Whitepaper sulla Sicurezza

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Whitepaper sulla Sicurezza

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

Destinatari: team di sicurezza enterprise, IT e procurement

Classificazione: Pubblico

1. Sintesi Esecutiva

AI Interview Analyzer è una piattaforma enterprise per le assunzioni che registra i colloqui con il consenso esplicito del candidato, li trascrive e li struttura, e produce supporto alla valutazione basato su evidenze per i recruiter. Poiché la piattaforma gestisce dati personali dei candidati e supporta i processi di assunzione, sicurezza e privacy sono trattate come vincoli progettuali primari, non come funzionalità aggiunte successivamente.

Questo whitepaper descrive, in termini concreti e verificabili, come proteggiamo i dati dei clienti e dei candidati. È scritto per le persone che valutano i fornitori: ingegneri della sicurezza, amministratori IT, responsabili della protezione dei dati e procurement. Ogni dato riportato in questo documento proviene direttamente dai nostri sistemi di ingegneria, e non da materiale di marketing.

Il messaggio centrale è semplice: **non ci limitiamo ad affermare che la piattaforma è sicura, la verifichiamo continuamente.** Il nostro codebase contiene **3,171 test automatizzati**, inclusa una suite di sicurezza dedicata che verifica autenticazione, autorizzazione, isolamento tra organizzazioni, difese contro le injection e cancellazione dei dati. Inoltre, eseguiamo un framework ripetibile di penetration testing contro deployment live e produciamo report di audit scritti. In sette audit di sicurezza interni tra marzo e aprile 2026, abbiamo registrato **zero critical findings**, con il nostro audit più recente concluso con un verdetto di **PASS**. (La certificazione formale di terze parti di questi controlli è nella nostra roadmap; vedere la Sezione 18.)

Caratteristica di sicurezza	Sintesi
Hosting	Microsoft Azure, solo regioni UE
Modello di rete	Endpoint privati, segmentazione di rete default-deny, nessun database pubblico
Crittografia	AES-256 at rest, TLS 1.2 o superiore in transito
Identità	Token firmati a breve durata, hashing delle password con bcrypt, supporto SSO
Controllo degli accessi	Controllo degli accessi basato sui ruoli con rigoroso isolamento per organizzazione
Secrets	Vault centralizzato dei secrets con accesso tramite managed identity
Privacy	Consenso esplicito, retention configurabile, cancellazione come unità singola
AI responsabile	Solo supporto decisionale, essere umano sempre nel loop
Assurance	3,171 test automatizzati più penetration test e audit ricorrenti

1.1 Come Leggere Questo Documento

Le Sezioni da 3 a 11 descrivono i controlli che proteggono i dati: architettura, rete, identità, applicazione, protezione dei dati, privacy e ciclo di vita di sviluppo sicuro. Le Sezioni 12 e 13 trattano il nostro distintivo programma di test continui e la nostra cronologia di audit. Le Sezioni da 14 a 17 trattano operazioni, threat modeling, gestione delle vulnerabilità e mappatura di compliance. Le appendici forniscono un catalogo dei controlli, una FAQ per i revisori e un glossario che un team di sicurezza può usare direttamente durante una valutazione.

2. Ambito del Documento e Approccio

2.1 Cosa Copre Questo Documento

Questo whitepaper copre l'architettura di sicurezza e le pratiche del servizio AI Interview Analyzer: l'ambiente di hosting, il design della rete, la gestione delle identità e degli accessi, i controlli a livello applicativo, la protezione dei dati, la privacy e l'allineamento normativo, il ciclo di vita di sviluppo sicuro e il nostro programma continuo di security testing.

