Sikkerheds-whitepaper

Enterprise Security Overview - AI Interview Analyzer

Udbyder:	AI Interview Analyzer Sp. z o.o.
Adresse:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Klassifikation:	PUBLIC
Dato:	24.06.2026

Contents

Sikkerheds-whitepaper

Udbyder: AI Interview Analyzer Sp. z o.o., Warszawa, Poland

Målgruppe: Sikkerheds-, IT- og indkøbsteams i enterprise-miljøer

Klassifikation: Offentlig

1. Resumé

AI Interview Analyzer er en enterprise-platform til rekruttering, der optager interviews med kandidatens udtrykkelige samtykke, transskriberer og strukturerer dem og producerer evidensbaseret evalueringsstøtte til rekrutteringsansvarlige. Fordi platformen håndterer kandidaters personoplysninger og understøtter ansættelsesprocesser, behandles sikkerhed og privatliv som primære designbegrænsninger, ikke som funktioner, der tilføjes senere.

Dette whitepaper beskriver i konkrete og verificerbare termer, hvordan vi beskytter kunde- og kandidatdata. Det er skrevet til de personer, der gennemgår leverandører: sikkerhedsingeniører, IT-administratorer, databeskyttelsesrådgivere og indkøb. Hver oplysning i dette dokument er trukket direkte fra vores egne engineering-systemer frem for fra marketingmateriale.

Det centrale budskab er enkelt: **vi hævder ikke blot, at platformen er sikker, vi tester løbende, at den er det.** Vores kodebase indeholder **3,171 automatiserede tests**, herunder en dedikeret sikkerhedssuite, der afprøver authentication, authorization, isolation på tværs af organisationer, forsvar mod injection og datasletning. Derudover kører vi et gentageligt penetrationstest-harness mod live-deployments og udarbejder skriftlige revisionsrapporter. På tværs af syv interne sikkerhedsrevisioner i marts og april 2026 registrerede vi **zero critical findings**, og vores seneste revision blev afsluttet med vurderingen **PASS**. (Formel tredjepartscertificering af disse kontroller er på vores roadmap; se Section 18.)

Sikkerhedskarakteristik	Resumé
Hosting	Microsoft Azure, kun EU-regioner
Netværksmodel	Private endpoints, standardmæssig deny-all netværkssegmentering, ingen offentlig database
Kryptering	AES-256 i hvile, TLS 1.2 eller højere under transit
Identitet	Kortlivede signerede tokens, bcrypt password hashing, SSO-understøttelse
Adgangskontrol	RBAC med streng isolation pr. organisation
Secrets	Centraliseret secrets vault med adgang via managed identity
Privatliv	Udtrykkeligt samtykke, konfigurerbar opbevaring, sletning som samlet enhed
Ansvarlig AI	Kun beslutningsstøtte, menneske altid i loopet
Sikkerhedsgaranti	3,171 automatiserede tests plus tilbagevendende penetrationstests og revisioner

1.1 Sådan læses dette dokument

Sektion 3 til 11 beskriver de kontroller, der beskytter data: arkitektur, netværk, identitet, applikation, databeskyttelse, privatliv og den sikre udviklingslivscyklus. Sektion 12 og 13 dækker vores særlige program for kontinuerlig testning og vores revisionshistorik. Sektion 14 til 17 dækker drift, threat modeling, sårbarhedshåndtering og compliance-mapping. Bilagene indeholder et kontrolkatalog, en FAQ til reviewere og en ordliste, som et sikkerhedsteam kan bruge direkte under en vurdering.

2. Dokumentets omfang og tilgang

2.1 Hvad dette dokument dækker

Dette whitepaper dækker sikkerhedsarkitekturen og praksisserne for AI Interview Analyzer-tjenesten: hostingmiljøet, netværksdesignet, identitets- og adgangsstyring, kontroller på applikationsniveau, databeskyttelse, privatliv og regulatorisk tilpasning, den sikre udviklingslivscyklus og vores program for kontinuerlig sikkerhedstestning.

2.2 Hvad der gør det verificerbart

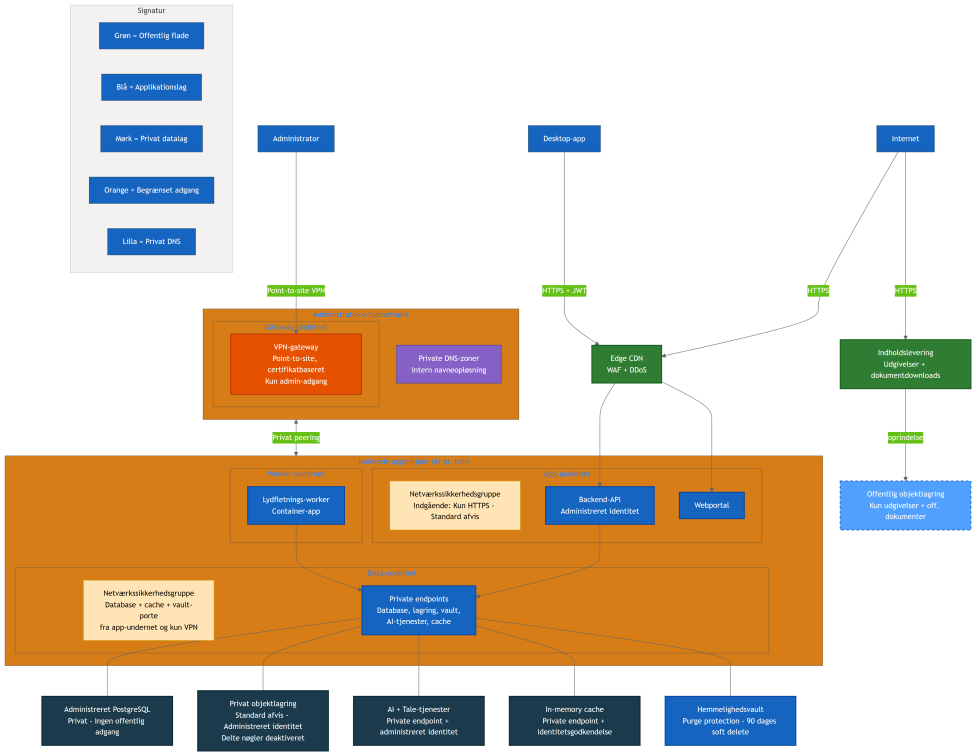
Leverandørers sikkerhedspåstande er nemme at skrive og svære at stole på. Vi har derfor knyttet hver større påstand i dette dokument til noget konkret og målbart i vores engineering-systemer: en kontrol implementeret i kode, en test der beviser, at kontrollen virker, en infrastrukturdefinition der håndhæver den, eller en revisionsrapport der registrerer en dokumenteret kontrol. Hvor en kontrol er en del af vores fremadrettede roadmap frem for leveret i dag, siger vi det udtrykkeligt. Vi vil hellere underkommunikere og blive betroet end overkommunikere og blive afsløret.

2.3 Delt ansvar

Platformen leveres som software as a service. Vi driver infrastrukturen, applikationen, AI-pipelinen og datahåndteringen. Kunden er ansvarlig for at administrere sine egne brugerkonti og roller, konfigurere databevaringsperioder, så de matcher interne politikker, og sikre, at kandidatens samtykke indhentes gennem det samtykkeflow, som platformen stiller til rådighed. Section 14 beskriver denne opdeling mere detaljeret.

