bereiken interne resources uitsluitend via een certificaatgebaseerde point-to-site VPN naar een management hub-netwerk, niet via het openbare internet.

Elke deploymentfase (development en production) is een volledig geïsoleerde omgeving met een eigen netwerk, storage accounts, database en secrets. Productiegegevens van klanten zijn nooit aanwezig in lagere omgevingen. Een gedeelde management hub bevat alleen de VPN-gateway en private DNS, privé gepeerd met elke omgeving.

# 4. Defense in depth

Er wordt niet vertrouwd op één enkele control om elke aanval te stoppen. Het platform gebruikt onafhankelijke, gelaagde controls zodat het falen van één laag niet leidt tot blootstelling van gegevens. De onderstaande lagen zijn elk geïmplementeerd en, zoals beschreven in Sectie 12, afzonderlijk getest.

**Gelaagd security-model: onafhankelijke controles op elk niveau**




| Laag | Representatieve controls |
|---|---|
| Netwerkedge | Alleen TLS-transport, edge WAF en DDoS-bescherming, private endpoints, default-deny-segmentatie |
| Identiteit en toegang | Kortlevende ondertekende tokens, bcrypt hashing, role-based access control, isolatie per organisatie |
| Applicatie | Schemavalidatie op alle input, uitsluitend ORM-datatoegang, output encoding, rate limiting |
| Gegevensbescherming | Encryptie at rest, secrets vault met managed identity, EU-dataresidentie, verwerking achter toestemming |
| Governance en privacy | Configureerbare retentie, wissen per eenheid, human-in-the-loop AI, audit logging |
| Continue assurance | Geautomatiseerde testsuite, herhaalbare penetratietests, terugkerende interne security-audits |

De rest van dit document behandelt elke laag afzonderlijk en beschrijft vervolgens hoe wij continu aantonen dat deze lagen standhouden.

# 5. Netwerksecurity

## 5.1 Standaard privé

De datalaag is by design privé. De beheerde PostgreSQL-database heeft openbare netwerktoegang uitgeschakeld en is alleen bereikbaar via een private endpoint. Private object storage is geconfigureerd om netwerktoegang standaard te weigeren, schakelt shared access keys volledig uit en is alleen toegankelijk via managed identity vanuit het applicatiesubnet. De cache, AI-diensten en secrets vault worden op dezelfde manier bereikt via private endpoints met private DNS-resolutie.

In de praktijk betekent dit dat er geen internetgerichte connection string naar de database bestaat en geen openbare storage-URL voor kandidaataudio: de database en private storage hebben openbare netwerktoegang expliciet uitgeschakeld. De secrets vault wordt door de applicatie bereikt via een private endpoint en wordt beschermd door platformidentiteitsauthenticatie en least-privilege-toegangsbeleid, waarbij applicatie-identiteiten alleen read-only-toegang krijgen tot de secrets die zij nodig hebben, zodat secrets niet kunnen worden opgehaald zonder een geldige, geautoriseerde identiteit. Het aanvalsoppervlak dat een externe aanvaller überhaupt kan benaderen, is beperkt tot de HTTPS-endpoints van de applicatie achter de edge-laag.

## 5.2 Netwerksegmentatie

Elke omgeving is opgedeeld in afzonderlijke subnets voor de applicatielaag, de datalaag en de asynchrone worker. Elk subnet wordt beheerd door een network security group waarvan de laatste regel al het inkomende verkeer weigert. Het applicatiesubnet accepteert alleen inkomend HTTPS. Het datasubnet accepteert alleen de specifieke poorten voor database, cache en vault, en alleen vanuit het applicatiesubnet of de administratieve VPN. Dit betekent dat zelfs een aanvaller die op de een of andere manier de applicatielaag bereikt, niet vrij kan pivoteren naar de datalaag; de enige toegestane paden zijn de paden die de applicatie legitiem gebruikt.

## 5.3 De edge

Openbaar applicatieverkeer wordt afgehandeld door een edge-laag die een web application firewall, DDoS-bescherming en een content delivery network biedt. Downloads van releases en documenten worden geleverd vanuit een dedicated openbaar storage account via een content-delivery front door, volledig gescheiden van de private storage die kandidaatgegevens bevat. Deze twee storage-vlakken worden nooit gemengd: een misconfiguratie in het openbare vlak kan geen private kandidaatgegevens blootstellen, omdat het verschillende accounts met verschillende netwerkregels zijn.

## 5.4 Administratieve toegang

Er is geen openbaar administratief endpoint naar het private netwerk. Operators verbinden via een point-to-site VPN-gateway die certificaatgebaseerde authenticatie gebruikt. Administratieve toegang tot database en cache is alleen mogelijk vanuit die tunnel, omdat deze diensten openbare netwerktoegang uitgeschakeld hebben. Hierdoor blijven dagelijkse beheeractiviteiten volledig van het openbare internet af.

# 6. Identity and access management

## 6.1 Authenticatie

Gebruikerssessies worden opgezet met een ondertekend access token dat dertig minuten geldig is, gecombineerd met een afzonderlijk, ondoorzichtig, server-side refresh token. Access tokens worden bij elk verzoek geverifieerd en de gebruiker wordt opnieuw gevalideerd tegen de database (inclusief een controle op een actief account) in plaats van uitsluitend te vertrouwen op de inhoud van het token. Uitloggen trekt de server-side refresh-sessie direct in, zodat een gestolen refresh token een logout niet kan overleven.

Wachtwoorden worden nooit in platte tekst opgeslagen. Ze worden gehasht met bcrypt met een unieke salt per wachtwoord. Voor organisaties die de voorkeur geven aan single sign-on ondersteunt het platform OAuth-login met Microsoft en Google; in dat geval wordt er helemaal geen wachtwoord bewaard.

Eigendom van e-mailadressen wordt geverifieerd via een eenmalige, tijdsgebonden verificatielink voordat een zelfgeregistreerd account als geverifieerd wordt behandeld, en het opnieuw verzenden van verificatie-e-mails is rate limited om misbruik te voorkomen.