2.2 Cosa lo Rende Verificabile

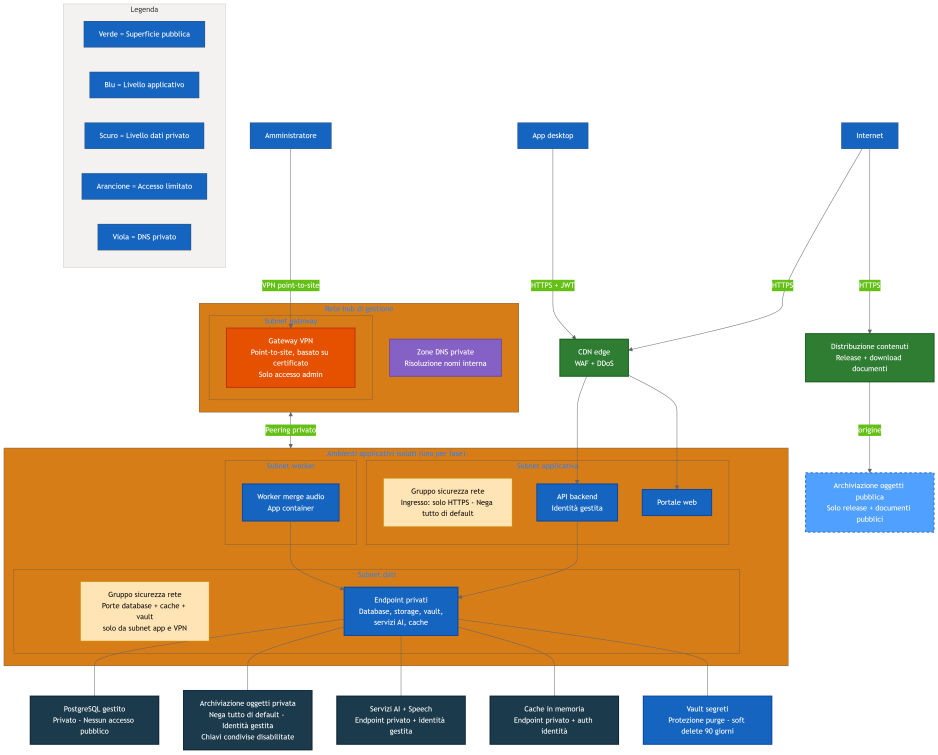
Le dichiarazioni di sicurezza dei fornitori sono facili da scrivere e difficili da considerare affidabili. Per questo motivo abbiamo collegato ogni affermazione principale di questo documento a qualcosa di concreto e misurabile all'interno dei nostri sistemi di ingegneria: un controllo implementato nel codice, un test che dimostra che il controllo funziona, una definizione infrastrutturale che lo impone oppure un report di audit che registra una verifica documentata. Quando un controllo fa parte della nostra roadmap futura anziché essere già disponibile oggi, lo dichiariamo esplicitamente. Preferiamo fare affermazioni prudenti ed essere ritenuti affidabili piuttosto che esagerare ed essere smentiti.

2.3 Responsabilità Condivisa

La piattaforma è erogata come software as a service. Noi gestiamo l'infrastruttura, l'applicazione, la pipeline AI e il trattamento dei dati. Il cliente è responsabile della gestione dei propri account utente e ruoli, della configurazione delle finestre di data retention in linea con la propria policy interna e dell'assicurare che il consenso del candidato sia ottenuto tramite il workflow di consenso fornito dalla piattaforma. La Sezione 14 descrive questa suddivisione in maggiore dettaglio.

3. Panoramica dell'Architettura di Sicurezza

La piattaforma è costruita come un numero limitato di servizi cooperanti anziché come un singolo monolite. Un'applicazione desktop e un portale web agiscono come client. Un backend API centrale gestisce tutta la persistenza, l'autenticazione, la fatturazione, la pipeline AI, il consenso, l'email, la gestione dei file e le dashboard. Un worker di merge audio elabora le registrazioni in modo asincrono. Tutto lo stato sensibile risiede dietro il backend API; i client non parlano mai direttamente con il database, lo storage o i servizi AI.



Il diagramma sopra mostra la topologia di produzione con nomi delle risorse intenzionalmente generalizzati. In esso sono visibili tre principi:

- **Nessuna esposizione diretta dei servizi dati.** Il database, l'object storage privato, i servizi AI e la cache hanno l'accesso alla rete pubblica disabilitato e sono raggiungibili solo tramite endpoint privati all'interno di una virtual network isolata. Il vault dei secrets è raggiunto dall'applicazione tramite un endpoint privato ed è ulteriormente protetto dall'autenticazione dell'identità della piattaforma e da policy di accesso least-privilege, per cui ogni accesso richiede un'identità valida e autorizzata indipendentemente dal percorso di rete.
- **Una superficie pubblica separata.** L'unico object storage pubblico contiene download di release e documenti pubblici. Non contiene mai dati dei candidati. Il traffico applicativo rivolto ai clienti passa attraverso un layer edge che fornisce web application firewall, protezione distributed-denial-of-service e content delivery.
- **L'accesso amministrativo è protetto.** Gli operatori raggiungono le risorse interne solo tramite una VPN point-to-site basata su certificati verso una management hub network, non tramite Internet pubblico.

Ogni fase di deployment (development e production) è un ambiente completamente isolato con la propria rete, storage account, database e secrets. I dati di produzione dei clienti non sono mai presenti negli ambienti inferiori. Un management hub condiviso contiene solo il gateway VPN e il DNS privato, con peering privato verso ciascun ambiente.

---

4. Defense in Depth

Nessun singolo controllo è considerato sufficiente a fermare ogni attacco. La piattaforma stratifica controlli indipendenti in modo che il fallimento di uno qualsiasi dei livelli non esponga i dati. I livelli sottostanti sono ciascuno implementati e, come descritto nella Sezione 12, testati individualmente.