3. Overblik over sikkerhedsarkitektur

Platformen er bygget som et lille antal samarbejdende tjenester snarere end som én enkelt monolit. En desktop-applikation og en webportal fungerer som klienter. Et centralt backend API ejer al persistence, authentication, billing, AI-pipelinen, samtykke, e-mail, filhåndtering og dashboards. En worker til lydsammenfletning behandler optagelser asynkront. AI følsom tilstand ligger bag backend API'et; klienter taler aldrig direkte med databasen, storage eller AI-tjenester.



Diagrammet ovenfor viser produktionstopologien med ressource-navne bevidst generaliseret. Tre principper er synlige i den:

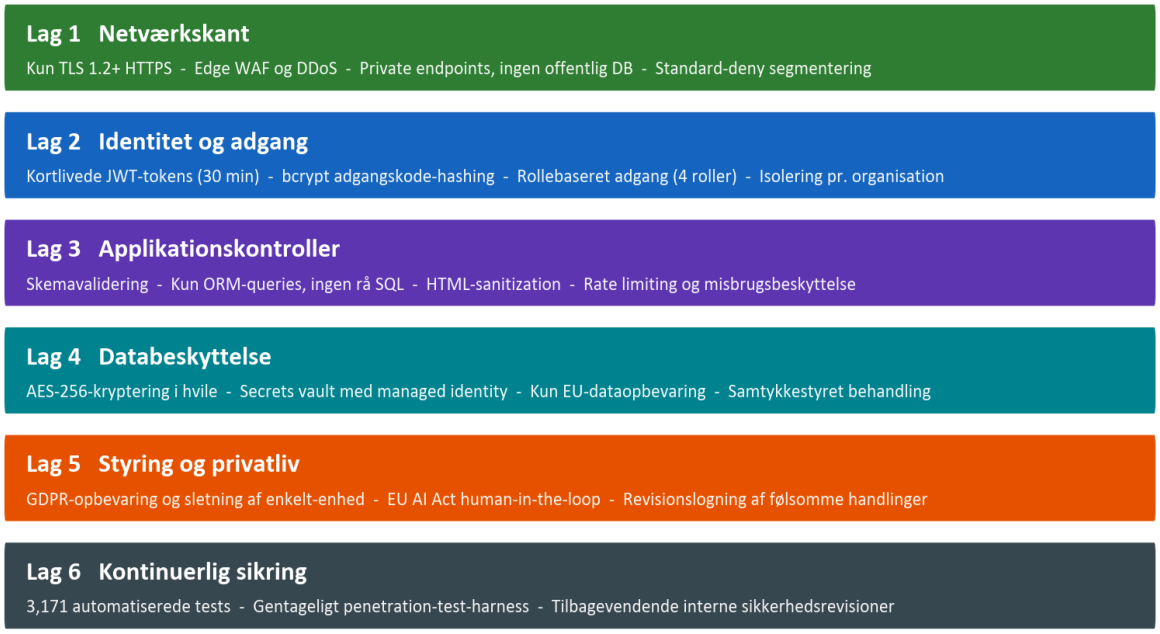
- **Ingen direkte eksponering af datatjenester.** Databasen, privat object storage, AI-tjenester og cache har offentlig netværksadgang deaktiveret og kan kun nås gennem private endpoints inde i et isoleret virtuelt netværk. Secrets vault nås af applikationen via et private endpoint og er yderligere beskyttet af platform identity authentication og least-privilege-adgangspolitikker, så enhver adgang kræver en gyldig, autoriseret identitet uanset netværkssti.
- **En adskilt offentlig flade.** Den eneste offentlige object storage indeholder release-downloads og offentlige dokumenter. Den indeholder aldrig kandidatdata. Kundevendt applikationstrafik passerer gennem et edge-lag, der leverer web application firewall, distributed-denial-of-service-beskyttelse og content delivery.
- **Administrativ adgang er kontrolleret.** Operatører når interne ressourcer kun gennem en certifikatbaseret point-to-site VPN ind i et management hub-netværk, ikke over det offentlige internet.

Hvert deployment-stadie (udvikling og produktion) er et fuldt isoleret miljø med eget netværk, egne storage accounts, database og secrets. Kunders produktionsdata er aldrig til stede i lavere miljøer. Et delt management hub indeholder kun VPN gateway og private DNS, privat peered til hvert miljø.

4. Defense in Depth

Ingen enkeltkontrol betros at stoppe ethvert angreb. Platformen lægger uafhængige kontroller i lag, så fejl i ét lag ikke eksponerer data. Lagene nedenfor er hver især implementeret og, som beskrevet i Section 12, testet individuelt.

Lagdelt sikkerhedsmodel: uafhængige kontroller på hvert niveau



Lag	Repræsentative kontroller
Netværksedge	Kun TLS-transport, edge WAF og DDoS-beskyttelse, private endpoints, standardmæssig deny-all-segmentering
Identitet og adgang	Kortlivede signerede tokens, bcrypt hashing, RBAC, isolation pr. organisation
Applikation	Schemavalidering på alle input, kun ORM-baseret dataadgang, output encoding, rate limiting
Databeskyttelse	Kryptering i hvile, secrets vault med managed identity, EU-dataresidens, behandling styret af samtykke
Governance og privatliv	Konfigurerbar opbevaring, sletning som samlet enhed, human-in-the-loop AI, audit logging
Kontinuerlig sikkerhedsgaranti	Automatiseret testsuite, gentagelige penetrationstests, tilbagevendende interne sikkerhedsrevisioner

Resten af dette dokument gennemgår hvert lag efter tur og beskriver derefter, hvordan vi løbende beviser, at lagene holder.

5. Netværkssikkerhed

5.1 Privat som standard

Datalaget er privat af konstruktion. Den administrerede PostgreSQL-database har offentlig netværksadgang deaktiveret og kan kun nås gennem et private endpoint. Privat object storage er konfigureret til som standard at afvise netværksadgang, deaktiverer shared access keys fuldstændigt og er kun tilgængelig via managed identity fra applikationssubnettet. Cache, AI-tjenester og secrets vault nås ligeledes gennem private endpoints med private DNS-opløsning.

I praksis betyder dette, at der ikke findes nogen internetvendt connection string til databasen og ingen offentlig storage-URL til kandidatens lydfiler: databasen og privat storage har offentlig netværksadgang direkte deaktiveret. Secrets vault nås af applikationen via et private endpoint og er beskyttet af platform identity authentication og least-privilege-adgangspolitikker, hvor applikationsidentiteter kun får read-only-adgang til de secrets, de har brug for, så secrets ikke kan hentes uden en gyldig, autoriseret identitet. Angrebsfladen, som en ekstern modstander overhovedet kan berøre, er begrænset til applikationens HTTPS-endpoints bag edge-laget.

5.2 Netværkssegmentering

Hvert miljø er opdelt i separate subnets for applikationslaget, datalaget og den asynkrone worker. Hvert subnet styres af en network security group, hvis sidste regel afviser al indgående trafik. Applikationssubnettet accepterer kun indgående HTTPS. Datasubnettet accepterer kun de specifikke porte til database, cache og vault, og kun fra applikationssubnettet eller den administrative VPN. Dette betyder, at selv en angriber, som på en eller anden måde nåede applikationslaget, ikke frit kan pivotere til datalaget; de eneste tilladte stier er dem, applikationen legitimt bruger.

5.3 Edge-laget

Offentlig applikationstrafik frontes af et edge-lag, der leverer web application firewall, DDoS-beskyttelse og et content delivery network. Downloads af releases og dokumenter serveres fra en dedikeret offentlig storage account gennem en content-delivery front door, fuldstændigt adskilt fra den private storage, der indeholder kandidatdata. De to storage-planer blandes aldrig: en fejlkonfiguration på den offentlige plan kan ikke eksponere private kandidatdata, fordi de ligger i forskellige accounts med forskellige netværksregler.