## 6.2 Role-based access control

Autorisatie wordt afgedwongen via een rollenmodel met vier rollen in oplopende mate van privilege: interviewer, hiring manager, recruiter en administrator. Toegang tot geprivilegieerde handelingen wordt afgedwongen door server-side dependencies die zowel de rol als de verificatiestatus van de aanroeper controleren. Deze rolcontroles beschermen ruim honderd afzonderlijke API-operaties.

| Rol | Typische mogelijkheden |
|---|---|
| Interviewer | Voert toegewezen interviews uit; ziet alleen interviews die aan hen zijn toegewezen |
| Hiring manager | Beheert recruitments waarvan zij eigenaar of lid zijn |
| Recruiter | Volledig recruitment- en kandidatenbeheer binnen de organisatie |
| Administrator | Organisatie-instellingen, facturatie, beheer van gebruikers en API-keys |

Naast grove rolcontroles past het platform regels voor zichtbaarheid op dataniveau toe. Hiring managers zien alleen de recruitments die zij hebben aangemaakt of waarvan zij lid zijn; interviewers zien alleen de interviews die aan hen zijn toegewezen. Privilege wordt dus afgedwongen zowel op het niveau van "welke actie" als op het niveau van "welke records".

## 6.3 Isolatie per organisatie

Het platform is multi-tenant en tenantisolatie wordt behandeld als een eersteklas security-control. Elke geauthenticeerde identiteit draagt een organisatie-identificatie en dataquery's worden tot die organisatie beperkt. Wanneer een gebruiker een record opvraagt dat toebehoort aan een andere organisatie, retourneert het platform een respons "not found" in plaats van te onthullen dat het record bestaat. Interne database-identificatoren worden nooit over de wire blootgesteld; de API presenteert display identifiers en mapt deze per verzoek opnieuw, wat een veelvoorkomende klasse van enumeratieaanvallen tussen tenants elimineert.

Dit is niet alleen een ontwerpintentie. Zoals beschreven in Sectie 12 voert onze geautomatiseerde suite een grote matrix tussen organisaties uit die probeert de gegevens van de ene organisatie te benaderen met credentials van een andere organisatie, en verifieert dat elke dergelijke poging faalt.

## 6.4 Programmatische toegang

Voor integraties kunnen organisaties op daarvoor in aanmerking komende plannen API-keys uitgeven. Keys gebruiken een herkenbare prefix, bevatten 128 bits entropie en worden alleen als hash opgeslagen; de ruwe key wordt eenmalig getoond bij creatie en daarna nooit meer. Elke key heeft een expliciet permissiebereik (read, write of ATS integration), kan worden beperkt

tot specifieke bronnetwerken, kan direct worden ingetrokken en is onderworpen aan rate limits per key die zijn afgeleid van de planlaag van de organisatie. Keyverificatie gebruikt een timing-safe vergelijking om te voorkomen dat informatie via responstiming weglekt.

# 7. Applicatiesecurity

De applicatie is zo geschreven dat volledige kwetsbaarheidsklassen worden verwijderd in plaats van geval per geval te worden gepatcht.

• **Injectie.** Alle databasetoegang verloopt via een object-relational mapper met geparametriseerde query's. De codebase bevat geen ruwe, met strings geformatteerde SQL. Dit elimineert SQL-injectie structureel.

• **Inputvalidatie.** Elke request body wordt gevalideerd tegen een strikt schema voordat deze de businesslogica bereikt. Te grote payloads worden geweigerd en list-endpoints zijn gepagineerd om resourcegebruik te begrenzen.

• **Output encoding en cross-site scripting.** Door gebruikers aangeleverde en door AI gegenereerde tekst wordt behandeld als niet-vertrouwd. Waar content als HTML moet worden weergegeven, gaat deze tijdens write time door een sanitizer op basis van een allow-list, en een dedicated testsuite bevestigt dat script tags, event handlers en javascript URL's worden verwijderd.

• **Mass assignment.** Update-operaties gebruiken expliciete schema's die geprivilegieerde velden zoals rol, organisatie en credit balance uitsluiten, zodat een client geen privilege-escalatie kan uitvoeren door extra velden mee te sturen.

• **Rate limiting.** Authenticatie- en misbruikgevoelige endpoints zijn rate limited met een duurzame, door de database ondersteunde limiter die herstarts overleeft en correct werkt over meerdere applicatie-instances. Login, registratie, password reset en het opnieuw verzenden van verificaties hebben elk hun eigen limieten. Client IP-resolutie is gehard tegen spoofing van forwarding headers.

• **Webhooks.** Inkomende webhooks van payment- en e-mailproviders worden geverifieerd aan de hand van providersignatures op de ruwe request body voordat zij worden verwerkt.

• **Bestandsuploads.** Uploads hebben een maximale grootte, worden gevalideerd, opgeslagen onder gegenereerde identificatoren in plaats van door gebruikers aangeleverde namen, en begrensd per verzoek en per organisatie.

• **Security headers.** In production bevatten responses strict transport security, content-type- en frame-opties, een referrer policy en een restrictieve permissions policy, en onderdrukken zij banners van server en framework.

# 8. Gegevensbescherming

## 8.1 Encryptie

Alle gegevens worden at rest versleuteld met AES-256 via de Azure-platformlagen voor storage- en database-encryptie. Al het netwerkverkeer wordt uitsluitend aangeboden via HTTPS met TLS 1.2 of hoger; platte HTTP wordt op elk niveau doorgestuurd naar HTTPS. In production sturen de API en webportal strict transport security headers mee, samen met een set hardening-headers, en onderdrukken zij server- en frameworkversiebanners.

## 8.2 Secrets management

Applicatiesecrets worden bewaard in een gecentraliseerde secrets vault met purge protection ingeschakeld en een soft-delete-venster van negentig dagen. Applicaties authenticeren naar Azure-resources met system-assigned managed identities in plaats van met langlevende keys; private storage heeft bijvoorbeeld shared access keys volledig uitgeschakeld, zodat toegang uitsluitend mogelijk is via identity-based role assignments die zijn beperkt tot de individuele resource. Vault access policies geven applicatieprincipals read-only-toegang tot de specifieke secrets die zij nodig hebben, volgens het least-privilege-principe.

## 8.3 Dataresidentie

Alle klant- en kandidaatgegevens worden opgeslagen en verwerkt binnen de Europese Unie. Applicatiehosting, database, storage, cache en secrets bevinden zich in West Europe, en AI-verwerking draait in EU-regio's. De AI-provider gebruikt klantgegevens niet om zijn modellen te trainen.

## 8.4 De levensloop van één interview

De duidelijkste manier om de beheersmaatregelen voor gegevensbescherming te begrijpen, is één interview van begin tot eind te volgen. Toestemming wordt vastgelegd en geregistreerd voordat iets wordt verwerkt. De upload wordt in transit versleuteld. Transcriptie en analyse draaien binnen EU-datacenters. Resultaten worden weggeschreven naar versleutelde storage. Elk record wordt vervolgens beheerd door één enkele retentieklok die eindigt in een gelogde, cascaderende verwijdering. Op elk moment kunnen rechten van kandidaten, zoals intrekking, verwijdering, inzage of dataportabiliteit, deze stroom onderbreken.