Modello di sicurezza a livelli: controlli indipendenti a ogni livello

Livello	Controlli rappresentativi
Edge di rete	Trasporto solo TLS, WAF e protezione DDoS all'edge, endpoint privati, segmentazione default-deny
Identità e accesso	Token firmati a breve durata, hashing bcrypt, controllo degli accessi basato sui ruoli, isolamento per organizzazione
Applicazione	Validazione dello schema su tutti gli input, accesso ai dati solo tramite ORM, codifica dell'output, rate limiting
Protezione dei dati	Crittografia at rest, vault dei secrets con managed identity, residenza dei dati nell'UE, trattamento subordinato al consenso
Governance e privacy	Retention configurabile, cancellazione come unità singola, AI human-in-the-loop, audit logging
Assurance continua	Suite di test automatizzati, penetration test ripetibili, audit di sicurezza interni ricorrenti

Il resto di questo documento esamina ciascun livello a turno e poi descrive come dimostriamo, in modo continuo, che i livelli restano efficaci.

5. Sicurezza di Rete

5.1 Privato per Impostazione Predefinita

Il livello dati è privato per costruzione. Il database PostgreSQL gestito ha l'accesso alla rete pubblica disabilitato ed è raggiungibile solo tramite un endpoint privato. L'object storage privato è configurato per negare l'accesso di rete per impostazione predefinita, disabilita completamente le shared access keys ed è accessibile solo tramite managed identity dalla subnet applicativa. Anche la cache, i servizi AI e il vault dei secrets sono raggiunti tramite endpoint privati con risoluzione DNS privata.

In pratica, questo significa che non esiste alcuna connection string esposta su Internet verso il database e nessun URL pubblico di storage per l'audio dei candidati: il database e lo storage privato hanno l'accesso alla rete pubblica disabilitato in modo assoluto. Il vault dei secrets è raggiunto dall'applicazione tramite un endpoint privato ed è protetto dall'autenticazione dell'identità della piattaforma e da policy di accesso least-privilege, con identità applicative a cui è concesso accesso in sola lettura solo ai secrets di cui hanno bisogno, per cui i secrets non possono essere recuperati senza un'identità valida e autorizzata. La superficie d'attacco che un avversario esterno può anche solo toccare è limitata agli endpoint HTTPS dell'applicazione dietro il layer edge.

5.2 Segmentazione di Rete

Ogni ambiente è suddiviso in subnet separate per il livello applicativo, il livello dati e il worker asincrono. Ogni subnet è governata da un network security group la cui regola finale nega tutto il traffico in ingresso. La subnet applicativa accetta solo traffico HTTPS in ingresso. La subnet dati accetta solo le specifiche porte di database, cache e vault, e solo dalla subnet applicativa o dalla VPN amministrativa. Questo significa che anche un attaccante che riuscisse in qualche modo a raggiungere il livello applicativo non potrebbe muoversi liberamente verso il livello dati; gli unici percorsi consentiti sono quelli che l'applicazione usa legittimamente.

5.3 L'Edge

Il traffico applicativo pubblico è posto davanti a un layer edge che fornisce web application firewall, protezione DDoS e una content delivery network. I download di release e documenti sono serviti da un public storage account dedicato tramite un front door di content delivery, completamente separato dallo storage privato che contiene i dati dei candidati. I due piani di storage non si mescolano mai: una configurazione errata sul piano pubblico non può esporre dati privati dei candidati, perché si tratta di account diversi con regole di rete differenti.

5.4 Accesso Amministrativo

Non esiste alcun endpoint amministrativo pubblico verso la rete privata. Gli operatori si connettono tramite un gateway VPN point-to-site che utilizza autenticazione basata su certificati. L'accesso amministrativo a database e cache è possibile solo dall'interno di quel tunnel, poiché tali servizi hanno l'accesso alla rete pubblica disabilitato. Questo mantiene le operazioni quotidiane completamente fuori da Internet pubblico.

6. Gestione delle Identità e degli Accessi

6.1 Autenticazione

Le sessioni utente vengono stabilite con un access token firmato valido per trenta minuti, abbinato a un refresh token separato, opaco e lato server. Gli access token vengono verificati a ogni richiesta e l'utente viene nuovamente validato rispetto al database (incluso un controllo di account attivo) anziché essere considerato affidabile solo sulla base del contenuto del token. Il logout revoca immediatamente la sessione di refresh lato server, per cui un refresh token rubato non può sopravvivere al logout.

Le password non vengono mai archiviate in chiaro. Sono sottoposte ad hashing con bcrypt utilizzando un salt univoco per password. Per le organizzazioni che preferiscono il single sign-on, la piattaforma supporta il login OAuth con Microsoft e Google, nel qual caso non viene conservata alcuna password.