5.4 Administrativ adgang

Der findes ikke noget offentligt administrativt endpoint ind til det private netværk. Operatører forbinder gennem en point-to-site VPN gateway, der bruger certifikatbaseret authentication. Administrativ adgang til database og cache er kun mulig inde fra denne tunnel, da disse tjenester har offentlig netværksadgang deaktiveret. Dette holder den daglige drift helt væk fra det offentlige internet.

6. Identitets- og adgangsstyring

6.1 Authentication

Brugersessioner etableres med et signeret access token, der er gyldigt i tredive minutter, parret med et separat, opaque, server-side refresh token. Access tokens verificeres ved hver request, og brugeren valideres igen mod databasen (herunder kontrol af aktiv konto) i stedet for alene at stole på indholdet i tokenet. Logout tilbagekalder server-side refresh-sessionen øjeblikkeligt, så et stjålet refresh token ikke kan overleve et logout.

Passwords lagres aldrig i klartekst. De hashes med bcrypt ved brug af et unikt salt pr. password. For organisationer, der foretrækker single sign-on, understøtter platformen OAuth-login med Microsoft og Google, og i så fald opbevares der slet ikke noget password.

Ejerskab af e-mail verificeres gennem et engangsverificeringslink med tidsbegrænsning, før en selvregistreret konto behandles som verificeret, og genudsendelser af verifikationsmails er rate limited for at forhindre misbrug.

6.2 Rollebaseret adgangskontrol

Authorization håndhæves gennem en rollemodel med fire roller med stigende privilegier: interviewer, hiring manager, recruiter og administrator. Adgang til privilegerede handlinger håndhæves af server-side dependencies, der kontrollerer både rollen og verificeringsstatus for den kaldende part. Disse rollekontroller beskytter langt over hundrede forskellige API-operationer.

Rolle	Typiske kapabiliteter
Interviewer	Gennemfører tildelte interviews; ser kun interviews, der er tildelt vedkommende
Hiring manager	Administrerer rekrutteringer, som vedkommende ejer eller er medlem af
Recruiter	Fuld rekrutterings- og kandidatstyring inden for organisationen
Administrator	Organisationsindstillinger, billing, administration af brugere og API keys

Ud over grove rollekontroller anvender platformen regler for synlighed på dataniveau. Hiring managers ser kun de rekrutteringer, de har oprettet eller er medlem af; interviewere ser kun de interviews, der er tildelt dem. Privilegier håndhæves derfor både på niveauet "hvilken handling" og på niveauet "hvilke poster".

6.3 Isolation pr. organisation

Platformen er multi-tenant, og tenant-isolation behandles som en førsteklasses sikkerhedskontrol. Hver authenticated identitet bærer en organisationsidentifikator, og dataforespørgsler scopes til denne organisation. Når en bruger anmoder om en post, der tilhører en anden organisation, returnerer platformen et "not found"-svar i stedet for at afsløre, at posten eksisterer. Interne databaseidentifikatorer eksponeres aldrig på linjen; API'et præsenterer display-identifikatorer og remapper dem pr. request, hvilket eliminerer en almindelig klasse af angreb med enumeration på tværs af tenants.

Dette er ikke kun en designintention. Som beskrevet i Section 12 kører vores automatiserede suite en stor matrix på tværs af organisationer, der forsøger at nå én organisations data med en anden organisations credentials og fastslår, at hvert sådant forsøg fejler.

6.4 Programmatisk adgang

Til integrationer kan organisationer på kvalificerede planer udstede API keys. Keys bruger et genkendeligt præfiks, indeholder 128 bits entropi og lagres kun som en hash; den rå nøgle vises én gang ved oprettelse og aldrig igen. Hver key bærer et udtrykkeligt permission scope (read, write eller ATS integration), kan begrænses til specifikke kildenetværk, kan tilbagekaldes øjeblikkeligt og er underlagt rate limits pr. key afledt af organisationens plan-niveau. Key-verifikation bruger en timing-safe sammenligning for at undgå informationslækage gennem svartider.

7. Applikationssikkerhed

Applikationen er skrevet til at eliminere hele kategorier af sårbarheder snarere end at patche dem fra sag til sag.

• **Injection.** Al databaseadgang går gennem en object-relational mapper med parameteriserede queries. Kodebasen indeholder ingen rå string-formateret SQL. Dette eliminerer strukturelt SQL injection.

• **Inputvalidering.** Hver request body valideres mod et strengt schema, før den når forretningslogikken. For store payloads afvises, og liste-endpoints er paginerede for at begrænse ressourceforbrug.

• **Output encoding og cross-site scripting.** Brugerleveret og AI-genereret tekst behandles som utroværdig. Hvor indhold skal rendres som HTML, passerer det gennem en sanitizer med allow-list ved skrivning, og en dedikeret testsuite bekræfter, at script-tags, event handlers og javascript-URL'er fjernes.

• **Mass assignment.** Update-operationer bruger eksplicitte schemaer, der udelukker privilegerede felter såsom rolle, organisation og credit balance, så en klient ikke kan eskalere privilegier ved at poste ekstra felter.

• **Rate limiting.** Authentication- og misbrugsudsatte endpoints er rate limited ved hjælp af en holdbar, database-backed limiter, der overlever restarts og fungerer korrekt på tværs af flere applikationsinstanser. Login, registrering, password reset og genudsendelse af verifikation har hver deres egne grænser. Klientens IP-opløsning er hærdet mod spoofing af forwarding headers.

• **Webhooks.** Indgående webhooks fra betalings- og e-mailudbydere verificeres mod udbyderens signaturer på den rå request body, før de behandles.

• **Filuploads.** Uploads har størrelsesgrænser, valideres, lagres under genererede identifikatorer snarere end brugersupplerede navne og begrænses pr. request og pr. organisation.

• **Sikkerhedsheaders.** I produktion bærer svar strict transport security, content-type- og frame-options, en referrer policy og en restriktiv permissions policy samt undertrykker server- og framework-bannere.

8. Databeskyttelse

8.1 Kryptering

Alle data er krypteret i hvile ved brug af AES-256 gennem Azure-platformens krypteringslag for storage og database. AI netværkstrafik serveres udelukkende over HTTPS ved brug af TLS 1.2 eller højere; klartekst HTTP omdirigeres til HTTPS på alle lag. I produktion udsender API'et og webportalen strict transport security-headers sammen med et sæt hardening-headers og undertrykker versionsbannere for server og framework.

8.2 Secrets Management

Applikations-secrets opbevares i en centraliseret secrets vault med purge protection aktiveret og et soft-delete-vindue på halvfems dage. Applikationer autentificerer til Azure-ressourcer ved brug af system-assigned managed identities snarere end langlivede nøgler; eksempelvis har privat storage shared access keys fuldstændigt deaktiveret, så adgang kun er mulig gennem identitetsbaserede rolle-tildelinger scoped til den enkelte ressource. Vault-adgangspolitikker giver applikationsprincipaler read-only-adgang til de specifikke secrets, de har brug for, i overensstemmelse med least privilege.

8.3 Dataresidens

Alle kunde- og kandidatdata lagres og behandles inden for Den Europæiske Union. Applikationshosting, databasen, storage, cache og secrets ligger i West Europe, og AI-behandling kører i EU-regioner. AI-udbyderen bruger ikke kundedata til at træne sine modeller.