# 9. Privacy by design en GDPR

Privacy is ingebouwd in het datamodel en de workflow, niet alleen achteraf toegevoegd via beleid.

## 9.1 Toestemming

Geen enkel interview wordt opgenomen of geanalyseerd zonder de expliciete toestemming van de kandidaat. Wanneer een kandidaat aan een recruitment wordt toegevoegd, verstuurt het platform per e-mail een unieke, eenmalige toestemmingslink. De kandidaat beoordeelt wat er gaat gebeuren en accepteert of weigert vervolgens. De toestemmingsstatus, inclusief het tijdstip van reactie, wordt vastgelegd bij die specifieke recruitment, zodat toestemming altijd is beperkt tot een concreet wervingsproces en niet globaal wordt verleend.

**Toestemming kandidaat: expliciet en vastgelegd vóór verwerking**


## 9.2 Retentie en verwijdering

Dataretentie is per organisatie configureerbaar, met een standaard van twaalf maanden en een configureerbaar minimum van dertig dagen, en kan per kandidaat worden overschreven. Er is één enkele retentieklok voor de gegevens van een kandidaat, niet een afzonderlijke timer per artifact. De klok start wanneer een hiring decision wordt vastgelegd. Voordat gegevens verlopen, verstuurt het platform een waarschuwing (standaard ongeveer vijftien dagen van tevoren) en biedt het een verlenging met één klik. Wanneer gegevens worden verwijderd, worden zij als één geheel verwijderd: het kandidaatrecord, interviews, transcripties, audio-opnamen, documenten en vergelijkingen worden allemaal samen verwijderd, en de verwijdering wordt vastgelegd in een audit log. Er blijft geen gedeeltelijk of verweesd residu achter.

De onderstaande lifecycle toont deze enkele klok en hoe deze samenkomt in één cascaderende verwijdering met een gelogd bewijs van verwijdering.

**Dataretentie: één klok per kandidaat, verwijdering per eenheid**


## 9.3 Rechten van betrokkenen en sub-processors

Het platform ondersteunt de rechten van betrokkenen die onder de GDPR zijn vereist, waaronder inzage, verwijdering, dataportabiliteit, bezwaar en uitleg. Verwerking wordt uitgevoerd onder een data processing agreement die klanten bij registratie accepteren en die per organisatie is geversioneerd. Onze sub-processors en hun rollen, allemaal binnen de EU of onder passende waarborgen, worden in die overeenkomst bekendgemaakt, en klanten ontvangen vooraf bericht van elke wijziging. Sectie 17 bevat het register van sub-processors en de compliance-mapping per artikel.

# 10. Responsible AI en de EU AI Act

Het platform valt binnen de high-risk-categorie van de EU AI Act omdat het arbeidsbeslissingen ondersteunt, en wij nemen die classificatie serieus.

De bepalende regel van het product is dat **de AI beslissingsondersteuning is, geen beslisser.** Het systeem accepteert of verwerpt een kandidaat nooit automatisch. Het transcribeert spraak, structureert vragen en antwoorden, scoort antwoorden tegen criteria die de recruiter heeft gedefinieerd en stelt feedback op, waarna een mens elke output beoordeelt voordat deze wordt gebruikt. Zo blijft een mens duidelijk in the loop.

Even belangrijk is wat de AI niet doet. Zij beoordeelt geen persoonlijkheid, "cultural fit", emotionele toestand, stemtoon, accent, gender, leeftijd, etniciteit, uiterlijk of lichaamstaal. Scoring is verankerd in bewijs uit het transcript en in door de recruiter gedefinieerde criteria, en kandidaatsnamen worden uitgesloten van de evaluatie-input om bias te verminderen. Wij publiceren een transparency card, gebruikersdocumentatie en een declaration of conformity waarin het systeem, de beperkingen en de waarborgen worden beschreven.

| Responsible-AI-control | Hoe deze werkt |
|---|---|
| Human in the loop | Elke score en elk stuk feedback wordt vóór gebruik door een recruiter beoordeeld |
| Geen geautomatiseerde beslissingen | Het systeem accepteert of verwerpt een kandidaat nooit automatisch |
| Op bewijs gebaseerde scoring | Scores verwijzen naar ondersteunend bewijs uit het transcript |
| Anti-bias-ontwerp | Namen uitgesloten van evaluatie; inhoud wordt zwaarder gewogen dan stijl |
| Scope-beperkingen | Persoonlijkheid, emotie, accent en beschermde kenmerken worden nooit beoordeeld |
| Veiligheid van kandidaatfeedback | Private kandidaatfeedback doorloopt een generation-and-validation safety guardrail |

Deze beperkingen zijn niet alleen in documentatie vastgelegd; zij zijn gecodeerd in de AI-promptlaag en worden getest door een dedicated AI-safety-testprogramma zoals beschreven in Sectie 12.3.

# 11. Secure development lifecycle

Security wordt afgedwongen in de manier waarop wij software bouwen en uitrollen, niet alleen in het draaiende systeem.