La titolarità dell'indirizzo email viene verificata tramite un link di verifica monouso e a tempo limitato prima che un account auto-registrato sia considerato verificato, e i reinvii dell'email di verifica sono soggetti a rate limiting per prevenire abusi.

6.2 Controllo degli Accessi Basato sui Ruoli

L'autorizzazione è applicata tramite un modello di ruoli con quattro ruoli a privilegio crescente: interviewer, hiring manager, recruiter e administrator. L'accesso a operazioni privilegiate è imposto da dipendenze lato server che verificano sia il ruolo sia lo stato di verifica del chiamante. Questi controlli di ruolo proteggono ben oltre cento distinte operazioni API.

Ruolo	Capacità tipiche
Interviewer	Conduce i colloqui assegnati; vede solo i colloqui assegnati a lui/lei
Hiring manager	Gestisce le selezioni di cui è proprietario o membro
Recruiter	Gestione completa di selezioni e candidati all'interno dell'organizzazione
Administrator	Impostazioni dell'organizzazione, fatturazione, amministrazione di utenti e API key

Oltre ai controlli di ruolo di alto livello, la piattaforma applica regole di visibilità a livello di dati. Gli hiring manager vedono solo le selezioni che hanno creato o di cui sono membri; gli interviewer vedono solo i colloqui a loro assegnati. Il privilegio è quindi applicato sia al livello di "quale azione" sia al livello di "quali record".

6.3 Isolamento per Organizzazione

La piattaforma è multi-tenant e l'isolamento dei tenant è trattato come un controllo di sicurezza di prima classe. Ogni identità autenticata porta con sé un identificatore di organizzazione e le query sui dati sono limitate a quell'organizzazione. Quando un utente richiede un record che appartiene a un'altra organizzazione, la piattaforma restituisce una risposta "not found" invece di rivelare che il record esiste. Gli identificatori interni del database non sono mai esposti sul wire; l'API presenta display identifier e li rimappa per ogni richiesta, eliminando così una classe comune di attacchi di enumerazione cross-tenant.

Questo non è solo un intento progettuale. Come descritto nella Sezione 12, la nostra suite automatizzata esegue una vasta matrice cross-organization che tenta di raggiungere i dati di un'organizzazione utilizzando le credenziali di un'altra organizzazione e verifica che ogni tentativo fallisca.

6.4 Accesso Programmatico

Per le integrazioni, le organizzazioni con piani idonei possono emettere API key. Le chiavi usano un prefisso riconoscibile, contengono 128 bit di entropia e sono archiviate solo come hash; la chiave grezza viene mostrata una sola volta al momento della creazione e mai più. Ogni chiave ha un esplicito permission scope (read, write o integrazione ATS), può essere limitata a specifiche reti di origine, può essere revocata istantaneamente ed è soggetta a limiti di frequenza per chiave derivati dal livello di piano dell'organizzazione. La verifica delle chiavi usa un confronto timing-safe per evitare la divulgazione di informazioni tramite il tempo di risposta.

7. Sicurezza dell'Applicazione

L'applicazione è scritta in modo da eliminare intere categorie di vulnerabilità anziché correggerle caso per caso.

- **Injection.** Tutto l'accesso al database passa attraverso un object-relational mapper con query parametrizzate. Il codebase non contiene SQL grezzo formattato come stringa. Questo elimina strutturalmente la SQL injection.
- **Validazione dell'input.** Ogni body di richiesta viene validato rispetto a uno schema rigoroso prima di raggiungere la business logic. I payload eccessivamente grandi vengono rifiutati e gli endpoint di lista sono paginati per limitare l'uso delle risorse.
- **Codifica dell'output e cross-site scripting.** Il testo fornito dall'utente e quello generato dall'AI sono trattati come non affidabili. Dove il contenuto deve essere reso come HTML, passa attraverso un sanitizer allow-list in fase di scrittura, e una suite di test dedicata conferma che tag script, event handler e URL javascript vengano rimossi.
- **Mass assignment.** Le operazioni di aggiornamento usano schemi espliciti che escludono campi privilegiati come ruolo, organizzazione e saldo crediti, per cui un client non può aumentare i propri privilegi pubblicando campi aggiuntivi.
- **Rate limiting.** Gli endpoint di autenticazione e soggetti ad abuso sono protetti da rate limiting usando un limiter durevole, supportato dal database, che sopravvive ai riavvii e funziona correttamente su più istanze applicative. Login, registrazione, reset della password e reinvio della verifica hanno ciascuno i propri limiti. La risoluzione dell'IP del client è rafforzata contro lo spoofing degli header di forwarding.
- **Webhook.** I webhook in ingresso dai provider di pagamento ed email vengono verificati rispetto alle firme del provider sul body grezzo della richiesta prima di essere elaborati.
- **Upload di file.** Gli upload hanno limiti di dimensione, vengono validati, archiviati sotto identificatori generati anziché nomi forniti dall'utente e limitati per richiesta e per organizzazione.
- **Header di sicurezza.** In produzione, le risposte includono strict transport security, opzioni content-type e frame, una referrer policy e una permissions policy restrittiva, e sopprimono i banner del server e del framework.