8.4 Livsforløbet for et enkelt interview

Den klareste måde at forstå databeskyttelseskontrollerne på er at følge ét interview fra ende til anden. Samtykke indhentes og registreres, før noget behandles. Uploaden krypteres under transit. Transskription og analyse kører inden for EU-datacentre. Resultater skrives til krypteret storage. Hver post styres derefter af ét samlet retention-ur, som ender i en logført, kaskaderende sletning. På ethvert tidspunkt kan kandidatrettigheder såsom tilbagetrækning, sletning, adgang eller portabilitet afbryde dette flow.

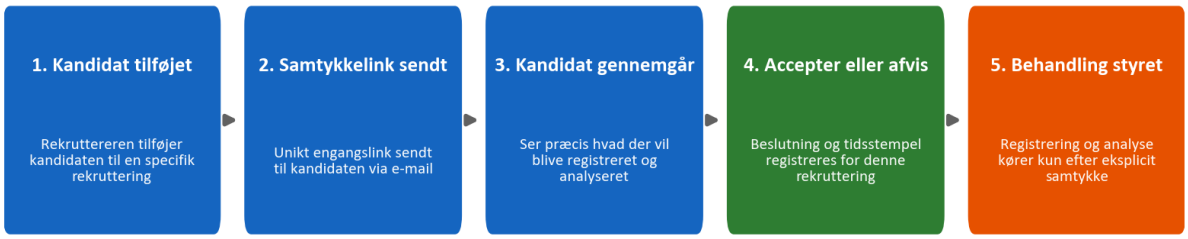
9. Privacy by Design og GDPR

Privatliv er indbygget i datamodellen og workflowet, ikke blot påført gennem politik alene.

9.1 Samtykke

Intet interview optages eller analyseres uden kandidatens udtrykkelige samtykke. Når en kandidat føjes til en rekruttering, udsender platformen et unikt samtykkelink til engangsbrug via e-mail. Kandidaten gennemgår, hvad der vil ske, og accepterer eller afslår. Samtykkestatus, herunder tidspunktet for svaret, registreres mod den specifikke rekruttering, så samtykke altid er scoped til en konkret ansættelsesproces frem for givet globalt.

Kandidatsamtykke: eksplicit og registreret før enhver behandling



9.2 Opbevaring og sletning

Dataopbevaring kan konfigureres pr. organisation, med en standard på tolv måneder og et konfigurerbart minimum på tredive dage, og kan tilsidesættes pr. kandidat. Der er ét samlet retention-ur for en kandidats data, ikke en separat timer pr. artefakt. Uret starter, når en ansættelsesbeslutning registreres. Før data udløber, sender platformen en advarsel (som standard omkring femten dage før) og tilbyder en forlængelse med ét klik. Når data slettes, slettes de som én samlet enhed: kandidatposten, interviews, transskripter, lydoptagelser, dokumenter og sammenligninger fjernes alle sammen, og sletningen registreres i en audit log. Der er ingen delvise eller forældreløse rester.

Livscyklussen nedenfor viser dette ene ur, og hvordan det konvergerer mod én kaskaderende sletning med et logført bevis på sletning.

Dataopbevaring: ét ur pr. kandidat, sletning af enkelt-enhed

9.3 Registreredes rettigheder og sub-processors

Platformen understøtter de registreredes rettigheder, som kræves efter GDPR, herunder adgang, sletning, portabilitet, indsigelse og forklaring. Behandling udføres under en data processing agreement, som kunder accepterer ved registrering, og som versionsstyres pr. organisation. Vores sub-processors og deres roller, alle inden for EU eller under passende

sikkerhedsforanstaltninger, oplyses i denne aftale, og kunder modtager forhåndsvarsel om enhver ændring. Section 17 indeholder registeret over sub-processors og artikel-for-artikel compliance-mappingen.

10. Ansvarlig AI og EU AI Act

Platformen falder inden for højrisikokategorien i EU AI Act, fordi den understøtter ansættelsesbeslutninger, og vi tager denne klassifikation alvorligt.

Den definerende regel for produktet er, at **AI'en er beslutningsstøtte, ikke en beslutningstager.** Systemet accepterer eller afviser aldrig automatisk en kandidat. Det transskriberer tale, strukturerer spørgsmål og svar, scorer svar mod kriterier, som den rekrutteringsansvarlige har defineret, og udarbejder feedback, og et menneske gennemgår hvert output, før det bruges. Dette holder et menneske fast i loopet.

Lige så vigtigt er det, hvad AI'en ikke gør. Den vurderer ikke personlighed, "cultural fit", følelsesmæssig tilstand, tonefald, accent, køn, alder, etnicitet, udseende eller kropssprog. Scoring forankres i evidens fra transskriptet og i recruiter-definerede kriterier, og kandidatnavne udelukkes fra evalueringsinputtet for at reducere bias. Vi offentliggør et transparency card, brugerdokumentation og en declaration of conformity, der beskriver systemet, dets begrænsninger og dets sikkerhedsforanstaltninger.

Kontrol for ansvarlig AI	Sådan fungerer den
Human in the loop	Hver score og hvert stykke feedback gennemgås af en recruiter før brug
Ingen automatiserede beslutninger	Systemet auto-accepterer eller auto-afviser aldrig en kandidat
Evidensbaseret scoring	Scores refererer til understøttende evidens fra transskriptet
Anti-bias-design	Navne udelukkes fra evaluering; substans scores over stil
Omfangsbegrænsninger	Personlighed, følelser, accent og beskyttede karakteristika vurderes aldrig
Sikkerhed for kandidatfeedback	Privat kandidatfeedback passerer et sikkerheds-autoværn for generation og validering

Disse begrænsninger er ikke kun beskrevet i dokumentation; de er kodet ind i AI prompt-laget og afprøves af et dedikeret AI-sikkerhedstestprogram beskrevet i Section 12.3.

11. Sikker udviklingslivscyklus

Sikkerhed håndhæves i den måde, vi bygger og leverer software på, ikke kun i det kørende system.