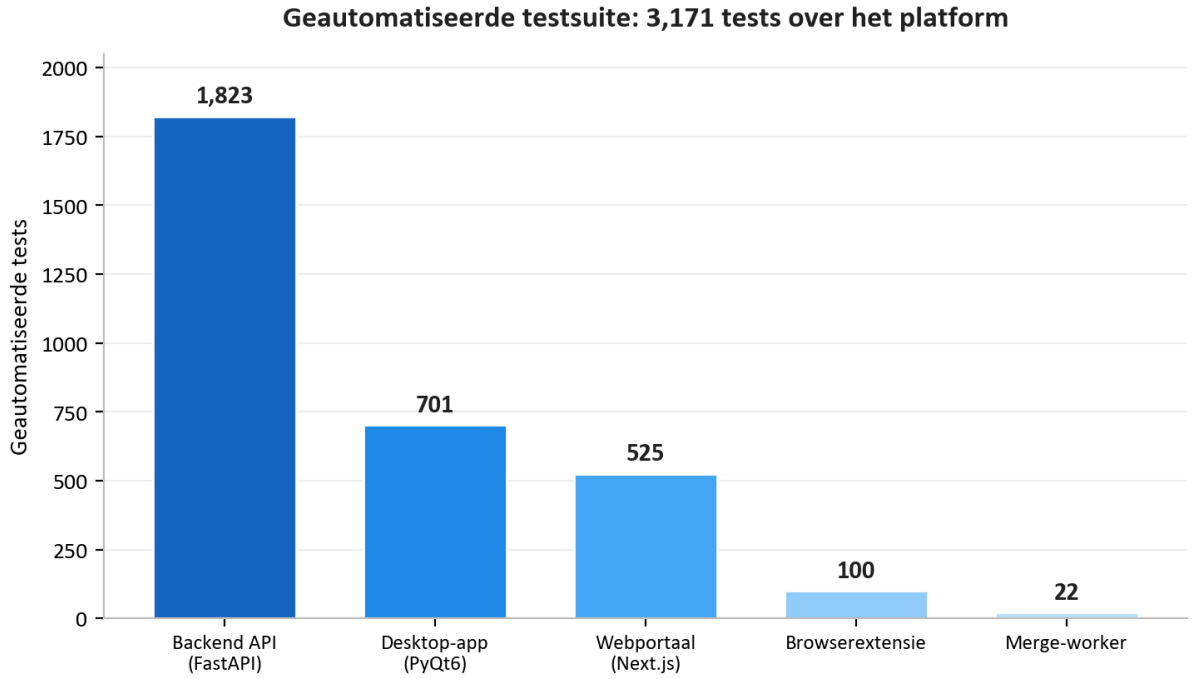
- **Scheiding van omgevingen.** Development en production zijn volledig gescheiden, elk met een eigen infrastructuur, storage accounts, database, secrets en subdomeinen. Er is geen gedeelde status.
- **Infrastructure as code.** De volledige cloudomgeving is als code gedefinieerd en als code beoordeeld, waardoor de security posture auditbaar en reproduceerbaar is. Een reviewer kan exact lezen welke poorten openstaan, welke resources privé zijn en welke identiteiten welke rechten hebben.
- **Vastgepinde, afgeschermde deployments.** Elke stap in de continuous-integration-pipeline is vastgepind op een exacte, onveranderlijke versie. Production deployments zijn tag-based, draaien alleen via de beschermde production-pipeline en zijn afgeschermd met verplichte goedkeuring. De geautomatiseerde testsuite fungeert als release gate: een deployment kan niet worden uitgerold als tests falen.
- **Dependency hygiene.** Geautomatiseerde dependency-monitoring stelt wekelijks updates voor over backend, desktop, web, infrastructuur en pipeline-definities heen, en dependency-audits maken deel uit van onze periodieke security review.
- **Ondertekende artifacts.** Desktopinstallers zijn code-signed, zodat klanten kunnen verifiëren dat de software die zij installeren daadwerkelijk van ons afkomstig is.
- **Secrets-discipline.** Secrets staan in de vault en in beschermde pipelinesecrets, nooit in source code.

# 12. Continue security-tests

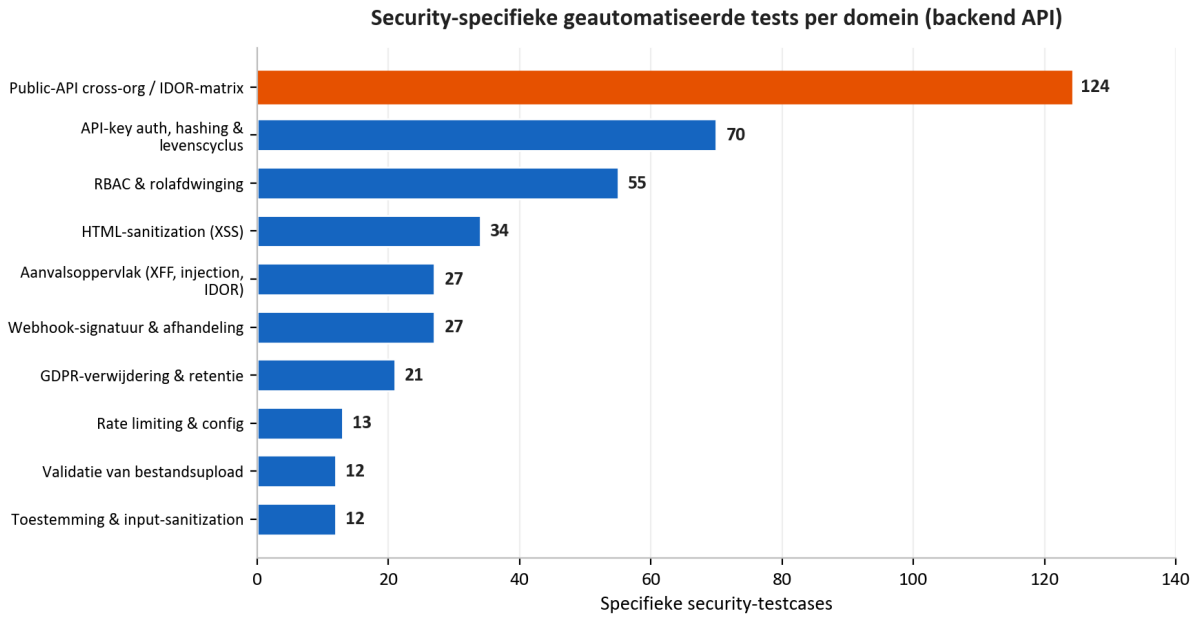
Dit vormt de kern van ons assurance-verhaal en het onderdeel dat de meeste leveranciers niet kunnen tonen. Wij behandelen security als iets dat continu moet worden gemeten, met uitvoerbare controles, in plaats van iets dat eenmalig wordt gesteld.

## 12.1 De geautomatiseerde testsuite

Het platform wordt gedekt door **3,171 geautomatiseerde tests** voor de backend API, de desktopapplicatie, de webportal, de browserextensie en de audio merge worker.




Dit zijn niet alleen functionele tests. Een substantiële, dedicated security-suite test de controls die eerder in dit document zijn beschreven. De onderstaande grafiek splitst de security-specifieke tests in de backend API uit per domein.



Onder vele andere dingen bevat deze suite een grote public-API-matrix die elk endpoint uitvoert als legitieme gebruiker, als de eigen API-key van de organisatie en als de API-key van een rivaliserende organisatie, en verifieert dat elke poging tussen organisaties wordt geblokkeerd. Zij bevat tientallen adversariële tests van het aanvalsoppervlak voor spoofing van forwarding headers, header injection en identifier leakage, een gerichte HTML-sanitization-suite voor cross-site scripting, role-enforcement-tests voor het volledige rollenmodel, en tests die aantonen dat kandidaatgegevens daadwerkelijk als eenheid worden verwijderd. Omdat deze tests als release gate draaien, zou een regressie die een van deze controls verzwakt de release stoppen in plaats van klanten te bereiken.