8. Protezione dei Dati

8.1 Crittografia

Tutti i dati sono crittografati at rest usando AES-256 tramite i layer di crittografia della piattaforma Azure per storage e database. Tutto il traffico di rete è servito esclusivamente su HTTPS usando TLS 1.2 o superiore; HTTP in chiaro viene reindirizzato a HTTPS a ogni livello. In produzione, l'API e il portale web emettono header strict transport security insieme a un insieme di header di hardening, e sopprimono i banner di versione di server e framework.

8.2 Gestione dei Secrets

I secrets dell'applicazione sono conservati in un vault centralizzato dei secrets con purge protection abilitata e una finestra di soft-delete di novanta giorni. Le applicazioni si autenticano alle risorse Azure usando system-assigned managed identities anziché chiavi a lunga durata; per esempio, lo storage privato ha le shared access keys completamente disabilitate, per cui l'accesso è possibile solo tramite assegnazioni di ruolo basate su identità limitate alla singola risorsa. Le policy di accesso al vault concedono ai principal applicativi accesso in sola lettura ai secrets specifici di cui hanno bisogno, seguendo il principio del least privilege.

8.3 Residenza dei Dati

Tutti i dati di clienti e candidati sono archiviati ed elaborati all'interno dell'Unione Europea. L'hosting dell'applicazione, il database, lo storage, la cache e i secrets risiedono in West Europe, e l'elaborazione AI avviene in regioni UE. Il provider AI non utilizza i dati dei clienti per addestrare i propri modelli.

8.4 Il Ciclo di Vita di un Singolo Colloquio

Il modo più chiaro per comprendere i controlli di protezione dei dati è seguire un colloquio dall'inizio alla fine. Il consenso viene acquisito e registrato prima che qualsiasi cosa venga elaborata. L'upload è crittografato in transito. Trascrizione e analisi vengono eseguite all'interno di data center UE. I risultati vengono scritti su storage crittografato. Ogni record è quindi governato da un unico retention clock che termina con una cancellazione a cascata registrata. In qualsiasi momento, i diritti del candidato come revoca, cancellazione, accesso o portabilità possono interrompere questo flusso.

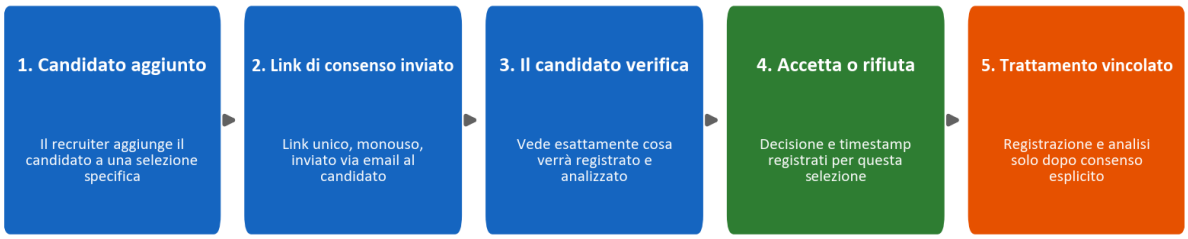
9. Privacy by Design e GDPR

La privacy è incorporata nel modello dei dati e nel workflow, non aggiunta solo tramite policy.

9.1 Consenso

Nessun colloquio viene registrato o analizzato senza il consenso esplicito del candidato. Quando un candidato viene aggiunto a una selezione, la piattaforma invia via email un link di consenso univoco e monouso. Il candidato esamina ciò che accadrà e accetta o rifiuta. Lo stato del consenso, incluso il momento della risposta, viene registrato rispetto a quella specifica selezione, quindi il consenso è sempre limitato a un processo di assunzione concreto anziché essere concesso globalmente.