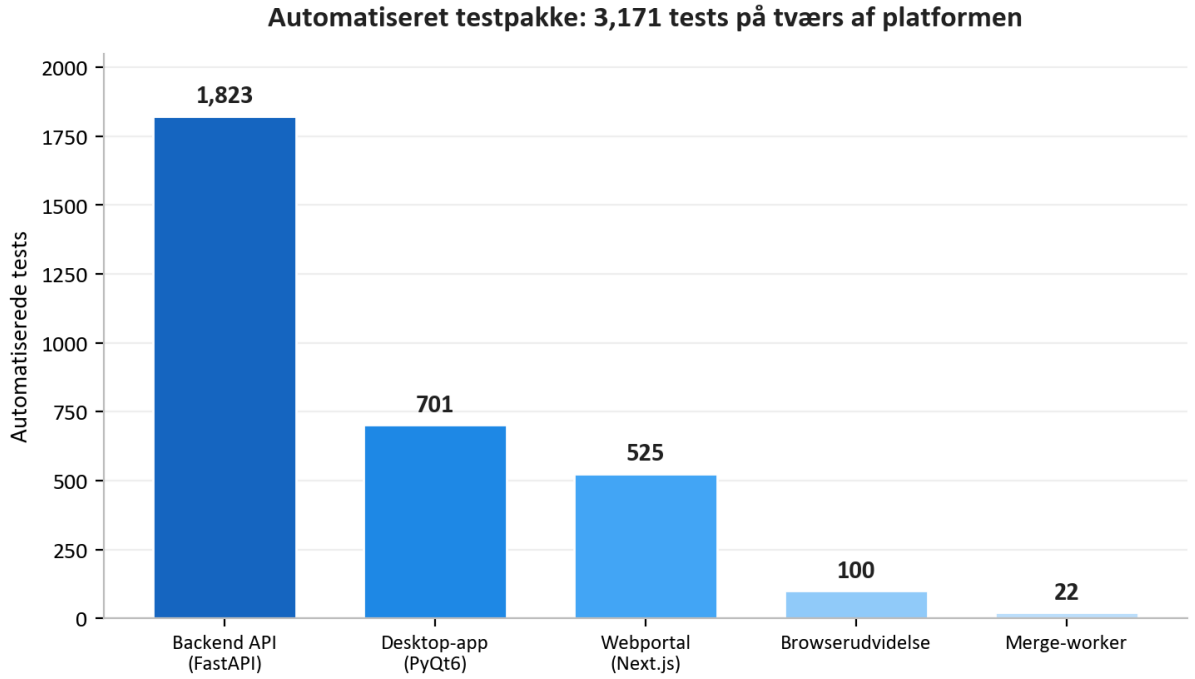
- **Miljøadskillelse.** Udvikling og produktion er fuldstændigt adskilt, hver med sin egen infrastruktur, storage accounts, database, secrets og subdomæner. Der er ingen delt tilstand.
- **Infrastructure as code.** Hele cloud-miljøet er defineret som kode og reviewet som kode, hvilket gør sikkerhedspositionen auditerbar og reproducerbar. En reviewer kan læse præcis, hvilke porte der er åbne, hvilke ressourcer der er private, og hvilke identiteter der har hvilke tilladelser.
- **Fastlåste, kontrollerede deployments.** Hvert trin i continuous-integration-pipelinen er fastlåst til en præcis, uforanderlig version. Produktionsdeployments er tag-baserede, køres kun gennem den beskyttede produktionspipeline og er kontrolleret bag påkrævet godkendelse. Den automatiserede testsuite fungerer som release-gate: et deployment kan ikke leveres, hvis tests fejler.
- **Afhængighedshygiejne.** Automatiseret overvågning af afhængigheder foreslår opdateringer ugentligt på tværs af backend, desktop, web, infrastruktur og pipeline-definitioner, og dependency audits er en del af vores periodiske sikkerhedsreview.
- **Signerede artefakter.** Desktop-installationsprogrammer er code-signed, så kunder kan verificere, at den software, de installerer, faktisk kommer fra os.
- **Disciplin omkring secrets.** Secrets ligger i vault og i beskyttede pipeline-secrets, aldrig i kildekode.

12. Kontinuerlig sikkerhedstestning

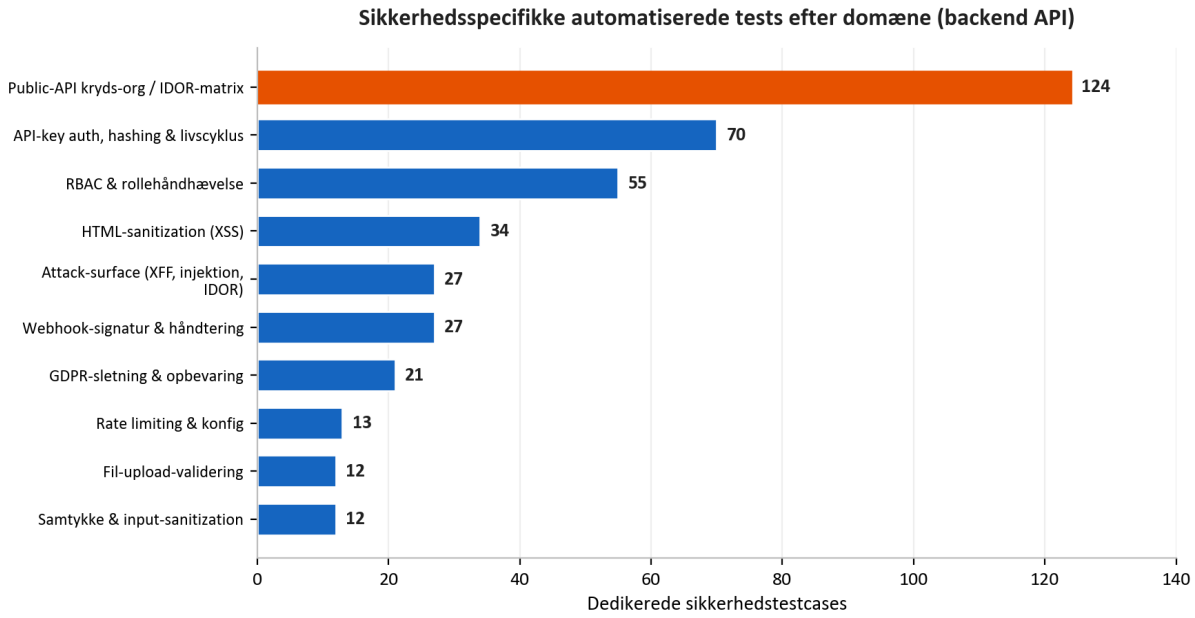
Dette er kernen i vores sikkerhedsgaranti og den del, de fleste leverandører ikke kan fremvise. Vi behandler sikkerhed som noget, der løbende skal måles med eksekverbare kontroller, snarere end noget, der hævdes én gang.

12.1 Den automatiserede testsuite

Platformen er dækket af **3,171 automatiserede tests**, der spænder over backend API, desktop-applikationen, webportalen, browserudvidelsen og workeren til lydsammenfletning.



Dette er ikke kun funktionelle tests. En væsentlig, dedikeret sikkerhedssuite afprøver de kontroller, der er beskrevet tidligere i dette dokument. Diagrammet nedenfor opdeler de sikkerhedsspecifikke tests i backend API'et efter domæne.



Blandt mange andre elementer indeholder denne suite en stor matrix for det offentlige API, som kører hvert endpoint som en legitim bruger, som organisationens egen API key og som en konkurrerende organisations API key og fastslår, at hvert forsøg på adgang på tværs af organisationer blokeres. Den indeholder dusinvis af adversarial tests af angrebsfladen for spoofing af forwarding headers, header injection og lækage af identifikatorer, en fokuseret HTML-sanitization-suite for cross-site scripting, rolle-håndhævelsestests for hele rollemodellen og tests, der beviser, at kandidatdata reelt slettes som en samlet enhed. Fordi disse tests kører som release-gate, vil en regression, der svækkede nogen af disse kontroller, stoppe releasen frem for at nå kunderne.

12.2 Live penetrationstest

Automatiserede unit tests beviser, at kontroller opfører sig korrekt isoleret set. For at bevise, at de holder samlet i et reelt deployment, vedligeholder vi en gentagelig penetrationstestmetodologi, der kører virkelige angrebsscripts mod et live-miljø. Den er organiseret i seks faser:

Fase	Fokus	Eksempler på hvad der afprøves
1. Statisk analyse	Kildekode	Secrets, injection-mønstre, farlige funktioner, manglende auth, usikker HTML
2. Arkitekturreview	Infrastruktur	Private endpoints, segmentering, TLS, konfiguration af secrets
3. Analyse af angrebsvektorer	Kildekontrol og cloud	Branch protection, identity scope, offentlig eksponering
4. Live penetrationstest	Kørende miljø	Uautentificeret probing, adgang på tværs af organisationer, injection, token tampering, SSRF, rate-limit bursts
5. Enterprise-scoring	Modenhed	Seksten sikkerhedskategorier scoret mod en enterprise-baseline
6. Afhængigheder og supply chain	Tredjepartsrisiko	Dependency CVE-audit, fastlåste pipeline actions, integritet af lock-filer