## 12.2 Live penetratietests

Geautomatiseerde unit tests bewijzen dat controls zich in isolatie correct gedragen. Om aan te tonen dat zij in een echte deployment samen standhouden, onderhouden wij een herhaalbare methodologie voor penetratietests die echte aanvalsscripts uitvoert tegen een live omgeving. Deze is georganiseerd in zes fasen:

| Fase | Focus | Voorbeelden van wat wordt getest |
|---|---|---|
| 1. Static analysis | Source code | Secrets, injectiepatronen, gevaarlijke functies, ontbrekende auth, onveilige HTML |
| 2. Architectuurreview | Infrastructuur | Private endpoints, segmentatie, TLS, configuratie van secrets |
| 3. Analyse van aanvalsvectoren | Source control en cloud | Branch protection, identity scope, openbare blootstelling |
| 4. Live penetratietests | Draaiende omgeving | Probing zonder authenticatie, toegang tussen organisaties, injectie, tokenmanipulatie, SSRF, rate-limit-bursts |
| 5. Enterprise scoring | Volwassenheid | Zestien securitycategorieën gescoord tegen een enterprise-baseline |
| 6. Dependencies en supply chain | Risico van derden | Dependency CVE-audit, vastgepinde pipeline-acties, integriteit van lock files |

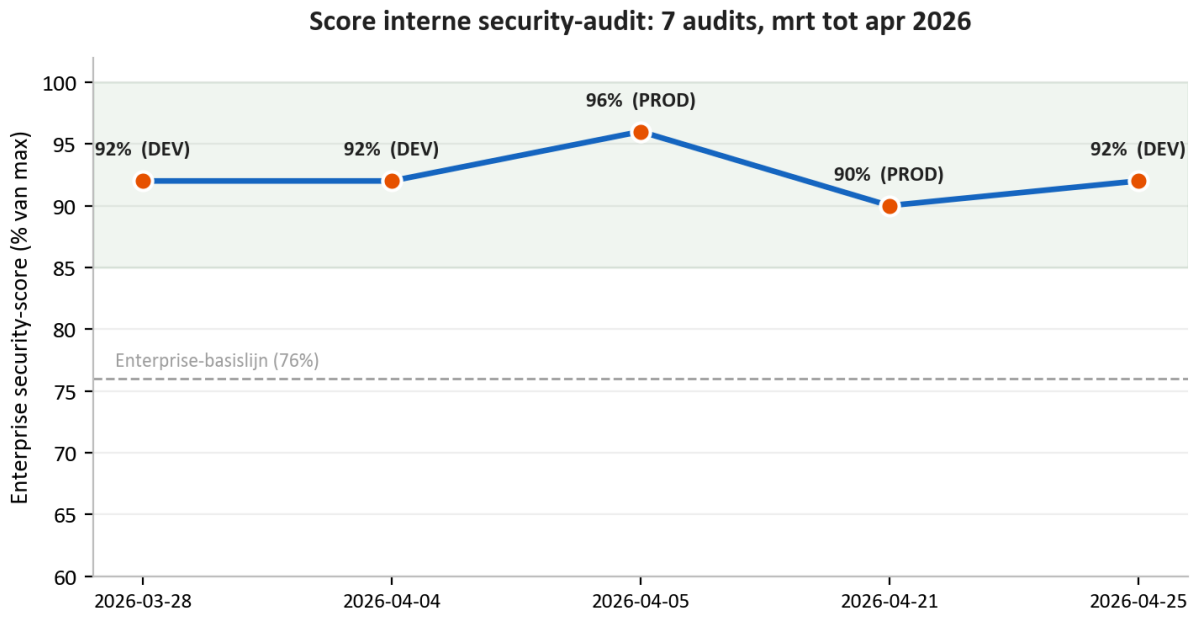
Fase 4 is echte adversariële testing tegen een uitgerold systeem, geen checklist. Zij test beschermde endpoints zonder credentials en bevestigt dat deze toegang weigeren; registreert twee organisaties en probeert de records van de ene organisatie te bereiken met het account van de andere; injecteert cross-site-scripting- en server-side-template-payloads en bevestigt dat deze worden geneutraliseerd; manipuleert authenticatietokens en bevestigt dat deze worden geweigerd; probeert server-side request forgery tegen cloudmetadata-endpoints; en veroorzaakt bursts op authenticatie-endpoints om te bevestigen dat rate limiting daadwerkelijk in de live omgeving wordt geactiveerd, niet alleen in theorie.

## 12.3 Veiligheidstests voor kandidaatfeedback

Omdat het platform private ontwikkelingsfeedback voor kandidaten kan genereren, voeren wij voor die functie een afzonderlijk adversarieel veiligheidsprogramma uit. Dit voedt het systeem doelbewust met harde en vijandige notities van recruiters en bevestigt dat de kandidaatgerichte output nooit vulgariteit bevat, nooit de identiteit of privé-opinie van een recruiter onthult of toeschrijft, en nooit oordelende persoonlijkheidslabels toepast. Dit beschermt zowel de kandidaat, die constructieve en respectvolle feedback moet ontvangen, als de klant, van wie een interne opinie nooit naar buiten mag lekken.