Consenso candidato: esplicito e registrato prima di ogni trattamento

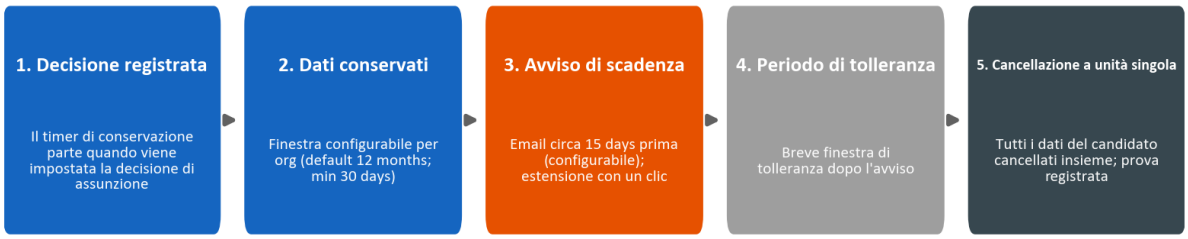


9.2 Retention e Cancellazione

La data retention è configurabile per organizzazione, con un valore predefinito di dodici mesi e un minimo configurabile di trenta giorni, e può essere sovrascritta per candidato. Esiste un unico retention clock per i dati di un candidato, non un timer separato per ogni artefatto. Il timer inizia quando viene registrata una decisione di assunzione. Prima che i dati scadano, la piattaforma invia un avviso (di default circa quindici giorni prima) e offre un'estensione con un clic. Quando i dati vengono cancellati, vengono cancellati come un'unità singola: il record del candidato, i colloqui, le trascrizioni, le registrazioni audio, i documenti e i confronti vengono tutti rimossi insieme, e la cancellazione viene registrata in un audit log. Non esistono residui parziali o orfani.

Il ciclo di vita sottostante mostra questo unico timer e come converga in una sola cancellazione a cascata con una prova registrata di cancellazione.

Conservazione dati: un timer per candidato, cancellazione a unità singola



9.3 Diritti dell'Interessato e Sub-processor

La piattaforma supporta i diritti dell'interessato richiesti dal GDPR, inclusi accesso, cancellazione, portabilità, opposizione e spiegazione. Il trattamento viene svolto nell'ambito di un data processing agreement che i clienti accettano al momento della registrazione e che è versionato per organizzazione. I nostri sub-processor e i loro ruoli, tutti all'interno dell'UE o soggetti a

garanzie appropriate, sono divulgati in tale accordo, e i clienti ricevono preavviso di qualsiasi modifica. La Sezione 17 contiene il registro dei sub-processor e la mappatura di compliance articolo per articolo.

10. AI Responsabile e EU AI Act

La piattaforma rientra nella categoria high-risk del EU AI Act perché supporta decisioni in materia di occupazione, e trattiamo tale classificazione con serietà.

La regola fondamentale del prodotto è che **l'AI è supporto decisionale, non un decisore.** Il sistema non accetta né rifiuta mai automaticamente un candidato. Trascrive il parlato, struttura domande e risposte, assegna punteggi alle risposte rispetto ai criteri definiti dal recruiter e redige feedback, e un essere umano esamina ogni output prima che venga utilizzato. Questo mantiene saldamente un essere umano nel loop.

È altrettanto importante ciò che l'AI non fa. Non valuta personalità, "cultural fit", stato emotivo, tono di voce, accento, genere, età, etnia, aspetto o linguaggio del corpo. Il punteggio è ancorato alle evidenze della trascrizione e ai criteri definiti dal recruiter, e i nomi dei candidati sono esclusi dall'input di valutazione per ridurre i bias. Pubblichiamo una transparency card, documentazione utente e una dichiarazione di conformità che descrivono il sistema, i suoi limiti e le sue salvaguardie.

Controllo di AI responsabile	Come funziona
Human in the loop	Ogni punteggio e ogni feedback vengono esaminati da un recruiter prima dell'uso
Nessuna decisione automatizzata	Il sistema non accetta né rifiuta automaticamente un candidato
Punteggio basato su evidenze	I punteggi fanno riferimento a evidenze di supporto dalla trascrizione
Progettazione anti-bias	Nomi esclusi dalla valutazione; viene valutata la sostanza più dello stile
Limiti di ambito	Personalità, emozione, accento e caratteristiche protette non vengono mai valutati
Sicurezza del feedback al candidato	Il feedback privato al candidato passa attraverso un guardrail di sicurezza di generazione e validazione

Questi vincoli non sono solo dichiarati nella documentazione; sono codificati nel prompt layer dell'AI e verificati da un programma di test dedicato alla sicurezza AI descritto nella Sezione 12.3.

11. Ciclo di Vita di Sviluppo Sicuro

La sicurezza è imposta nel modo in cui costruiamo e rilasciamo il software, non solo nel sistema in esecuzione.