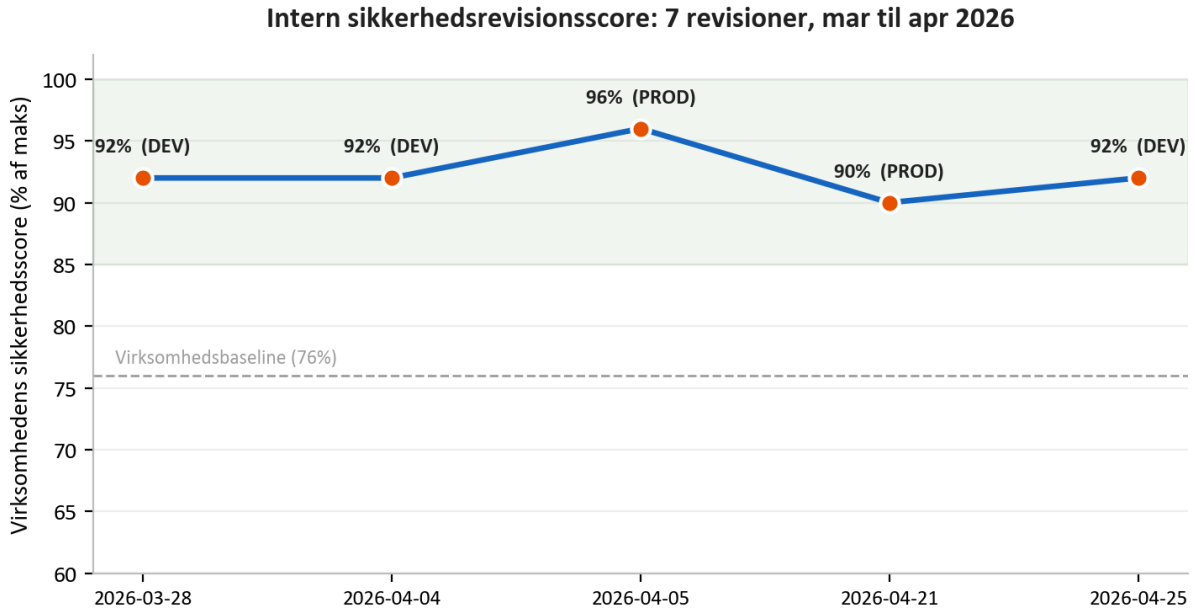
Fase 4 er reel adversarial testning mod et deployed system, ikke en tjekliste. Den sonderer beskyttede endpoints uden credentials og bekræfter, at de afviser adgang; den registrerer to organisationer og forsøger at nå den ene organisations poster med den andens konto; den injicerer cross-site-scripting- og server-side-template-payloads og bekræfter, at de neutraliseres; den manipulerer authentication tokens og bekræfter, at de afvises; den forsøger server-side request forgery mod cloud-metadata-endpoints; og den laver bursts mod authentication-endpoints for at bekræfte, at rate limiting faktisk udløses i live-miljøet, ikke kun i teorien.

12.3 Sikkerhedstest af kandidatfeedback

Fordi platformen kan generere privat udviklingsfeedback til kandidater, kører vi et separat adversarial sikkerhedsprogram mod denne funktion. Det fodrer bevidst systemet med hårde og fjendtlige recruiter-noter og bekræfter, at det kandidatvendte output aldrig indeholder vulgaritet, aldrig afslører eller tilskriver en recruiters identitet eller private mening og aldrig anvender dømmende personlighedsetiketter. Dette beskytter både kandidaten, som skal modtage konstruktiv og respektfuld feedback, og kunden, som aldrig bør få en intern vurdering lækket udad.

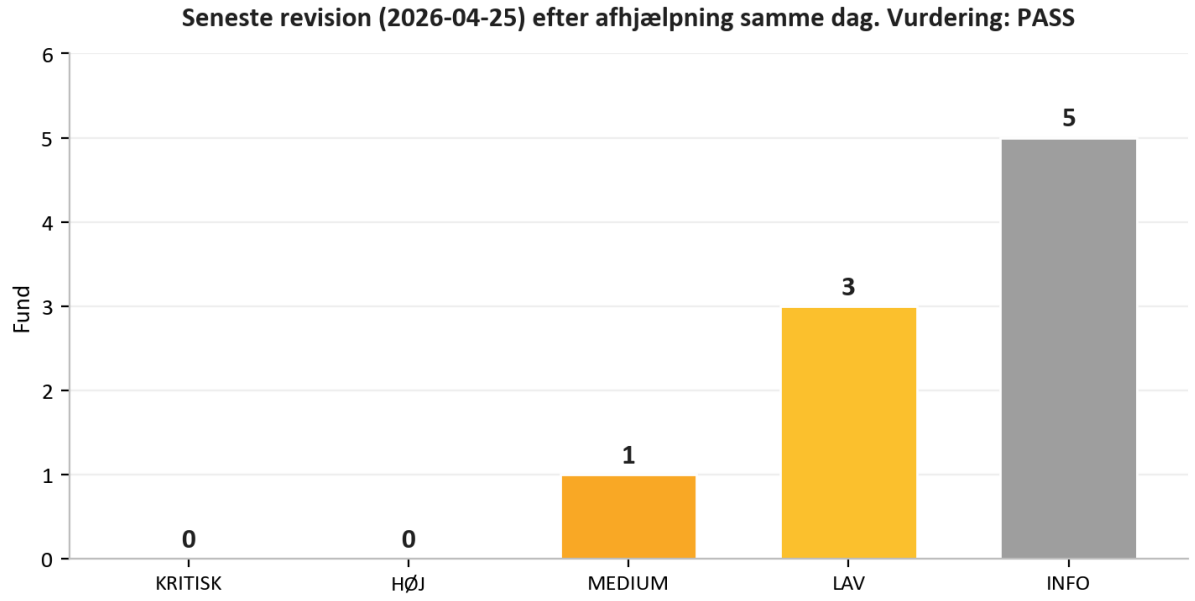
13. Resultater af sikkerhedsrevisioner

Vi udfører tilbagevendende sikkerhedsrevisioner ved hjælp af en struktureret, gentagelig penetrationstestmetodologi og dokumenterer hver revision som en dateret rapport med severity-rated findings, evidens og afhjælpning. Dette er interne revisioner udført af vores egen sikkerhedsproces; formel tredjepartscertificering af de samme kontroller er på vores roadmap. Mellem slutningen af marts og slutningen af april 2026 gennemførte vi **seven such audits** på tværs af udvikling og produktion.



Det resultat, der betyder mest for en potentiel kunde, er konsistensen: **across all seven audits there were zero critical findings.** Ved de sjældne lejligheder, hvor en mere alvorlig problemstilling opstod, blev den afhjulpet hurtigt, ofte samme dag, og reverificeret. Scoringsrubrikken blev bevidst strammet i denne periode (den maksimalt mulige score blev hævet, efterhånden som vi tilføjede flere kategorier at vurdere), hvilket er grunden til, at den normaliserede scorelinje forbliver høj, selv om barren blev hævet.

Vores seneste revision, den 25 April 2026, illustrerer, hvordan processen fungerer i praksis. To mere alvorlige problemer blev identificeret, begge blev rettet og reverificeret samme dag, og revisionen blev afsluttet med vurderingen **PASS** uden exploit-klare problemer tilbage i den aktuelle threat model.



