Document tehnic de securitate

Enterprise Security Overview - AI Interview Analyzer

Furnizor:	AI Interview Analyzer Sp. z o.o.
Adresă:	ul. Jedrusik 6/53, 01-748 Warszawa, Poland
NIP:	5253079974
REGON:	54402118500000
Clasificare:	PUBLIC
Data:	24.06.2026

Contents

Document tehnic de securitate

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

Public țintă: Echipe enterprise de securitate, IT și achiziții

Clasificare: Public

1. Rezumat executiv

AI Interview Analyzer este o platformă enterprise pentru recrutare care înregistrează interviuri cu consimțământul explicit al candidatului, le transcrie și le structurează și produce suport de evaluare bazat pe dovezi pentru recrutori. Deoarece platforma prelucrează date cu caracter personal ale candidaților și susține procese de angajare, securitatea și confidențialitatea sunt tratate ca constrângeri primare de proiectare, nu ca funcționalități adăugate ulterior.

Acest document tehnic descrie, în termeni concreți și verificabili, modul în care protejăm datele clienților și ale candidaților. Este redactat pentru persoanele care evaluează furnizori: ingineri de securitate, administratori IT, responsabili cu protecția datelor și achiziții. Fiecare cifră din acest document este extrasă direct din propriile noastre sisteme de inginerie, nu din materiale de marketing.

Mesajul central este simplu: **nu afirmăm doar că platforma este securizată, ci testăm continuu acest lucru.** Baza noastră de cod conține **3,171 teste automate**, inclusiv o suită dedicată de securitate care verifică autentificarea, autorizarea, izolarea între organizații, protecțiile împotriva injecțiilor și ștergerea datelor. În plus, rulăm un cadru repetabil de testare de penetrare împotriva implementărilor active și producem rapoarte scrise de audit. În șapte audituri interne de securitate din martie și aprilie 2026, am înregistrat **zero constatări critice**, iar cel mai recent audit al nostru s-a încheiat cu verdictul **PASS**. (Certificarea formală de către terți a acestor controale este inclusă în foaia noastră de parcurs; a se vedea Secțiunea 18.)

Caracteristică de securitate	Rezumat
Găzduire	Microsoft Azure, numai regiuni din UE
Model de rețea	Endpoint-uri private, segmentare de rețea default-deny, fără bază de date publică
Criptare	AES-256 în repaus, TLS 1.2 sau mai mare în tranzit
Identitate	Token-uri semnate cu durată scurtă de viață, hash-uire a parolelor cu bcrypt, suport SSO
Controlul accesului	RBAC cu izolare strictă per organizație
Secrete	Vault centralizat pentru secrete cu acces prin managed identity
Confidențialitate	Consimțământ explicit, retenție configurabilă, ștergere per unitate unică
AI responsabil	Doar suport decizional, om întotdeauna în buclă
Asigurare	3,171 teste automate plus teste de penetrare și audituri recurente

1.1 Cum se citește acest document

Secțiunile 3 până la 11 descriu controalele care protejează datele: arhitectură, rețea, identitate, aplicație, protecția datelor, confidențialitate și ciclul de viață al dezvoltării securizate. Secțiunile 12 și 13 acoperă programul nostru distinctiv de testare continuă și istoricul auditurilor noastre. Secțiunile 14 până la 17 acoperă operațiunile, modelarea amenințărilor, managementul vulnerabilităților și maparea conformității. Anexele oferă un catalog de controale, un FAQ pentru evaluatori și un glosar pe care o echipă de securitate îl poate utiliza direct în timpul unei evaluări.

2. Domeniul documentului și abordare

2.1 Ce acoperă acest document

Acest document tehnic acoperă arhitectura de securitate și practicile serviciului AI Interview Analyzer: mediul de găzduire, proiectarea rețelei, gestionarea identității și a accesului, controalele la nivel de aplicație, protecția datelor, confidențialitatea și alinierea la reglementări, ciclul de viață al dezvoltării securizate și programul nostru de testare continuă a securității.

2.2 Ce îl face verificabil

Afirmațiile furnizorilor privind securitatea sunt ușor de scris și greu de crezut. Prin urmare, am corelat fiecare afirmație majoră din acest document cu ceva concret și cuantificabil din sistemele noastre de inginerie: un control implementat în cod, un test care dovedește că acel control funcționează, o definiție de infrastructură care îl impune sau un raport de audit care consemnează o verificare documentată. Acolo unde un control face parte din foaia noastră de parcurs viitoare, și nu este implementat astăzi, precizăm acest lucru explicit. Preferăm să afirmăm mai puțin și să fim credibili decât să exagerăm și să fim contrazișși.

2.3 Responsabilitate partajată

Platforma este livrată ca software as a service. Noi operăm infrastructura, aplicația, pipeline-ul AI și prelucrarea datelor. Clientul este responsabil de gestionarea propriilor conturi de utilizator și roluri, de configurarea ferestrelor de retenție a datelor pentru a corespunde politicii sale interne și de asigurarea că se obține consimțământul candidatului prin fluxul de consimțământ oferit de platformă. Secțiunea 14 descrie această împărțire mai detaliat.

3. Prezentare generală a arhitecturii de securitate

Platforma este construită ca un număr redus de servicii cooperante, nu ca un monolit unic. O aplicație desktop și un portal web acționează ca clienți. Un API backend central deține toată persistența, autentificarea, facturarea, pipeline-ul AI, consimțământul, emailul, gestionarea fișierelor și dashboard-urile. Un worker de îmbinare audio procesează înregistrările asincron. Toată starea sensibilă se află în spatele API-ului backend; clienții nu comunică niciodată direct cu baza de date, stocarea sau serviciile AI.

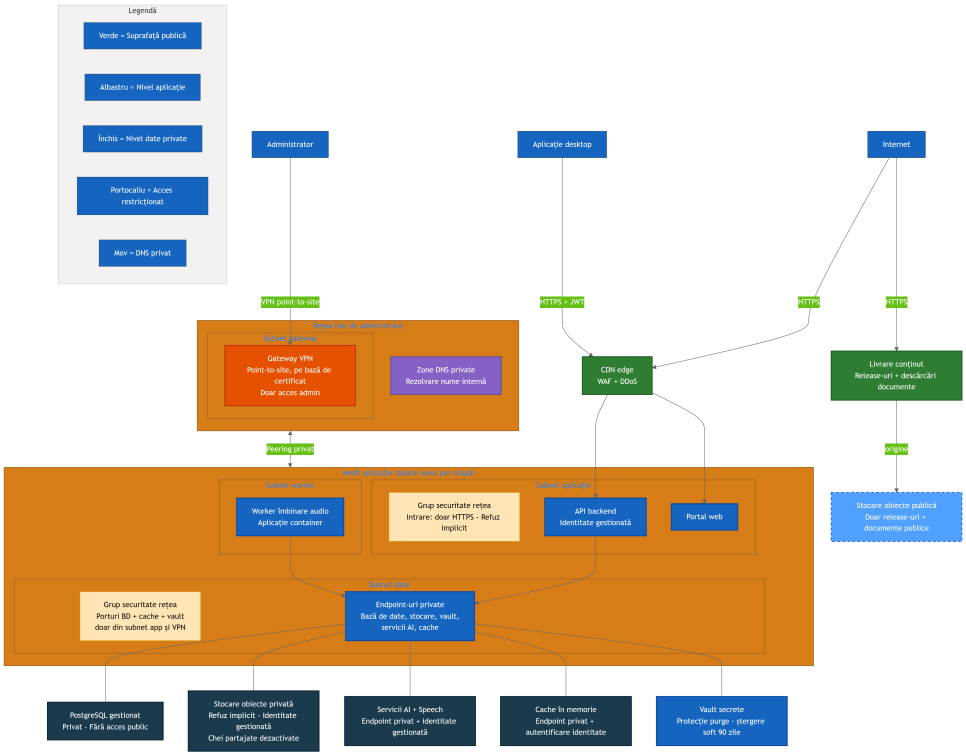


Diagrama de mai sus arată topologia de producție, cu numele resurselor generalizate intenționat. În ea sunt vizibile trei principii:

- **Fără expunere directă a serviciilor de date.** Baza de date, object storage privat, serviciile AI și cache-ul au accesul la rețeaua publică dezactivat și sunt accesibile doar prin endpoint-uri private în interiorul unei rețele virtuale izolate. Vault-ul de secrete este accesat de aplicație printr-un endpoint privat și este protejat suplimentar prin autentificare de identitate la nivel de platformă și politici de acces de tip least-privilege, astfel încât orice acces necesită o identitate validă și autorizată, indiferent de traseul de rețea.
- **O suprafață publică separată.** Singurul object storage public deține descărcări de release și documente publice. Acesta nu conține niciodată date ale candidaților. Traficul aplicației orientat către client trece printr-un strat edge care furnizează web application firewall, protecție distribuită împotriva denial-of-service și livrare de conținut.
- **Accesul administrativ este controlat strict.** Operatorii ajung la resursele interne doar printr-un VPN point-to-site bazat pe certificate către o rețea hub de management, nu prin internetul public.

Fiecare etapă de implementare (development și production) este un mediu complet izolat, cu propria sa rețea, propriile conturi de stocare, bază de date și secrete. Datele de producție ale clienților nu sunt prezente niciodată în mediile inferioare. Un hub de management partajat deține doar gateway-ul VPN și DNS-ul privat, conectate privat la fiecare mediu.

---

4. Apărare în profunzime

Nu ne bazăm pe un singur control pentru a opri orice atac. Platforma suprapune controale independente astfel încât compromiterea oricărui strat să nu expună datele. Straturile de mai jos sunt fiecare implementate și, așa cum este descris în Secțiunea 12, testate individual.

Model de securitate stratificat: controale independente la fiecare nivel

Strat	Controale reprezentative
Edge de rețea	Transport numai prin TLS, WAF și protecție DDoS la edge, endpoint-uri private, segmentare default-deny
Identitate și acces	Token-uri semnate cu durată scurtă de viață, hash-uire cu bcrypt, RBAC, izolare per organizație
Aplicație	Validare de schemă pentru toate datele de intrare, acces la date doar prin ORM, codificare a ieșirii, rate limiting
Protecția datelor	Criptare în repaus, vault de secrete cu managed identity, rezidența datelor în UE, prelucrare condiționată de consimțământ
Guvernanță și confidențialitate	Retenție configurabilă, ștergere per unitate unică, AI cu om în buclă, jurnalizare de audit
Asigurare continuă	Suită de teste automate, teste de penetrare repetabile, audituri interne recurente de securitate

Restul acestui document parcurge pe rând fiecare strat și apoi descrie cum demonstrăm, continuu, că aceste straturi rezistă.

5. Securitatea rețelei

5.1 Privat în mod implicit

Stratul de date este privat prin construcție. Baza de date PostgreSQL administrată are accesul la rețeaua publică dezactivat și este accesibilă numai printr-un endpoint privat. Object storage-ul privat este configurat să refuze accesul de rețea în mod implicit, dezactivează complet cheile de acces partajat și este accesibil doar prin managed identity din subnet-ul aplicației. Cache-ul, serviciile AI și vault-ul de secrete sunt accesate în mod similar prin endpoint-uri private cu rezoluție DNS privată.

În practică, aceasta înseamnă că nu există niciun connection string expus la internet către baza de date și niciun URL public de stocare pentru audio-ul candidaților: baza de date și stocarea privată au accesul la rețeaua publică dezactivat în mod direct. Vault-ul de secrete este accesat de aplicație printr-un endpoint privat și este protejat prin autentificare de identitate la nivel de platformă și politici de acces de tip least-privilege, cu identități ale aplicației cărora li se acordă acces read-only doar la secretele de care au nevoie, astfel încât secretele nu pot fi recuperate fără o identitate validă și autorizată. Suprafața de atac pe care un adversar extern o poate atinge este limitată la endpoint-urile HTTPS ale aplicației din spatele stratului edge.

5.2 Segmentarea rețelei

Fiecare mediu este împărțit în subnet-uri separate pentru stratul aplicației, stratul de date și worker-ul asincron. Fiecare subnet este guvernat de un network security group a cărui regulă finală refuză tot traficul de intrare. Subnet-ul aplicației acceptă doar trafic HTTPS de intrare. Subnet-ul de date acceptă doar porturile specifice pentru baza de date, cache și vault, și numai din subnet-ul aplicației sau din VPN-ul administrativ. Aceasta înseamnă că nici chiar un atacator care ar ajunge cumva în stratul aplicației nu poate pivota liber către stratul de date; singurele căi permise sunt cele pe care aplicația le utilizează legitim.

5.3 Stratul edge

Traficul public al aplicației este plasat în fața unui strat edge care furnizează web application firewall, protecție DDoS și un content delivery network. Descărcările de release și documente sunt servite dintr-un cont dedicat de stocare publică printr-un front door de livrare de conținut, complet separat de stocarea privată care deține datele candidaților. Cele două planuri de stocare nu se amestecă niciodată: o configurare greșită în planul public nu poate expune date private ale candidaților, deoarece sunt conturi diferite cu reguli de rețea diferite.

5.4 Acces administrativ

Nu există niciun endpoint administrativ public în rețeaua privată. Operatorii se conectează printr-un gateway VPN point-to-site care utilizează autentificare bazată pe certificate. Accesul administrativ la baza de date și cache este posibil doar din interiorul acelui tunel, deoarece aceste servicii au accesul la rețeaua publică dezactivat. Aceasta menține operațiunile de zi cu zi complet în afara internetului public.

6. Gestionarea identității și a accesului

6.1 Autentificare

Sesiunile utilizatorilor sunt stabilite cu un access token semnat valabil treizeci de minute, asociat cu un refresh token separat, opac, pe partea de server. Access token-urile sunt verificate la fiecare cerere, iar utilizatorul este revalidat în baza de date (inclusiv o verificare a faptului că acel cont este activ), în loc să se acorde încredere exclusiv conținutului token-ului. Deconectarea revocă imediat sesiunea de refresh de pe server, astfel încât un refresh token furat nu poate supraviețui unei deconectări.

Parolele nu sunt stocate niciodată în clar. Ele sunt hash-uite cu bcrypt folosind un salt unic pentru fiecare parolă. Pentru organizațiile care preferă single sign-on, platforma suportă autentificare OAuth cu Microsoft și Google, caz în care nu este deținută nicio parolă.

Proprietatea asupra adresei de email este verificată printr-un link de verificare de unică folosință, limitat în timp, înainte ca un cont autoînregistrat să fie tratat ca verificat, iar retransmiterile emailului de verificare sunt supuse la rate limiting pentru a preveni abuzul.

6.2 Role-Based Access Control

Autorizarea este impusă printr-un model de roluri cu patru roluri de privilegiu crescător: intervievator, manager de recrutare, recrutor și administrator. Accesul la operațiuni privilegiate este impus de dependențe pe partea de server care verifică atât rolul, cât și starea de verificare a solicitantului. Aceste verificări de rol protejează mult peste o sută de operațiuni API distincte.