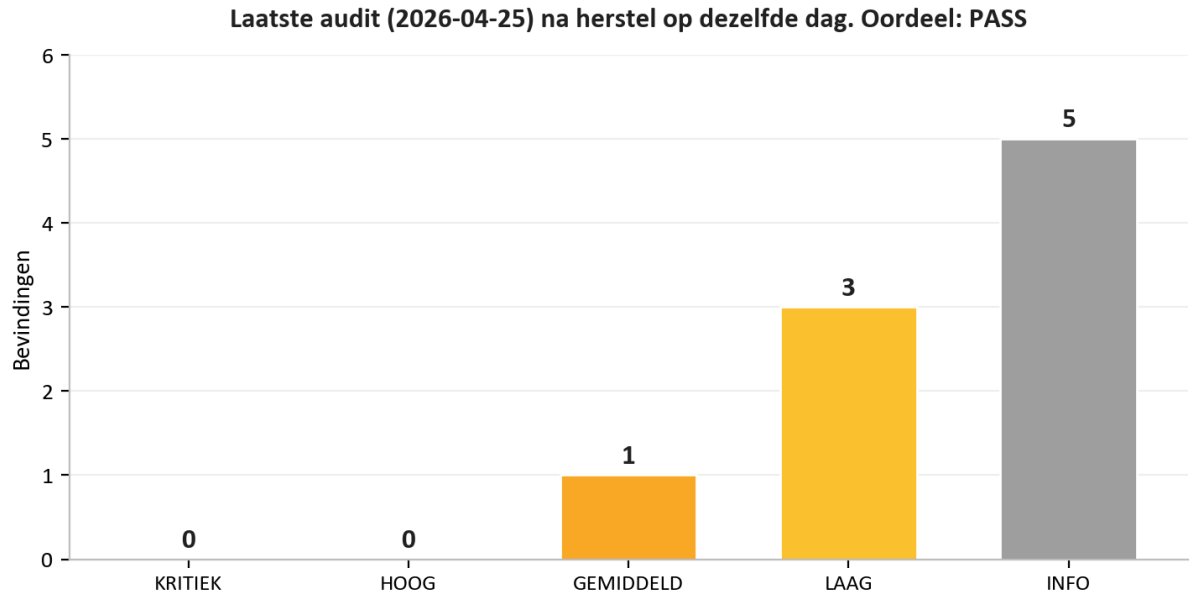
# 13. Resultaten van security-audits

Wij voeren terugkerende security-audits uit met behulp van een gestructureerde, herhaalbare methodologie voor penetratietests en werken elke audit uit in een gedateerd rapport met bevindingen per ernst, bewijs en remediatie. Dit zijn interne audits die door ons eigen securityproces worden uitgevoerd; formele certificering door derden van dezelfde controls staat op onze roadmap. Tussen eind maart en eind april 2026 hebben wij **seven such audits** voltooid over development en production.




Het resultaat dat voor een potentiële klant het belangrijkst is, is de consistentie: **over alle zeven audits waren er zero critical findings.** In de zeldzame gevallen waarin een issue met hogere ernst naar voren kwam, werd dit snel verholpen, vaak nog dezelfde dag, en opnieuw geverifieerd. De scoringsrubriek werd in deze periode bewust aangescherpt (de maximaal mogelijke score werd verhoogd naarmate wij meer te beoordelen categorieën toevoegden), daarom blijft de genormaliseerde scorelijn hoog, ook terwijl de lat hoger werd gelegd.

Onze meest recente audit, op 25 April 2026, illustreert hoe het proces in de praktijk werkt. Twee issues met hogere ernst werden geïdentificeerd, beide werden dezelfde dag opgelost en opnieuw geverifieerd, en de audit werd afgesloten met het oordeel **PASS** zonder exploit-ready issues die binnen het huidige threat model overbleven.



| Audit | Omgeving | Critical | Oordeel |
|---|---|---|---|
| 2026-03-28 | Development | 0 | Klaar voor production |
| 2026-04-04 | Development | 0 | Enterprise-ready |
| 2026-04-05 | Production | 0 | Enterprise-ready |
| 2026-04-20 | Development | 0 | Production-ready, notities |
| 2026-04-20 | Development | 0 | Pass met notities |
| 2026-04-21 | Production | 0 | Veilig, geen exploiteerbare bevindingen |
| 2026-04-25 | Development | 0 | Pass |

Het patroon over deze audits is het eerlijkste bewijs dat wij kunnen bieden: issues worden gevonden, omdat wij er hard naar zoeken, en zij worden snel gesloten, omdat het proces erop is ingericht om ze te sluiten. Een leverancier die nooit een bevinding rapporteert, is meestal een leverancier die niet zoekt.

---

# 14. Operationele weerbaarheid en gedeelde verantwoordelijkheid

## 14.1 Monitoring en logging

Applicatie- en platformtelemetrie stromen naar een gecentraliseerde log analytics-workspace en een applicatiemonitoringdienst, waardoor wij zicht hebben op beschikbaarheid en gedrag. Gevoelige handelingen zoals gegevensverwijdering, acceptatie van juridische overeenkomsten en AI-invocations worden vastgelegd in dedicated audit tables, zodat er een duurzaam register bestaat van wie wat met belangrijke gegevens heeft gedaan.

## 14.2 Backup en herstel

De beheerde database bewaart geautomatiseerde backups, en private storage wordt beschermd door soft-delete-retentie op zowel blobs als containers, zodat onopzettelijke of kwaadwillige verwijdering binnen het retentievenster kan worden hersteld. Kritieke infrastructuur heeft deletion locks om onopzettelijke teardown van production-resources te voorkomen.

## 14.3 Samenvatting van gedeelde verantwoordelijkheid

| Gebied | AI Interview Analyzer | Klant |
|---|---|---|
| Infrastructuur, netwerk, patching | Ja | - |
| Applicatiesecurity en AI-pipeline | Ja | - |
| Encryptie, secrets, dataresidentie | Ja | - |
| Beheer van gebruikers en rollen | Biedt de controls | Beheert gebruikers en rollen |
| Configuratie van retentiebeleid | Biedt de controls | Stelt het retentievenster in |
| Toestemming van kandidaten | Biedt de workflow | Zorgt dat deze wordt gebruikt |
| Sterke eindgebruikerscredentials en SSO | Ondersteunt SSO en beleid | Handhaaft intern beleid |

# 15. Threat model en OWASP-mapping

Wij ontwerpen tegen een concrete set adversaries: een externe aanvaller zonder credentials, een nieuwsgierige of kwaadwillige geauthenticeerde gebruiker van de ene organisatie die de gegevens van een andere organisatie probeert te bereiken, een gecompromitteerde dependency en een fout van een insider. De onderstaande tabel koppelt de breed gebruikte OWASP Top 10-risicocategorieën aan de specifieke controls die deze in dit platform mitigeren, en elk daarvan wordt getest door de tests die in Sectie 12 zijn beschreven.

| OWASP-risico | Hoe het platform dit mitigeert |
|---|---|
| Broken access control | Role-based access control op elk geprivilegieerd endpoint; scoping per organisatie; "not found" bij toegang tussen organisaties; remapping van identifiers; testmatrix tussen organisaties |
| Cryptographic failures | TLS 1.2+ in transit; AES-256 at rest; bcrypt password hashing; secrets in een managed vault |
| Injection | Uitsluitend ORM-gebaseerde geparametriseerde query's; strikte schemavalidatie; HTML-sanitization tijdens write time |
| Insecure design | Gelaagde defense in depth; threat modeling en architectuurreview in elke audit |
| Security misconfiguration | Infrastructure as code; default-deny network groups; security headers; uitgeschakelde shared storage keys; API-schema niet blootgesteld in production |
| Vulnerable components | Wekelijkse geautomatiseerde dependency-monitoring; dependency CVE-audits in periodieke review |
| Identification and authentication failures | Kortlevende tokens; rate-limited login; e-mailverificatie; SSO-ondersteuning; geen plaintext passwords |
| Software and data integrity failures | Vastgepinde, onveranderlijke pipelinestappen; code-signed desktopinstallers; webhook-signature-verificatie; tag-gated production deployments |
| Security logging and monitoring failures | Gecentraliseerde telemetrie; dedicated audit tables voor gevoelige handelingen |
| Server-side request forgery | Uitgaande calls beperkt tot vertrouwde endpoints; SSRF-probes in de harness voor penetratietests |

Deze mapping vormt de ruggengraat van ons assurance-argument: voor elke bekende aanvalsklasse is er een benoemde control, en voor elke benoemde control is er een test.