Revision	Miljø	Kritisk	Vurdering
2026-03-28	Udvikling	0	Klar til produktion
2026-04-04	Udvikling	0	Enterprise-klar
2026-04-05	Produktion	0	Enterprise-klar
2026-04-20	Udvikling	0	Klar til produktion, noter
2026-04-20	Udvikling	0	Bestået med noter
2026-04-21	Produktion	0	Sikker, ingen udnyttelige fund
2026-04-25	Udvikling	0	Bestået

Mønstret på tværs af disse revisioner er det mest ærlige bevis, vi kan tilbyde: problemer findes, fordi vi leder grundigt efter dem, og de lukkes hurtigt, fordi processen er bygget til at lukke dem. En leverandør, der aldrig rapporterer et fund, er som regel en leverandør, der ikke leder.

---

14. Operationel robusthed og delt ansvar

14.1 Overvågning og logging

Applikations- og platformtelemetri flyder ind i et centraliseret log analytics-workspace og en application-monitoring-tjeneste, hvilket giver os synlighed i tilgængelighed og adfærd. Følsomme handlinger såsom datasletning, accept af juridiske aftaler og AI-kald registreres i dedikerede audit-tabeller, så der findes en holdbar registrering af, hvem der gjorde hvad ved vigtige data.

14.2 Backup og gendannelse

Den administrerede database opbevarer automatiserede backups, og privat storage er beskyttet af soft-delete retention på både blobs og containere, så utilsigtet eller ondsindet sletning kan gendannes inden for retention-vinduet. Kritisk infrastruktur har deletion locks for at forhindre utilsigtet nedtagning af produktionsressourcer.

14.3 Resumé af delt ansvar

Område	AI Interview Analyzer	Kunde
Infrastruktur, netværk, patching	Ja	-
Applikationssikkerhed og AI-pipeline	Ja	-
Kryptering, secrets, dataresidens	Ja	-
Administration af brugere og roller	Leverer kontrollerne	Administrerer brugere og roller
Konfiguration af opbevaringspolitik	Leverer kontrollerne	Fastsætter retention-vinduet
Kandidatsamtykke	Leverer workflowet	Sikrer at det bruges
Stærke slutbruger-credentials og SSO	Understøtter SSO og politik	Håndhæver intern politik

15. Threat model og OWASP-mapping

Vi designer mod et konkret sæt modstandere: en ekstern angriber uden credentials, en nysgerrig eller ondsindet authenticated bruger fra én organisation, der forsøger at nå en anden organisations data, en kompromitteret dependency og en intern fejl. Tabellen nedenfor mapper de bredt anvendte OWASP Top 10-risikokategorier til de specifikke kontroller, der adresserer dem i denne platform, og hver af dem afprøves af den testning, der er beskrevet i Section 12.

OWASP-risiko	Hvordan platformen afbøder den
Brudt adgangskontrol	RBAC på hvert privilegeret endpoint; scoping pr. organisation; "not found" ved adgang på tværs af organisationer; remapping af identifikatorer; testmatrix på tværs af organisationer
Kryptografiske fejl	TLS 1.2+ under transit; AES-256 i hvile; bcrypt password hashing; secrets i en managed vault
Injection	Kun ORM-baserede parameteriserede queries; streng schemavalidering; HTML-sanitization ved skrivning
Usikkert design	Lagdelt defense in depth; threat modeling og arkitekturreview i hver revision
Sikkerhedsfejlkonfiguration	Infrastructure as code; standardmæssige deny-all netværksgrupper; sikkerhedsheaders; deaktiverede delte storage-nøgler; API-schema ikke eksponeret i produktion
Sårbare komponenter	Ugentlig automatiseret dependency-overvågning; dependency CVE-audits i periodisk review
Fejl i identification og authentication	Kortlivede tokens; rate-limited login; e-mailverifikation; SSO-understøttelse; ingen passwords i klartekst
Fejl i software- og dataintegritet	Fastlåste, uforanderlige pipeline-trin; signerede desktop-installationsprogrammer; verifikation af webhook-signaturer; tag-kontrollerede produktionsdeployments
Fejl i sikkerhedslogging og overvågning	Centraliseret telemetri; dedikerede audit-tabeller for følsomme handlinger
Server-side request forgery	Udgående kald begrænset til betroede endpoints; SSRF-sonderinger i penetrationstest-harness

Denne mapping er rygraden i vores sikkerhedsargument: for hver velkendt angrebsklasse findes der en navngiven kontrol, og for hver navngiven kontrol findes der en test.

16. Sårbarhedshåndtering og ansvarlig disclosure

Sikkerhed bliver aldrig færdig, så vi driver en kontinuerlig løkke af opdagelse og afhjælpning.

- **Opdagelse.** Sårbarheder fremkommer fra fire kilder: den automatiserede testsuite, de tilbagevendende penetrationstestrevisioner, automatiseret dependency-overvågning og rapporter fra kunder eller forskere.
- **Triage.** Hvert fund tildeles en severity (critical, high, medium, low eller informational) med evidens og en ejer af afhjælpningen, præcis som registreret i vores revisionsrapporter.
- **Mål for afhjælpning.** Critical og high findings prioriteres til øjeblikkelig afhjælpning; i vores revisionshistorik er mere alvorlige fund typisk blevet løst og reverificeret samme dag. Medium og lavere fund planlægges ind i den normale vedligeholdelsesrytme.
- **Verifikation.** Rettelser retestes, og hvor relevant udføres et live-check mod det deployed miljø for at bekræfte, at problemet reelt er lukket, ikke blot lukket i kode.
- **Disclosure.** Sikkerhedsbekymringer kan rapporteres direkte til os. Vi anerkender rapporter, undersøger dem og holder rapportøren informeret frem til løsning.

17. Compliance-mapping

17.1 GDPR

GDPR-område	Platformimplementering
Lovligt grundlag (Art. 6)	Udtrykkeligt kandidatsamtykke indhentet før behandling
Dataminimering og opbevaringsbegrænsning (Art. 5)	Kun interviewrelevante data behandles; konfigurerbar opbevaring med automatisk sletning
Retten til sletning (Art. 17)	Sletning af alle kandidatdata som samlet enhed med logført bevis på sletning
Den registreredes rettigheder (Art. 15 til 20)	Adgang, sletning, portabilitet og indsigelse understøttes
Databehandlerforpligtelser (Art. 28)	Data processing agreement accepteres ved registrering og versionsstyres pr. organisation
Behandlingssikkerhed (Art. 32)	Kryptering, adgangskontrol, isolation og kontinuerlig testning som beskrevet i dette dokument
Transparens om sub-processors	Oplyst i data processing agreement med forhåndsvarsel om ændringer

17.2 EU AI Act

Platformen behandles som et højrisiko-AI-system, der understøtter ansættelsesbeslutninger, og vi vedligeholder dokumentation i overensstemmelse med forordningen, herunder et transparency card, brugerdokumentation og en declaration of conformity. De centrale sikkerhedsforanstaltninger, menneskeligt tilsyn, transparens, evidensbaseret scoring og strenge begrænsninger for, hvad AI'en evaluerer, er beskrevet i Section 10. Vi fortsætter med at modne vores formelle conformity-dokumentation i takt med, at forordningens implementeringstidslinje skrider frem.

17.3 Hostingcertificeringer

Platformen kører udelukkende på Microsoft Azure, hvis datacentre har uafhængige certificeringer, herunder ISO 27001 og SOC 2. Disse certificeringer dækker de fysiske lag og platformslagene under vores applikation; kontrollerne på applikationslaget er dem, der beskrives gennem hele dette dokument.