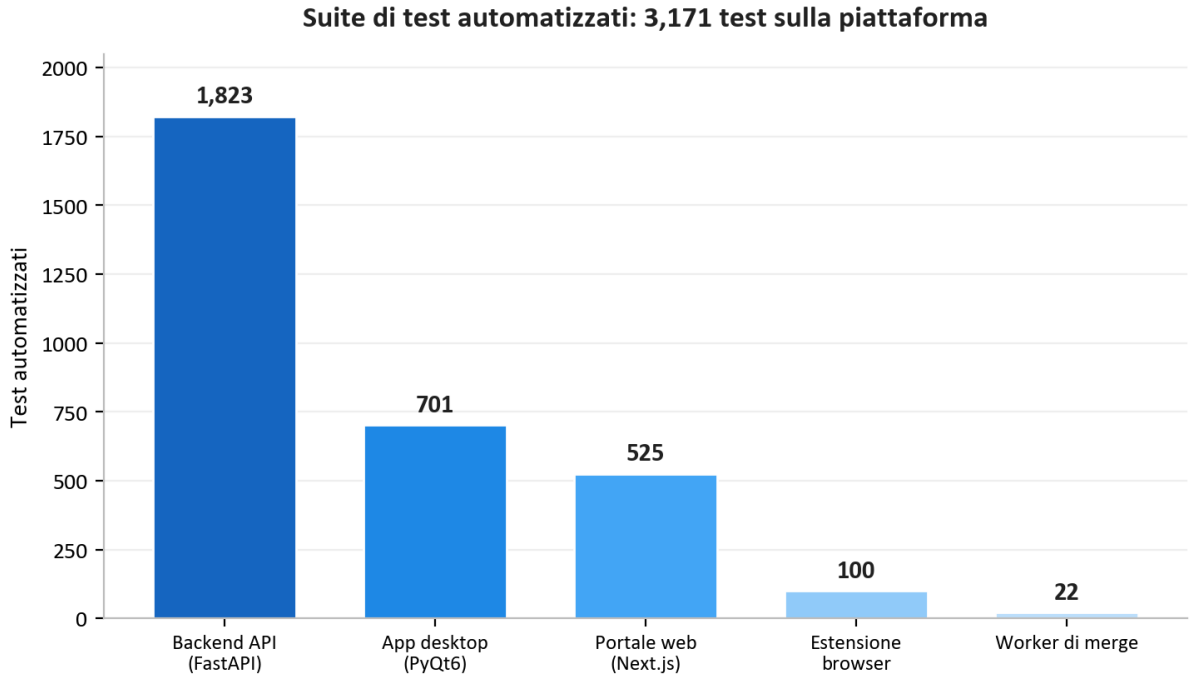
- **Separazione degli ambienti.** Development e production sono completamente separati, ciascuno con la propria infrastruttura, storage account, database, secrets e sottodomini. Non esiste stato condiviso.
- **Infrastructure as code.** L'intero ambiente cloud è definito come codice e revisionato come codice, il che rende la postura di sicurezza verificabile e riproducibile. Un revisore può leggere esattamente quali porte sono aperte, quali risorse sono private e quali identità dispongono di quali permessi.
- **Deployment pinned e protetti.** Ogni fase della pipeline di continuous integration è fissata a una versione esatta e immutabile. I deployment di produzione sono basati su tag, vengono eseguiti solo attraverso la pipeline di produzione protetta e sono subordinati ad approvazione obbligatoria. La suite di test automatizzati funge da release gate: un deployment non può essere rilasciato se i test falliscono.
- **Igiene delle dipendenze.** Il monitoraggio automatizzato delle dipendenze propone aggiornamenti settimanali per backend, desktop, web, infrastruttura e definizioni di pipeline, e gli audit delle dipendenze fanno parte della nostra revisione periodica della sicurezza.
- **Artefatti firmati.** Gli installer desktop sono firmati digitalmente, così i clienti possono verificare che il software che installano provenga effettivamente da noi.
- **Disciplina dei secrets.** I secrets risiedono nel vault e nei secrets protetti della pipeline, mai nel codice sorgente.