Rol	Capabilități tipice
Intervievator	Desfășoară interviurile atribuite; vede doar interviurile care îi sunt atribuite
Manager de recrutare	Gestionează recrutările pe care le deține sau în care este membru
Recrutor	Gestionare completă a recrutărilor și candidaților în cadrul organizației
Administrator	Setări ale organizației, facturare, administrarea utilizatorilor și a cheilor API

Dincolo de verificările grosiere bazate pe rol, platforma aplică reguli de vizibilitate la nivel de date. Managerii de recrutare văd doar recrutările pe care le-au creat sau în care sunt membri; intervievatorii văd doar interviurile care le sunt atribuite. Prin urmare, privilegiile sunt impuse atât la nivelul „ce acțiune”, cât și la nivelul „care înregistrări”.

6.3 Izolare per organizație

Platforma este multi-tenant, iar izolarea tenant-ului este tratată ca un control de securitate de primă clasă. Fiecare identitate autentificată poartă un identificator de organizație, iar interogările de date sunt limitate la acea organizație. Când un utilizator solicită o înregistrare care aparține altei organizații, platforma returnează un răspuns de tip „not found” în loc să dezvăluie că înregistrarea există. Identificatorii interni ai bazei de date nu sunt expuși niciodată pe fir; API-ul prezintă identificatori de afișare și îi remapează per cerere, ceea ce elimină o clasă comună de atacuri de enumerare cross-tenant.

Aceasta nu este doar o intenție de design. După cum este descris în Secțiunea 12, suita noastră automată execută o matrice extinsă cross-organization care încearcă să ajungă la datele unei organizații folosind credențialele altei organizații și verifică faptul că fiecare astfel de încercare eșuează.

6.4 Acces programatic

Pentru integrări, organizațiile din planurile eligibile pot emite chei API. Cheile folosesc un prefix recognoscibil, includ 128 de biți de entropie și sunt stocate doar sub formă de hash; cheia brută este afișată o singură dată la creare și niciodată din nou. Fiecare cheie are un scope explicit de permisiuni (read, write sau integrare ATS), poate fi restricționată la rețele sursă specifice, poate fi revocată instantaneu și este supusă unor limite de rată per cheie derivate din nivelul de plan al organizației. Verificarea cheilor

folosește o comparație timing-safe pentru a evita scurgerile de informații prin timpul de răspuns.

7. Securitatea aplicației

Aplicația este scrisă pentru a elimina categorii întregi de vulnerabilități, nu pentru a le remedia de la caz la caz.

• **Injecție.** Tot accesul la baza de date se realizează printr-un object-relational mapper cu interogări parametrizate. Baza de cod nu conține SQL formatat brut ca șir de caractere. Acest lucru elimină structural SQL injection.

• **Validarea intrării.** Fiecare corp de cerere este validat față de o schemă strictă înainte de a ajunge la logica de business. Payload-urile supradimensionate sunt respinse, iar endpoint-urile de listare sunt paginate pentru a limita consumul de resurse.

• **Codificarea ieșirii și cross-site scripting.** Textul furnizat de utilizator și cel generat de AI sunt tratate ca nefiind de încredere. Acolo unde conținutul trebuie redat ca HTML, acesta trece printr-un sanitizer bazat pe allow-list la momentul scrierii, iar o suită dedicată de teste confirmă că tag-urile script, event handler-ele și URL-urile javascript sunt eliminate.

• **Mass assignment.** Operațiunile de actualizare folosesc scheme explicite care exclud câmpuri privilegiate precum rol, organizație și sold de credite, astfel încât un client să nu poată escalada privilegiile prin trimiterea unor câmpuri suplimentare.

• **Rate limiting.** Endpoint-urile de autentificare și cele predispuse la abuz sunt supuse la rate limiting folosind un limiter durabil, bazat pe bază de date, care supraviețuiește repornirilor și funcționează corect în mai multe instanțe ale aplicației. Login-ul, înregistrarea, resetarea parolei și retransmiterile verificării au fiecare propriile limite. Rezolvarea IP-ului clientului este consolidată împotriva spoofing-ului headerelor de forwarding.

• **Webhook-uri.** Webhook-urile de intrare de la furnizori de plăți și email sunt verificate față de semnăturile furnizorului pe corpul brut al cererii înainte de a fi procesate.

• **Încărcări de fișiere.** Încărcările au limită de dimensiune, sunt validate, stocate sub identificatori generați, nu sub nume furnizate de utilizator, și sunt restricționate per cerere și per organizație.

• **Header-e de securitate.** În production, răspunsurile includ HSTS, opțiuni pentru tipul de conținut și frame, o politică de referrer și o permissions policy restrictivă și suprimă bannerele serverului și framework-ului.

8. Protecția datelor

8.1 Criptare

Toate datele sunt criptate în repaus folosind AES-256 prin straturile de criptare ale platformei Azure pentru stocare și baze de date. Tot traficul de rețea este servit exclusiv prin HTTPS folosind TLS 1.2 sau superior; HTTP în clar este redirecționat către HTTPS la fiecare nivel. În production, API-ul și portalul web emit header-e HSTS împreună cu un set de header-e de consolidare și suprimă bannerele de versiune ale serverului și framework-ului.

8.2 Gestionarea secretelor

Secretele aplicației sunt păstrate într-un vault centralizat pentru secrete, cu purge protection activat și o fereastră de soft-delete de nouăzeci de zile. Aplicațiile se autentifică la resursele Azure folosind managed identities atribuite de sistem, în locul unor chei de lungă durată; de exemplu, stocarea privată are cheile de acces partajat dezactivate complet, astfel încât accesul este posibil doar prin atribuiri de rol bazate pe identitate, limitate la resursa individuală. Politicile de acces la vault acordă principalilor aplicației acces read-only la secretele specifice de care au nevoie, în conformitate cu principiul least privilege.

8.3 Rezidența datelor

Toate datele clienților și candidaților sunt stocate și prelucrate în interiorul Uniunii Europene. Găzduirea aplicației, baza de date, stocarea, cache-ul și secretele se află în West Europe, iar prelucrarea AI rulează în regiuni din UE. Furnizorul AI nu utilizează datele clienților pentru antrenarea modelelor sale.

8.4 Viața unui singur interviu

Cel mai clar mod de a înțelege controalele de protecție a datelor este să urmărim un interviu de la un capăt la altul. Consimțământul este capturat și înregistrat înainte de a fi prelucrat orice. Încărcarea este criptată în tranzit. Transcrierea și analiza rulează în centre de date din UE. Rezultatele sunt scrise în stocare criptată. Fiecare înregistrare este apoi guvernată de un singur ceas de retenție care se încheie cu o ștergere în cascadă jurnalizată. În orice moment, drepturile candidatului, precum retragerea, ștergerea, accesul sau portabilitatea, pot întrerupe acest flux.

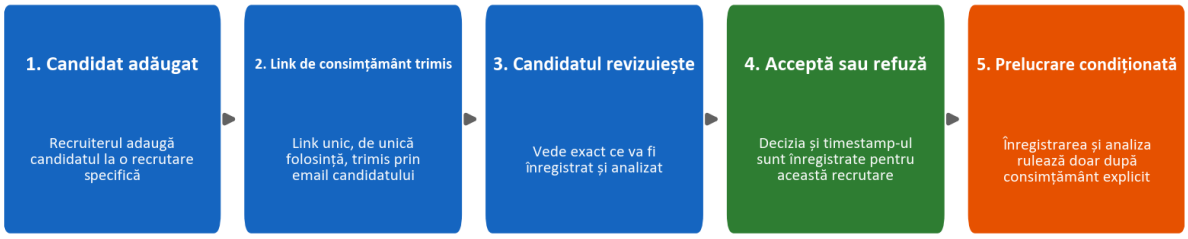
9. Confidențialitate prin design și GDPR

Confidențialitatea este integrată în modelul de date și în fluxul de lucru, nu adăugată ulterior doar prin politici.