17.4 Register over sub-processors

Sub-processor	Formål	Region
Microsoft Azure	Hosting, AI- og talebehandling, storage, transaktionel e-mail	EU (West Europe, Sweden Central)
Stripe	Abonnements- og betalingsbehandling	EU (Ireland)
Fakturownia	Fakturering	EU (Poland)
ATS connector (optional)	Integration til applicant-tracking, kun aktiveret efter anmodning	EU

18. Security roadmap

Vi behandler sikkerhed som et program i løbende forbedring. Aktuelle initiativer på vores roadmap omfatter styrkelse af mulighederne for multi-factor authentication for administrative konti, udvidelse af centraliseret audit logging af dataadgang, fortsat stramning af aktualiteten i dependencies efter en regelmæssig kadence og fremdrift mod formel tredjepartscertificering af de kontroller, der er beskrevet i dette dokument. Ingen af disse udgør et hul, der eksponerer kundedata i dag; hver af dem er en forbedring af en allerede lagdelt sikkerhedsposition.

19. Resumé

AI Interview Analyzer beskytter kandidat- og kundedata gennem en lagdelt arkitektur: et netværk, der som standard er privat uden offentlige datatjenester, stærk identitet og isolation pr. organisation, applikationskode der designer hele sårbarhedsklasser væk, kryptering og EU-dataresidens samt privatlivskontroller indbygget i datamodellen. Det, der adskiller platformen, er evidensen bag disse påstande. Med 3,171 automatiserede tests, en gentagelig metodologi for live penetrationstest, et dedikeret AI-sikkerhedsprogram og en historik med syv interne sikkerhedsrevisioner med zero critical findings kan vi vise, ikke bare sige, at platformen er sikker.

Bilag A: Katalog over sikkerhedskontroller

En kondenseret reference over primære kontroller og den evidens, der understøtter hver enkelt.

Kontrol	Mekanisme	Evidens
Kryptering under transport	Kun HTTPS, TLS 1.2+, HTTP omdirigeret	Infrastructure as code; arkitekturrevision
Kryptering i hvile	AES-256 platformkryptering på storage og database	Platformkonfiguration; arkitekturrevision
Passwordbeskyttelse	bcrypt med salt pr. password	Kildekontrol; authentication-tests
Sessionsstyring	30-minutters signerede tokens, tilbagekaldelig server-side refresh	Kildekontrol; authentication-tests
Authorization	Adgangskontrol med fire roller på privilegerede endpoints	Testsuite for rollehåndhævelse
Tenant-isolation	Query-scoping pr. organisation; 404 ved cross-org	Testmatrix på tværs af organisationer
API key-sikkerhed	Hashet lagring, scoped permissions, rate limits pr. key	API key-testsuite
Forsvar mod injection	Kun ORM-baserede parameteriserede queries	Statisk analyse; injection-tests
Forsvar mod cross-site scripting	HTML-sanitization ved skrivning	HTML-sanitization-testsuite
Rate limiting	Holdbar database-backed limiter på auth-endpoints	Rate-limit-tests; live burst-checks
Webhook-integritet	Verifikation af udbyders signatur på rå body	Webhook-testsuite
Secrets Management	Managed vault, purge protection, managed identity	Infrastructure as code; arkitekturrevision
Netværksisolation	Private endpoints; standardmæssig deny-all-segmentering	Infrastructure as code; arkitekturrevision
Datasletning	Kaskaderende sletning som samlet enhed med audit log	GDPR-sletningstestsuite
Supply chain	Fastlåste pipeline-trin; ugentlig dependency-overvågning	Pipelinekonfiguration; dependency-audit

Bilag B: Ofte stillede spørgsmål til sikkerhedsreviewere

Hvor lagres vores data? Udelukkende inden for Den Europæiske Union, på Microsoft Azure, i West Europe med AI-behandling i EU-regioner. Kandidatdata forlader aldrig EU.

Bruges vores data til at træne AI-modeller? Nej. AI-udbyderen bruger ikke kundedata til træning.

Kan databasen nås fra internettet? Nej. Offentlig netværksadgang er deaktiveret, og databasen kan kun nås gennem et private endpoint inde i det virtuelle netværk.

Kan én kunde se en anden kundes data? Nej. Hver query scopes til den kaldende organisations data, adgang på tværs af organisationer returnerer "not found", og en automatiseret matrix tester løbende denne isolation.

Hvordan lagres passwords? Hashet med bcrypt og et unikt salt pr. password. Single sign-on med Microsoft og Google understøttes, og i så fald lagres der intet password.

Understøtter I single sign-on? Ja, via Microsoft og Google OAuth.

Hvor længe er access tokens gyldige? Tredive minutter, parret med en tilbagekaldelig server-side refresh-session, som ugyldiggøres ved logout.

Hvordan håndteres kandidatsamtykke? Hver kandidat modtager et unikt samtykkelink til engangsbrug og skal acceptere, før nogen optagelse eller analyse finder sted. Samtykket registreres mod den specifikke ansættelsesproces.

Hvordan slettes data? Som én samlet enhed, der dækker kandidatposten, interviews, transskripter, lyd, dokumenter og sammenligninger, på en konfigurerbar retention-plan med logført bevis på sletning. Kandidater kan også anmode direkte om sletning.

Har I en data processing agreement? Ja, den accepteres ved registrering og versionsstyres pr. organisation, inklusive registeret over sub-processors.

Træffer AI'en ansættelsesbeslutninger? Nej. Den leverer kun beslutningsstøtte; et menneske gennemgår hvert output og træffer alle beslutninger.

Hvordan beviser I jeres sikkerhedspåstande? Gennem 3,171 automatiserede tests, herunder en dedikeret sikkerhedssuite, en gentagelig seksfaset penetrationstestmetodologi kørt mod live-miljøer, et AI-sikkerhedstestprogram og tilbagevendende skriftlige revisionsrapporter.

Hvad sker der, når I finder en sårbarhed? Den tildeles en severity med evidens og en ejer, afhjælpes efter en prioriteret tidsplan, reverificeres inklusive live-checks hvor relevant og registreres i en revisionsrapport.

Kan vi udføre vores egen penetrationstest? Sikkerhedsvurderinger kan arrangeres gennem jeres account representative under passende scope og planlægning.

Bilag C: Ordliste

Term	Betydning
AES-256	En stærk symmetrisk krypteringsstandard, der bruges til at beskytte data i hvile
bcrypt	En specialbygget password-hashing-funktion med salt pr. password
Managed identity	En platformudstedt identitet, der lader en tjeneste autentificere uden lagrede nøgler
Private endpoint	En privat netværksadresse, der holder en cloud-tjeneste væk fra det offentlige internet
Network security group	Et sæt regler for tilladelse og afvisning, der filtrerer netværkstrafik til et subnet
RBAC	Rollebaseret adgangskontrol, der giver tilladelser i henhold til en brugers rolle
IDOR	Insecure direct object reference, en adgangskontrolfejl som platformen forsvarer sig imod
SSRF	Server-side request forgery, en angrebsklasse der sonderes i vores penetrationstests
Web application firewall	En edge-kontrol, der filtrerer ondsindet webtrafik
Data processing agreement	Kontrakten, der regulerer, hvordan en databehandler håndterer personoplysninger på vegne af en dataansvarlig

Bilag D: Kontakt- og dokumentstyring

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

For et sikkerhedsreview, en kopi af vores data processing agreement eller vores EU AI Act-conformity-dokumentation, kontakt venligst jeres account representative.

Dette dokument beskriver sikkerhedspositionen for AI Interview Analyzer-tjenesten pr. den genereringsdato, der vises i footeren. Det leveres til evalueringsformål og udgør ikke en del af nogen kontrakt. Specifikke kontraktuelle sikkerhedsforpligtelser er fastsat i den gældende aftale og data processing agreement.