# 16. Vulnerability management en responsible disclosure

Security is nooit af, daarom draaien wij een continue lus van ontdekking en remediatie.

- **Ontdekking.** Kwetsbaarheden komen uit vier bronnen naar voren: de geautomatiseerde testsuite, de terugkerende audits van penetratietests, geautomatiseerde dependency-monitoring en meldingen van klanten of onderzoekers.
- **Triage.** Elke bevinding krijgt een ernst toegewezen (critical, high, medium, low of informational) met bewijs en een eigenaar voor remediatie, precies zoals vastgelegd in onze auditrapporten.
- **Doelstellingen voor remediatie.** Critical- en high-bevindingen krijgen prioriteit voor onmiddellijke remediatie; in onze auditgeschiedenis zijn bevindingen met hogere ernst doorgaans nog dezelfde dag opgelost en opnieuw geverifieerd. Medium- en lagere bevindingen worden ingepland in de reguliere onderhoudscadans.
- **Verificatie.** Fixes worden opnieuw getest, en waar relevant wordt een live controle uitgevoerd tegen de uitgerolde omgeving om te bevestigen dat het issue daadwerkelijk is gesloten, niet alleen in code.
- **Openbaarmaking.** Security-zorgen kunnen rechtstreeks aan ons worden gemeld. Wij bevestigen ontvangst van meldingen, onderzoeken deze en houden de melder op de hoogte tot en met de oplossing.

# 17. Compliance-mapping

## 17.1 GDPR

| GDPR-gebied | Implementatie in het platform |
|---|---|
| Rechtmatige grondslag (Art. 6) | Expliciete toestemming van de kandidaat vastgelegd vóór verwerking |
| Dataminimalisatie en opslagbeperking (Art. 5) | Alleen interviewrelevante gegevens worden verwerkt; configureerbare retentie met automatische verwijdering |
| Recht op verwijdering (Art. 17) | Verwijdering per eenheid van alle kandidaatgegevens, met gelogd bewijs van verwijdering |
| Rechten van betrokkenen (Art. 15 tot 20) | Inzage, verwijdering, dataportabiliteit en bezwaar worden ondersteund |
| Verplichtingen van verwerkers (Art. 28) | Data processing agreement geaccepteerd bij registratie en geversioneerd per organisatie |
| Beveiliging van verwerking (Art. 32) | Encryptie, toegangsbeheer, isolatie en continue tests zoals beschreven in dit document |
| Transparantie over sub-processors | Bekendgemaakt in de data processing agreement met voorafgaande kennisgeving van wijzigingen |

## 17.2 EU AI Act

Het platform wordt behandeld als een high-risk AI-systeem dat arbeidsbeslissingen ondersteunt, en wij onderhouden documentatie die in lijn is met de regelgeving, waaronder een transparency card, gebruikersdocumentatie en een declaration of conformity. De kernwaarborgen, menselijk toezicht, transparantie, op bewijs gebaseerde scoring en strikte scope-beperkingen op wat de AI evalueert, worden beschreven in Sectie 10. Wij blijven onze formele conformiteitsdocumentatie verder ontwikkelen naarmate de implementatietijdlijn van de regelgeving vordert.

## 17.3 Hostingcertificeringen

Het platform draait volledig op Microsoft Azure, waarvan de datacenters onafhankelijke certificeringen hebben, waaronder ISO 27001 en SOC 2. Deze certificeringen dekken de fysieke en platformlagen onder onze applicatie; de controls op applicatieniveau zijn degene die in dit document worden beschreven.

## 17.4 Register van sub-processors

| Sub-processor | Doel | Regio |
|---|---|---|
| Microsoft Azure | Hosting, AI- en spraakverwerking, storage, transactionele e-mail | EU (West Europe, Sweden Central) |
| Stripe | Verwerking van abonnementen en betalingen | EU (Ireland) |
| Fakturownia | Facturatie | EU (Poland) |
| ATS connector (optioneel) | Integratie met applicant tracking, alleen ingeschakeld op verzoek | EU |

# 18. Security-roadmap

Wij behandelen security als een programma van continue verbetering. Huidige initiatieven op onze roadmap omvatten het versterken van multi-factor-authentication-opties voor administratieve accounts, het uitbreiden van gecentraliseerde audit logging van datatoegang, het regelmatig verder aanscherpen van dependency currency, en het voortzetten van formele certificering door derden van de controls die in dit document zijn beschreven. Geen van deze punten is vandaag een gat dat klantgegevens blootstelt; elk punt is een verbetering van een reeds gelaagde posture.

# 19. Samenvatting

AI Interview Analyzer beschermt kandidaat- en klantgegevens via een gelaagde architectuur: een standaard privé netwerk zonder openbare datadiensten, sterke identiteit en isolatie per organisatie, applicatiecode die volledige kwetsbaarheidsklassen wegontwerpt, encryptie en EU-dataresidentie, en privacy-controls die zijn ingebouwd in het datamodel. Wat het platform onderscheidt, is het bewijs achter die claims. Met 3,171 geautomatiseerde tests, een herhaalbare methodologie voor live penetratietests, een dedicated AI-safety-programma en een trackrecord van zeven interne security-audits met zero critical findings, kunnen wij aantonen, en niet slechts zeggen, dat het platform veilig is.