9.1 Consimțământ

Niciun interviu nu este înregistrat sau analizat fără consimțământul explicit al candidatului. Atunci când un candidat este adăugat într-un proces de recrutare, platforma emite prin email un link unic de consimțământ, de unică folosință. Candidatul analizează ce se va întâmpla și fie acceptă, fie refuză. Starea consimțământului, inclusiv momentul răspunsului, este înregistrată pentru acel proces de recrutare specific, astfel încât consimțământul este întotdeauna limitat la un proces concret de angajare, nu acordat global.

Consimțământ candidat: explicit și înregistrat înainte de orice prelucrare

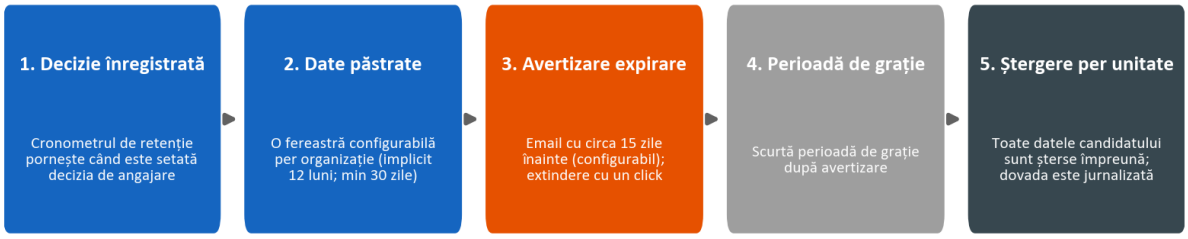


9.2 Retenție și ștergere

Retenția datelor este configurabilă per organizație, cu un implicit de douăsprezece luni și un minim configurabil de treizeci de zile, și poate fi suprascrisă per candidat. Există un singur ceas de retenție pentru datele unui candidat, nu un cronometru separat per artefact. Ceasul începe atunci când este înregistrată o decizie de angajare. Înainte de expirarea datelor, platforma trimite un avertisment (implicit cu aproximativ cincisprezece zile înainte) și oferă o extensie cu un singur clic. Atunci când datele sunt șterse, ele sunt șterse ca o singură unitate: înregistrarea candidatului, interviurile, transcrierile, înregistrările audio, documentele și comparațiile sunt toate eliminate împreună, iar ștergerea este consemnată într-un jurnal de audit. Nu există reziduuri parțiale sau orfane.

Ciclul de viață de mai jos arată acest ceas unic și modul în care converge către o singură ștergere în cascadă, cu o dovadă jurnalizată de ștergere.

Retenția datelor: un cronometru per candidat, ștergere per unitate



9.3 Drepturile persoanei vizate și subîmputerniciți

Platforma suportă drepturile persoanei vizate cerute de GDPR, inclusiv accesul, ștergerea, portabilitatea, opoziția și explicația. Prelucrarea se desfășoară în baza unui DPA pe care clienții îl acceptă la înregistrare și care este versionat per organizație. Subîmputerniciții noștri și rolurile lor, toți în UE sau sub garanții adecvate, sunt divulgați în acel acord, iar clienții primesc notificare prealabilă privind orice modificare. Secțiunea 17 conține registrul subîmputerniciților și maparea conformității articol cu articol.

10. AI responsabil și EU AI Act

Platforma se încadrează în categoria high-risk a EU AI Act deoarece susține decizii privind ocuparea forței de muncă, iar noi tratăm această clasificare cu maximă seriozitate.

Regula definitorie a produsului este că **AI-ul oferă suport decizional, nu este un factor de decizie.** Sistemul nu acceptă și nu respinge niciodată automat un candidat. El transcrie vorbirea, structurează întrebările și răspunsurile, notează răspunsurile în raport cu criteriile definite de recrutor și redactează feedback, iar un om revizuiește fiecare rezultat înainte de utilizare. Astfel, un om rămâne ferm în buclă.

La fel de important este ceea ce AI-ul nu face. Nu evaluează personalitatea, „potrivirea culturală", starea emoțională, tonul vocii, accentul, genul, vârsta, etnia, aspectul sau limbajul corpului. Scorarea este ancorată în dovezi din transcriere și în criterii definite de recrutor, iar numele candidaților sunt excluse din inputul de evaluare pentru a reduce părtinirea. Publicăm un card de transparență, documentație pentru utilizatori și o declarație de conformitate care descriu sistemul, limitările sale și măsurile sale de protecție.

Control de AI responsabil	Cum funcționează
Om în buclă	Fiecare scor și fiecare element de feedback este revizuit de un recrutor înainte de utilizare
Fără decizii automate	Sistemul nu acceptă și nu respinge niciodată automat un candidat
Scorare bazată pe dovezi	Scorurile fac referire la dovezi justificative din transcriere
Design anti-bias	Numele sunt excluse din evaluare; conținutul este evaluat înaintea stilului
Limite de domeniu	Personalitatea, emoția, accentul și caracteristicile protejate nu sunt niciodată evaluate
Siguranța feedback-ului pentru candidați	Feedback-ul privat pentru candidați trece printr-o balustradă de siguranță de generare și validare

Aceste constrângeri nu sunt doar enunțate în documentație; ele sunt codificate în stratul de prompt AI și exercitate de un program dedicat de testare a siguranței AI descris în Secțiunea 12.3.

11. Ciclul de viață al dezvoltării securizate

Securitatea este impusă prin modul în care construim și livrăm software, nu doar în sistemul aflat în execuție.

• **Separarea mediilor.** Development și production sunt complet separate, fiecare cu propria infrastructură, propriile conturi de stocare, bază de date, secrete și subdomenii. Nu există stare partajată.

• **Infrastructure as code.** Întregul mediu cloud este definit ca și cod și revizuit ca și cod, ceea ce face postura de securitate auditabilă și reproductibilă. Un evaluator poate vedea exact ce porturi sunt deschise, ce resurse sunt private și ce identități au ce permisiuni.

• **Implementări fixate și controlate.** Fiecare pas din pipeline-ul de continuous integration este fixat la o versiune exactă, imuabilă. Implementările în production sunt bazate pe tag-uri, rulează numai prin pipeline-ul protejat de production și sunt blocate în spatele unei aprobări obligatorii. Suita de teste automate rulează ca poartă de release: o implementare nu poate fi livrată dacă testele eșuează.

• **Igiena dependențelor.** Monitorizarea automată a dependențelor propune actualizări săptămânale pentru backend, desktop, web, infrastructură și definițiile pipeline-urilor, iar auditurile dependențelor fac parte din evaluarea noastră periodică de securitate.

• **Artefacte semnate.** Instalatoarele desktop sunt semnate digital, astfel încât clienții să poată verifica faptul că software-ul pe care îl instalează provine cu adevărat de la noi.

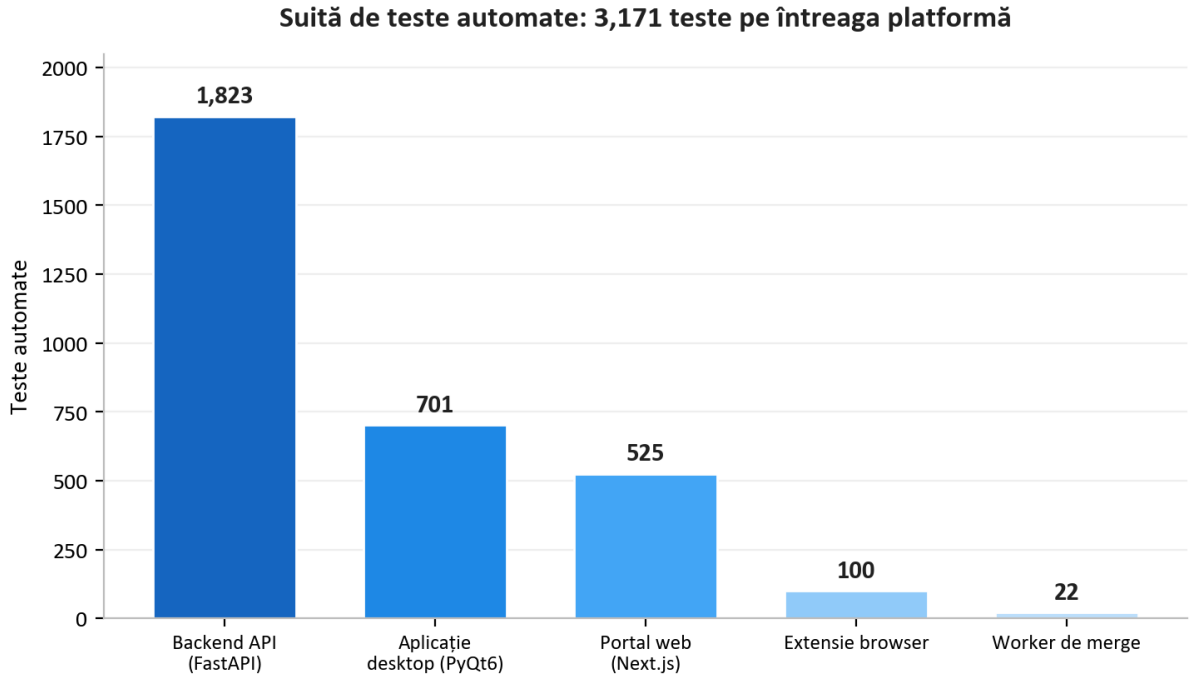
• **Disciplina secretelor.** Secretele se află în vault și în secretele protejate ale pipeline-ului, niciodată în codul sursă.

12. Testare continuă a securității

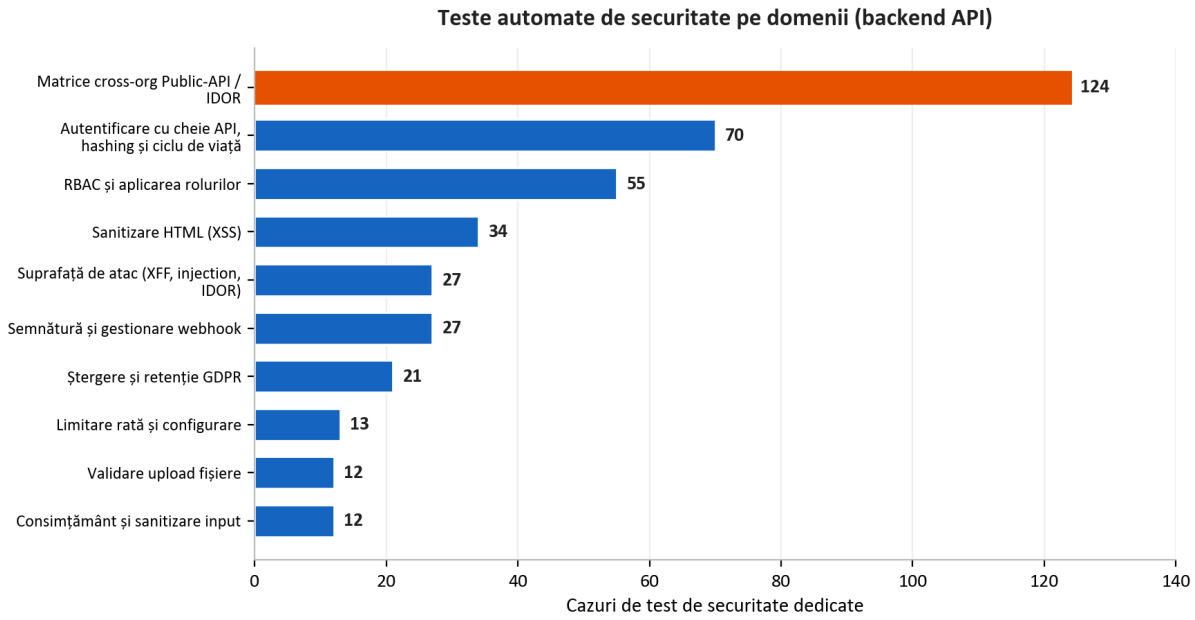
Acesta este nucleul argumentului nostru de asigurare și partea pe care majoritatea furnizorilor nu o pot demonstra. Tratăm securitatea ca pe ceva ce trebuie măsurat continuu, cu verificări executabile, nu afirmat o singură dată.

12.1 Suita de teste automate

Platforma este acoperită de **3,171 teste automate** care acoperă API-ul backend, aplicația desktop, portalul web, extensia de browser și worker-ul de îmbinare audio.



Acestea nu sunt doar teste funcționale. O suită substanțială și dedicată de securitate verifică controalele descrise anterior în acest document. Graficul de mai jos detaliază testele specifice de securitate din API-ul backend pe domenii.



Printre multe altele, această suită include o matrice amplă a API-ului public care rulează fiecare endpoint ca utilizator legitim, ca propria cheie API a organizației și ca o cheie API a unei organizații rivale, verificând că fiecare încercare cross-organization este blocată. Include zeci de teste adverse ale suprafeței de atac pentru spoofing al headerelor de forwarding, header injection și scurgeri de identificatori, o suită concentrată de sanitizare HTML pentru cross-site scripting, teste de impunere a rolurilor pentru întregul model de roluri și teste care dovedesc că datele candidatului sunt într-adevăr șterse ca unitate. Deoarece aceste teste rulează ca poartă de release, o regresie care ar slăbi oricare dintre aceste controale ar opri release-ul în loc să ajungă la clienți.

12.2 Testare de penetrare live

Testele automate unitare dovedesc că controalele se comportă corect în izolare. Pentru a demonstra că ele rezistă împreună într-o implementare reală, menținem o metodologie repetabilă de testare de penetrare care rulează scripturi de atac reale împotriva unui mediu live. Aceasta este organizată în șase faze:

Fază	Focalizare	Exemple din ceea ce este verificat
1. Analiză statică	Cod sursă	Secrete, modele de injecție, funcții periculoase, lipsă auth, HTML nesigur
2. Revizuire de arhitectură	Infrastructură	Endpoint-uri private, segmentare, TLS, configurarea secretelor
3. Analiza vectorilor de atac	Control sursă și cloud	Protecția branch-urilor, scope de identitate, expunere publică
4. Testare de penetrare live	Mediu în execuție	Probing neautentificat, acces cross-org, injecție, manipularea token-urilor, SSRF, rafale de rate-limit
5. Scor enterprise	Maturitate	Șaisprezece categorii de securitate punctate față de o linie de bază enterprise
6. Dependențe și supply chain	Risc terț	Audit CVE al dependențelor, acțiuni de pipeline fixate, integritatea lock-file-ului