# Appendix A: Catalogus van security-controls

Een beknopte referentie van primaire controls en het bewijs dat elk daarvan ondersteunt.

| Control | Mechanisme | Bewijs |
|---|---|---|
| Encryptie van transport | Alleen HTTPS, TLS 1.2+, HTTP doorgestuurd | Infrastructure as code; architectuuraudit |
| Encryptie at rest | AES-256-platformencryptie op storage en database | Platformconfiguratie; architectuuraudit |
| Bescherming van wachtwoorden | bcrypt met salt per wachtwoord | Source control; authenticatietests |
| Sessiebeheer | 30-minuten ondertekende tokens, intrekbare server-side refresh | Source control; authenticatietests |
| Autorisatie | Toegangsbeheer met vier rollen op geprivilegieerde endpoints | Role-enforcement-testsuite |
| Tenantisolatie | Query-scoping per organisatie; 404 bij cross-org | Testmatrix tussen organisaties |
| Beveiliging van API-keys | Gehashte opslag, scoped permissions, rate limits per key | API-key-testsuite |
| Bescherming tegen injectie | Uitsluitend ORM-gebaseerde geparametriseerde query's | Static analysis; injectietests |
| Bescherming tegen cross-site scripting | HTML-sanitization tijdens write time | HTML-sanitization-testsuite |
| Rate limiting | Duurzame, database-backed limiter op auth-endpoints | Rate-limit-tests; live burst-controles |
| Integriteit van webhooks | Verificatie van providersignatures op raw body | Webhook-testsuite |
| Secrets management | Managed vault, purge protection, managed identity | Infrastructure as code; architectuuraudit |
| Netwerkisolatie | Private endpoints; default-deny-segmentatie | Infrastructure as code; architectuuraudit |
| Gegevensverwijdering | Cascaderende verwijdering per eenheid met audit log | GDPR-deletion-testsuite |
| Supply chain | Vastgepinde pipelinestappen; wekelijkse dependency-monitoring | Pipelineconfiguratie; dependency-audit |

# Appendix B: Veelgestelde vragen voor security-reviewers

**Waar worden onze gegevens opgeslagen?** Volledig binnen de Europese Unie, op Microsoft Azure, in West Europe met AI-verwerking in EU-regio's. Kandidaatgegevens verlaten de EU nooit.

**Worden onze gegevens gebruikt om AI-modellen te trainen?** Nee. De AI-provider gebruikt klantgegevens niet voor training.

**Is de database bereikbaar vanaf het internet?** Nee. Openbare netwerktoegang is uitgeschakeld en de database is alleen bereikbaar via een private endpoint binnen het virtuele netwerk.

**Kan de ene klant de gegevens van een andere klant zien?** Nee. Elke query is scoped tot de organisatie van de aanroeper, toegang tussen organisaties retourneert "not found", en een geautomatiseerde matrix test deze isolatie continu.

**Hoe worden wachtwoorden opgeslagen?** Gehasht met bcrypt en een unieke salt per wachtwoord. Single sign-on met Microsoft en Google wordt ondersteund; in dat geval wordt geen wachtwoord opgeslagen.

**Ondersteunen jullie single sign-on?** Ja, via Microsoft en Google OAuth.

**Hoe lang zijn access tokens geldig?** Dertig minuten, gekoppeld aan een intrekbare server-side refresh-sessie die bij logout ongeldig wordt gemaakt.

**Hoe wordt toestemming van kandidaten afgehandeld?** Elke kandidaat ontvangt een unieke, eenmalige toestemmingslink en moet accepteren vóór enige opname of analyse. Toestemming wordt vastgelegd bij het specifieke wervingsproces.

**Hoe worden gegevens verwijderd?** Als één geheel dat het kandidaatrecord, interviews, transcripties, audio, documenten en vergelijkingen omvat, volgens een configureerbaar retentieschema, met een gelogd bewijs van verwijdering. Kandidaten kunnen ook rechtstreeks verwijdering verzoeken.

**Hebben jullie een data processing agreement?** Ja, geaccepteerd bij registratie en geversioneerd per organisatie, inclusief het register van sub-processors.

**Neemt de AI wervingsbeslissingen?** Nee. Zij biedt alleen beslissingsondersteuning; een mens beoordeelt elke output en neemt alle beslissingen.

**Hoe bewijzen jullie jullie security-claims?** Via 3,171 geautomatiseerde tests, waaronder een dedicated security-suite, een herhaalbare zesfasige methodologie voor penetratietests die tegen live omgevingen wordt uitgevoerd, een AI-safety-testprogramma en terugkerende schriftelijke auditrapporten.

**Wat gebeurt er wanneer jullie een kwetsbaarheid vinden?** Deze krijgt een ernst, bewijs en een eigenaar toegewezen, wordt volgens prioriteit verholpen, opnieuw geverifieerd inclusief live controles waar relevant, en vastgelegd in een auditrapport.

**Kunnen wij onze eigen penetratietest uitvoeren?** Security assessments kunnen via uw accountvertegenwoordiger worden geregeld met passende scope en planning.

---

# Appendix C: Glossary

| Term | Betekenis |
|---|---|
| AES-256 | Een sterke symmetrische encryptiestandaard die wordt gebruikt om gegevens at rest te beschermen |
| bcrypt | Een speciaal ontworpen password-hashing-functie met salting per wachtwoord |
| Managed identity | Een door het platform uitgegeven identiteit waarmee een dienst kan authenticeren zonder opgeslagen keys |
| Private endpoint | Een privénetwerkadres dat een cloudservice van het openbare internet afschermt |
| Network security group | Een set allow- en deny-regels die netwerkverkeer naar een subnet filtert |
| RBAC | Role-based access control, waarbij rechten worden verleend op basis van de rol van een gebruiker |
| IDOR | Insecure direct object reference, een flaw in toegangsbeheer waartegen het platform zich verdedigt |
| SSRF | Server-side request forgery, een aanvalsklasse die in onze penetratietests wordt onderzocht |
| Web application firewall | Een edge-control die kwaadwillig webverkeer filtert |
| Data processing agreement | Het contract dat regelt hoe een verwerker persoonsgegevens verwerkt namens een verwerkingsverantwoordelijke |

# Appendix D: Contact en documentbeheer

**AI Interview Analyzer Sp. z o.o.**

ul. Jedrusik 6/53, 01-748 Warszawa, Poland

NIP: 5253079974

Voor een security-review, een kopie van onze data processing agreement of onze conformiteitsdocumentatie voor de EU AI Act kunt u contact opnemen met uw accountvertegenwoordiger.

*Dit document beschrijft de security posture van de AI Interview Analyzer-dienst op de generatiedatum die in de footer wordt getoond. Het wordt verstrekt voor evaluatiedoeleinden en maakt geen deel uit van een contract. Specifieke contractuele security-verplichtingen zijn vastgelegd in de toepasselijke overeenkomst en data processing agreement.*