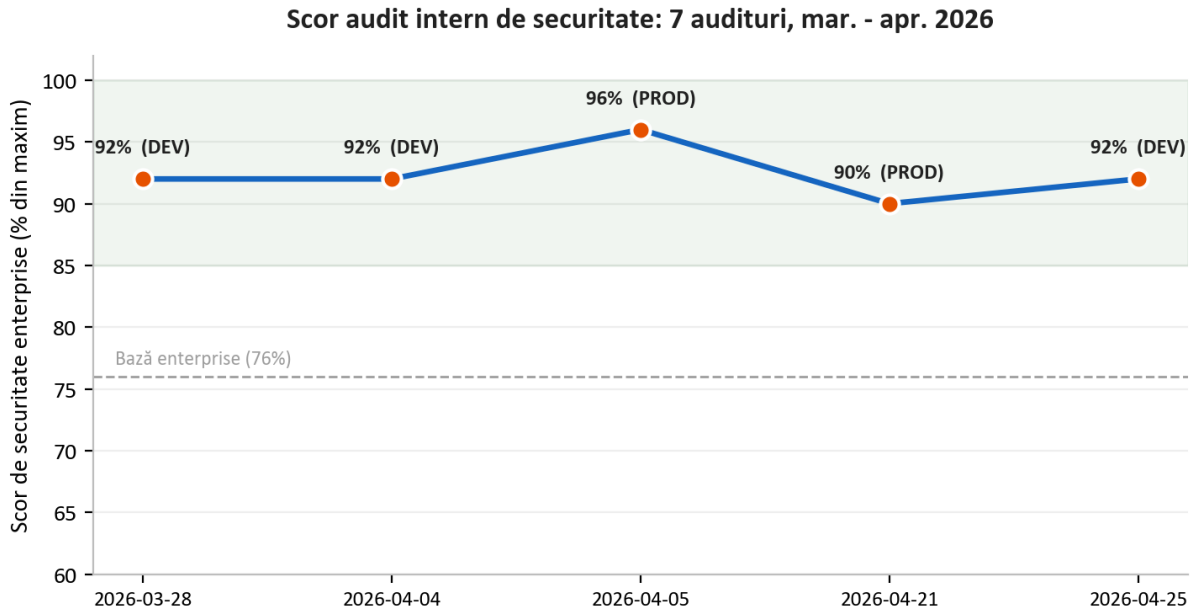
Faza 4 este testare adversarială reală împotriva unui sistem implementat, nu o listă de verificare. Aceasta sondează endpoint-uri protejate fără credențiale și confirmă că refuză accesul; înregistrează două organizații și încearcă să ajungă la înregistrările uneia cu contul celeilalte; injectează payload-uri de cross-site-scripting și server-side-template și confirmă că sunt neutralizate; manipulează token-uri de autentificare și confirmă că sunt respinse; încearcă server-side request forgery împotriva endpoint-urilor cloud metadata; și generează rafale pe endpoint-urile de autentificare pentru a confirma că rate limiting se declanșează efectiv în mediul live, nu doar teoretic.

12.3 Testarea siguranței feedback-ului pentru candidați

Deoarece platforma poate genera feedback privat de dezvoltare pentru candidați, rulăm un program separat de siguranță adversarială pentru această funcționalitate. El alimentează în mod deliberat sistemul cu note dure și ostile ale recrutorilor și confirmă că output-ul orientat către candidat nu conține niciodată vulgaritate, nu dezvăluie și nu atribuie niciodată identitatea sau opinia privată a unui recrutor și nu aplică niciodată etichete de personalitate cu caracter de judecată. Aceasta protejează atât candidatul, care ar trebui să primească feedback constructiv și respectuos, cât și clientul, care nu ar trebui niciodată să permită scurgerea unei opinii interne în exterior.

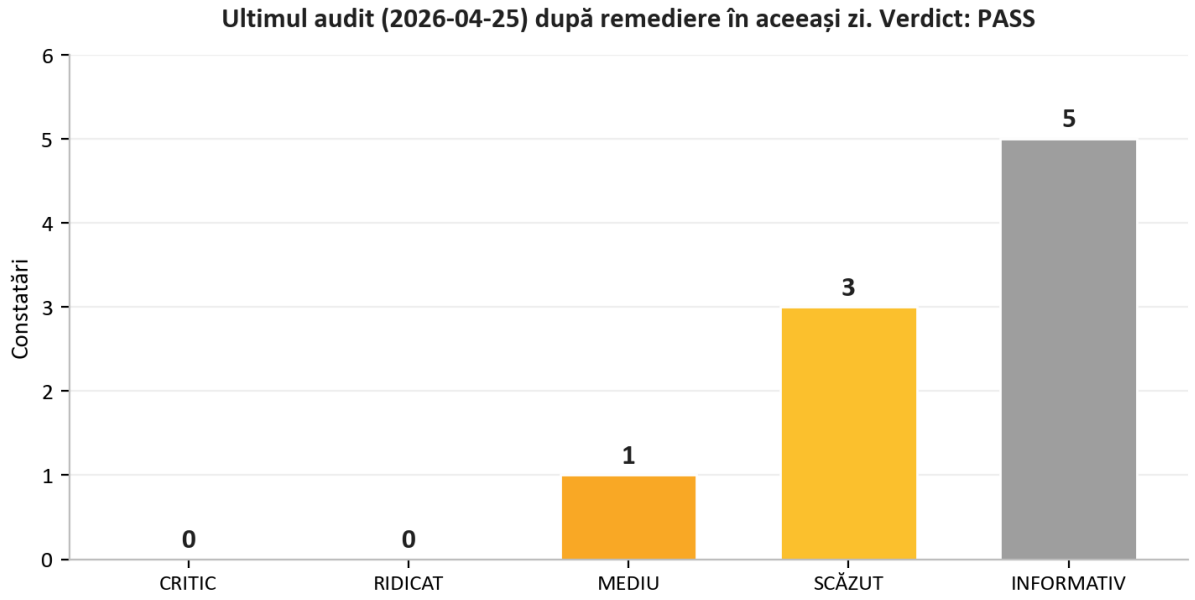
13. Rezultatele auditurilor de securitate

Desfășurăm audituri recurente de securitate utilizând o metodologie structurată și repetabilă de testare de penetrare și redactăm fiecare audit sub forma unui raport datat, cu constatări clasificate pe severitate, dovezi și remediere. Acestea sunt audituri interne derulate prin propriul nostru proces de securitate; certificarea formală de către terți a acelorași controale face parte din foaia noastră de parcurs. Între sfârșitul lui martie și sfârșitul lui aprilie 2026 am finalizat **șapte astfel de audituri** în development și production.



Rezultatul care contează cel mai mult pentru un client potențial este consecvența: **în toate cele șapte audituri au existat zero constatări critice.** În rarele ocazii în care a apărut o problemă de severitate mai ridicată, aceasta a fost remediată rapid, adesea în aceeași zi, și reverificată. Rubrica de scor a fost înăsprită în mod deliberat în această perioadă (scorul maxim posibil a fost crescut pe măsură ce am adăugat mai multe categorii de evaluat), motiv pentru care linia scorului normalizat rămâne ridicată chiar dacă pragul a crescut.

Cel mai recent audit al nostru, din 25 April 2026, ilustrează modul în care funcționează procesul în practică. Au fost identificate două probleme de severitate mai ridicată, ambele au fost remediate și reverificate în aceeași zi, iar auditul s-a încheiat cu verdictul **PASS** fără probleme exploatabile rămase în modelul actual de amenințare.



Audit	Mediu	Critic	Verdict
2026-03-28	Development	0	Pregătit pentru production
2026-04-04	Development	0	Pregătit pentru enterprise
2026-04-05	Production	0	Pregătit pentru enterprise
2026-04-20	Development	0	Pregătit pentru production, note
2026-04-20	Development	0	Pass cu note
2026-04-21	Production	0	Sigur, fără constatări exploatabile
2026-04-25	Development	0	Pass

Tiparul din aceste audituri este cea mai onestă dovadă pe care o putem oferi: problemele sunt găsite, pentru că le căutăm riguros, și sunt închise rapid, pentru că procesul este construit să le închidă. Un furnizor care nu raportează niciodată o constatare este, de obicei, un furnizor care nu caută.

14. Reziliență operațională și responsabilitate partajată

14.1 Monitorizare și jurnalizare

Telemetria aplicației și a platformei este direcționată către un workspace centralizat de analiză a jurnalelor și un serviciu de monitorizare a aplicației, oferindu-ne vizibilitate asupra disponibilității și comportamentului. Acțiunile sensibile, precum ștergerea datelor, acceptarea acordurilor legale și invocările AI, sunt înregistrate în tabele de audit dedicate, astfel încât să existe o evidență durabilă a cine a făcut ce asupra datelor importante.

14.2 Backup și recuperare

Baza de date administrată păstrează backup-uri automate, iar stocarea privată este protejată prin retenție soft-delete atât pe blob-uri, cât și pe containere, astfel încât ștergerea accidentală sau malițioasă să poată fi recuperată în interiorul ferestrei de retenție. Infrastructura critică are lock-uri de ștergere pentru a preveni dezafectarea accidentală a resurselor de production.

14.3 Rezumat al responsabilității partajate

Domeniu	AI Interview Analyzer	Client
Infrastructură, rețea, patching	Da	-
Securitatea aplicației și pipeline-ul AI	Da	-
Criptare, secrete, rezidența datelor	Da	-
Administrarea utilizatorilor și rolurilor	Oferă controalele	Gestionează utilizatorii și rolurile
Configurarea politicii de retenție	Oferă controalele	Setează fereastra de retenție
Consimțământul candidatului	Oferă fluxul	Se asigură că este utilizat
Credite puternice pentru utilizatorii finali și SSO	Suportă SSO și politica	Aplică politica internă

15. Modelul de amenințare și maparea OWASP

Proiectăm împotriva unui set concret de adversari: un atacator extern fără credențiale, un utilizator autentificat curios sau malițios al unei organizații care încearcă să ajungă la datele altei organizații, o dependență compromisă și o eroare internă. Tabelul de mai jos mapează categoriile de risc larg utilizate din OWASP Top 10 la controalele specifice care le adresează în această platformă, fiecare dintre acestea fiind verificat prin testarea descrisă în Secțiunea 12.

Risc OWASP	Cum îl atenuează platforma
Broken access control	RBAC pe fiecare endpoint privilegiat; limitare per organizație; „not found” la acces cross-org; remapare de identificatori; matrice de teste cross-org
Cryptographic failures	TLS 1.2+ în tranzit; AES-256 în repaus; hash-uire a parolelor cu bcrypt; secrete într-un vault administrat
Injection	Interogări parametrizate doar prin ORM; validare strictă de schemă; sanitizare HTML la scriere
Insecure design	Apărare în profunzime pe straturi; modelare de amenințări și revizuire de arhitectură în fiecare audit
Security misconfiguration	Infrastructure as code; grupuri de rețea default-deny; header-e de securitate; chei partajate de stocare dezactivate; schema API neexpusă în production
Vulnerable components	Monitorizare automată săptămânală a dependențelor; audituri CVE ale dependențelor în evaluarea periodică
Identification and authentication failures	Token-uri cu durată scurtă de viață; login cu rate limiting; verificare email; suport SSO; fără parole în clar
Software and data integrity failures	Pași de pipeline fixați și imuabili; instalatoare desktop semnate; verificarea semnăturii webhook-urilor; implementări în production controlate prin tag-uri
Security logging and monitoring failures	Telemetrie centralizată; tabele de audit dedicate pentru acțiuni sensibile
Server-side request forgery	Apeluri outbound restricționate la endpoint-uri de încredere; sonde SSRF în cadrul de testare de penetrare

Această mapare este coloana vertebrală a argumentului nostru de asigurare: pentru fiecare clasă cunoscută de atac există un control numit, iar pentru fiecare control numit există un test.

16. Managementul vulnerabilităților și divulgare responsabilă

Securitatea nu este niciodată finalizată, așa că operăm o buclă continuă de descoperire și remediere.

• **Descoperire.** Vulnerabilitățile sunt identificate din patru surse: suita de teste automate, auditurile recurente de testare de penetrare, monitorizarea automată a dependențelor și rapoartele de la clienți sau cercetători.

• **Triere.** Fiecărei constatări i se atribuie o severitate (critical, high, medium, low sau informational), împreună cu dovezi și un responsabil pentru remediere, exact așa cum este consemnat în rapoartele noastre de audit.

• **Ținte de remediere.** Constatările critical și high sunt prioritizate pentru remediere imediată; în istoricul nostru de audit, constatările de severitate mai ridicată au fost de obicei rezolvate și reverificate în aceeași zi. Constatările medium și inferioare sunt programate în cadența regulată de mentenanță.

• **Verificare.** Remedierile sunt retestate și, acolo unde este relevant, se execută o verificare live împotriva mediului implementat pentru a confirma că problema este cu adevărat închisă, nu doar închisă în cod.

• **Divulgare.** Problemele de securitate ne pot fi raportate direct. Confirmăm primirea raportărilor, investigăm și ținem raportorul la curent până la rezolvare.

17. Maparea conformității

17.1 GDPR

Domeniu GDPR	Implementarea în platformă
Temei legal (Art. 6)	Consimțământ explicit al candidatului capturat înainte de prelucrare
Minimizarea datelor și limitarea stocării (Art. 5)	Sunt prelucrate doar date relevante pentru interviu; retenție configurabilă cu ștergere automată
Dreptul la ștergere (Art. 17)	Ștergere ca unitate unică a tuturor datelor candidatului, cu dovadă jurnalizată a ștergerii
Drepturile persoanei vizate (Art. 15 to 20)	Sunt suportate accesul, ștergerea, portabilitatea și opoziția
Obligațiile persoanei împuternicite (Art. 28)	DPA acceptat la înregistrare și versionat per organizație
Securitatea prelucrării (Art. 32)	Criptare, control al accesului, izolare și testare continuă, după cum este descris în acest document
Transparența subîmputerniciților	Divulgată în DPA cu notificare prealabilă privind modificările

17.2 EU AI Act

Platforma este tratată ca un sistem AI high-risk care susține decizii privind ocuparea forței de muncă, iar noi menținem documentație aliniată reglementării, inclusiv un card de transparență, documentație pentru utilizatori și o declarație de conformitate. Măsurile de protecție de bază, supravegherea umană, transparența, scorarea bazată pe dovezi și limitele stricte de domeniu privind ceea ce evaluează AI-ul sunt descrise în Secțiunea 10. Continuăm să maturizăm documentația noastră formală de conformitate pe măsură ce avansează calendarul de implementare al reglementării.

17.3 Certificări de găzduire

Platforma rulează integral pe Microsoft Azure, ale cărui centre de date dețin certificări independente, inclusiv ISO 27001 și SOC 2. Aceste certificări acoperă straturile fizice și de platformă de sub aplicația noastră; controalele la nivel de aplicație sunt cele descrise în întregul acest document.

17.4 Registrul subîmputerniciților

Subîmputernicit	Scop	Regiune
Microsoft Azure	Găzduire, prelucrare AI și speech, stocare, email tranzacțional	UE (West Europe, Sweden Central)
Stripe	Procesarea abonamentelor și plăților	UE (Ireland)
Fakturownia	Facturare	UE (Poland)
Conector ATS (opțional)	Integrare cu sistemul de urmărire a candidaților, activată doar la cerere	UE

18. Foaie de parcurs pentru securitate

Tratăm securitatea ca pe un program de îmbunătățire continuă. Inițiativele curente din foaia noastră de parcurs includ consolidarea opțiunilor de autentificare multi-factor pentru conturile administrative, extinderea jurnalizării centralizate de audit a accesului la date, continuarea înăspririi actualității dependențelor într-o cadență regulată și progresarea certificării formale de către terți a controalelor descrise în acest document. Niciuna dintre acestea nu reprezintă un gol care expune datele clienților astăzi; fiecare este o îmbunătățire a unei posturi deja stratificate.

19. Rezumat

AI Interview Analyzer protejează datele candidaților și ale clienților printr-o arhitectură stratificată: o rețea privată în mod implicit fără servicii publice de date, identitate puternică și izolare per organizație, cod de aplicație care elimină prin design clase întregi de vulnerabilități, criptare și rezidență a datelor în UE și controale de confidențialitate integrate în modelul de date. Ceea ce diferențiază platforma este dovada din spatele acestor afirmații. Cu 3,171 teste automate, o metodologie repetabilă de testare de penetrare live, un program dedicat de siguranță AI și un istoric de șapte audituri interne de securitate cu zero constatări critice, putem demonstra, nu doar afirma, că platforma este securizată.

Anexa A: Catalogul controalelor de securitate

O referință condensată a controalelor principale și a dovezilor care susțin fiecare dintre ele.

Control	Mecanism	Dovezi
Criptarea transportului	Numai HTTPS, TLS 1.2+, HTTP redirecționat	Infrastructure as code; audit de arhitectură
Criptare în repaus	Criptare la nivel de platformă AES-256 pentru stocare și bază de date	Configurarea platformei; audit de arhitectură
Protecția parolelor	bcrypt cu salt per parolă	Control sursă; teste de autentificare
Gestionarea sesiunilor	Token-uri semnate de 30 minute, refresh pe server revocabil	Control sursă; teste de autentificare
Autorizare	Control al accesului cu patru roluri pe endpoint-urile privilegiate	Suită de teste de impunere a rolurilor
Izolarea tenant-ului	Limitarea interogărilor per organizație; 404 la cross-org	Matrice de teste cross-organization
Securitatea cheilor API	Stocare hash-uită, permisiuni cu scope, rate limiting per cheie	Suită de teste pentru chei API
Protecție împotriva injecției	Interogări parametrizate doar prin ORM	Analiză statică; teste de injecție
Protecție împotriva cross-site scripting	Sanitizare HTML la momentul scrierii	Suită de teste de sanitizare HTML
Rate limiting	Limiter durabil bazat pe bază de date pe endpoint-urile auth	Teste de rate-limit; verificări live de burst
Integritatea webhook-urilor	Verificarea semnăturii furnizorului pe corpul brut	Suită de teste pentru webhook
Gestionarea secretelor	Vault administrat, purge protection, managed identity	Infrastructure as code; audit de arhitectură
Izolarea rețelei	Endpoint-uri private; segmentare default-deny	Infrastructure as code; audit de arhitectură
Ștergerea datelor	Ștergere în cascadă ca unitate unică cu jurnal de audit	Suită de teste GDPR pentru ștergere
Supply chain	Pași de pipeline fixați; monitorizare săptămânală a dependențelor	Configurarea pipeline-ului; audit al dependențelor

Anexa B: Întrebări frecvente pentru evaluatorii de securitate

Unde sunt stocate datele noastre? Integral în Uniunea Europeană, pe Microsoft Azure, în West Europe, cu prelucrare AI în regiuni din UE. Datele candidaților nu părăsesc niciodată UE.

Sunt datele noastre folosite pentru antrenarea modelelor AI? Nu. Furnizorul AI nu folosește datele clienților pentru antrenare.

Este baza de date accesibilă de pe internet? Nu. Accesul la rețeaua publică este dezactivat, iar baza de date este accesibilă doar printr-un endpoint privat din interiorul rețelei virtuale.

Poate un client să vadă datele altui client? Nu. Fiecare interogare este limitată la organizația apelantului, accesul cross-organization returnează „not found”, iar o matrice automată testează continuu această izolare.

Cum sunt stocate parolele? Hash-uite cu bcrypt și un salt unic per parolă. Este suportat single sign-on cu Microsoft și Google, caz în care nu se stochează nicio parolă.

Suportați single sign-on? Da, prin Microsoft și Google OAuth.

Cât timp sunt valabile access token-urile? Treizeci de minute, asociate cu o sesiune de refresh revocabilă pe server care este invalidată la logout.

Cum este gestionat consimțământul candidatului? Fiecare candidat primește un link unic de consimțământ, de unică folosință, și trebuie să accepte înainte de orice înregistrare sau analiză. Consimțământul este înregistrat pentru procesul specific de angajare.

Cum sunt șterse datele? Ca o singură unitate care acoperă înregistrarea candidatului, interviurile, transcrierile, audio-ul, documentele și comparațiile, într-un program de retenție configurabil, cu o dovadă jurnalizată a ștergerii. Candidații pot solicita de asemenea ștergerea direct.

Aveți un DPA? Da, acceptat la înregistrare și versionat per organizație, inclusiv registrul subîmputerniciților.

AI-ul ia decizii de angajare? Nu. Oferă doar suport decizional; un om revizuiește fiecare rezultat și ia toate deciziile.

Cum dovediți afirmațiile de securitate? Prin 3,171 teste automate, inclusiv o suită dedicată de securitate, o metodologie repetabilă în șase faze de testare de penetrare rulată împotriva mediilor live, un program de testare a siguranței AI și rapoarte scrise de audit recurente.

Ce se întâmplă când găsiți o vulnerabilitate? I se atribuie o severitate împreună cu dovezi și un responsabil, este remediată conform unui calendar de prioritate, este reverificată, inclusiv prin verificări live unde este relevant, și este consemnată într-un raport de audit.

Putem efectua propriul nostru test de penetrare? Evaluările de securitate pot fi organizate prin reprezentantul dumneavoastră de cont, în condiții de domeniu și programare adecvate.

Anexa C: Glosar

Termen	Semnificație
AES-256	Un standard puternic de criptare simetrică utilizat pentru a proteja datele în repaus
bcrypt	O funcție de hash-uire a parolelor construită special, cu salting per parolă
Managed identity	O identitate emisă de platformă care permite unui serviciu să se autentifice fără chei stocate
Private endpoint	O adresă de rețea privată care menține un serviciu cloud în afara internetului public
Network security group	Un set de reguli de permitere și refuz care filtrează traficul de rețea către un subnet
RBAC	Role-based access control, acordarea permisiunilor în funcție de rolul unui utilizator
IDOR	Insecure direct object reference, un defect de control al accesului împotriva căruia platforma se apără
SSRF	Server-side request forgery, o clasă de atac sondată în testele noastre de penetrare
Web application firewall	Un control edge care filtrează traficul web malițios
Data processing agreement	Contractul care guvernează modul în care o persoană împuternicită prelucrează date cu caracter personal în numele unui operator

Anexa D: Contact și controlul documentului

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Pentru o evaluare de securitate, o copie a DPA-ului nostru sau documentația noastră de conformitate EU AI Act, vă rugăm să contactați reprezentantul dumneavoastră de cont.

Acest document descrie postura de securitate a serviciului AI Interview Analyzer la data generării indicată în subsol. Este furnizat în scopuri de evaluare și nu face parte din niciun contract. Angajamentele contractuale specifice privind securitatea sunt prevăzute în acordul aplicabil și în DPA.