12. Security Testing Continuo

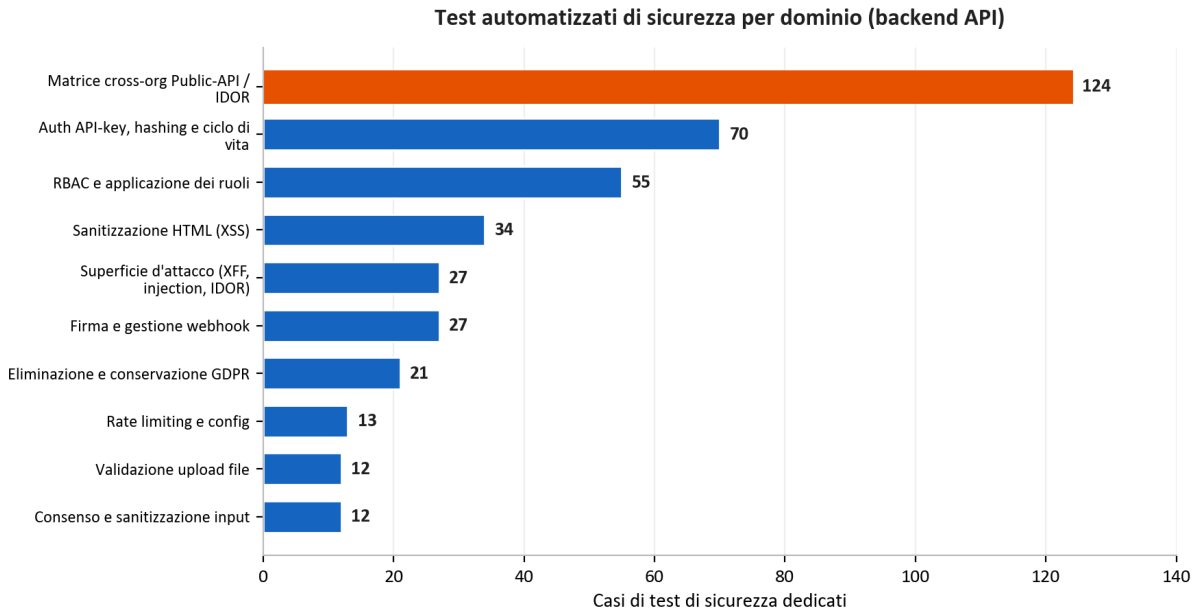
Questo è il cuore del nostro approccio di assurance e la parte che la maggior parte dei fornitori non può mostrare. Trattiamo la sicurezza come qualcosa da misurare continuamente, con controlli eseguibili, anziché da affermare una sola volta.

12.1 La Suite di Test Automatizzati

La piattaforma è coperta da **3,171 test automatizzati** che si estendono al backend API, all'applicazione desktop, al portale web, all'estensione del browser e al worker di merge audio.



Non si tratta solo di test funzionali. Una sostanziale suite di sicurezza dedicata verifica i controlli descritti in precedenza in questo documento. Il grafico seguente suddivide i test specifici di sicurezza nel backend API per dominio.



Tra molti altri, questa suite include un'ampia matrice della public API che esegue ogni endpoint come utente legittimo, come API key della propria organizzazione e come API key di un'organizzazione rivale, verificando che ogni tentativo cross-organization venga bloccato. Include decine di test avversariali sulla attack surface per spoofing di forwarding header, header injection e leakage di identificatori, una suite focalizzata di sanitizzazione HTML per il cross-site scripting, test di enforcement dei ruoli per l'intero modello di ruoli e test che dimostrano che i dati del candidato vengono realmente cancellati come unità. Poiché questi test vengono eseguiti come release gate, una regressione che indebolisse uno qualsiasi di questi controlli fermerebbe la release invece di raggiungere i clienti.

12.2 Live Penetration Testing

I test unitari automatizzati dimostrano che i controlli si comportano correttamente in isolamento. Per dimostrare che funzionano insieme in un deployment reale, manteniamo una metodologia ripetibile di penetration testing che esegue veri script di attacco contro un ambiente live. È organizzata in sei fasi:

Fase	Focus	Esempi di ciò che viene verificato
1. Analisi statica	Codice sorgente	Secrets, pattern di injection, funzioni pericolose, auth mancante, HTML non sicuro
2. Revisione dell'architettura	Infrastruttura	Endpoint privati, segmentazione, TLS, configurazione dei secrets
3. Analisi dei vettori di attacco	Source control e cloud	Protezione dei branch, scope delle identità, esposizione pubblica
4. Live penetration testing	Ambiente in esecuzione	Probing non autenticato, accesso cross-org, injection, manomissione dei token, SSRF, burst sui limiti di frequenza
5. Scoring enterprise	Maturità	Sedici categorie di sicurezza valutate rispetto a una baseline enterprise
6. Dipendenze e supply chain	Rischio di terze parti	Audit CVE delle dipendenze, azioni di pipeline pinned, integrità del lock file

La Fase 4 è un vero test avversariale contro un sistema distribuito, non una checklist. Sonda endpoint protetti senza credenziali e conferma che rifiutino l'accesso; registra due organizzazioni e tenta di raggiungere i record di una organizzazione con l'account dell'altra; inietta payload di cross-site-scripting e server-side-template e conferma che vengano neutralizzati; manomette i token di autenticazione e conferma che vengano rifiutati; tenta server-side request forgery contro endpoint di metadata cloud; e genera burst sugli endpoint di autenticazione per confermare che il rate limiting si attivi realmente nell'ambiente live, non solo in teoria.

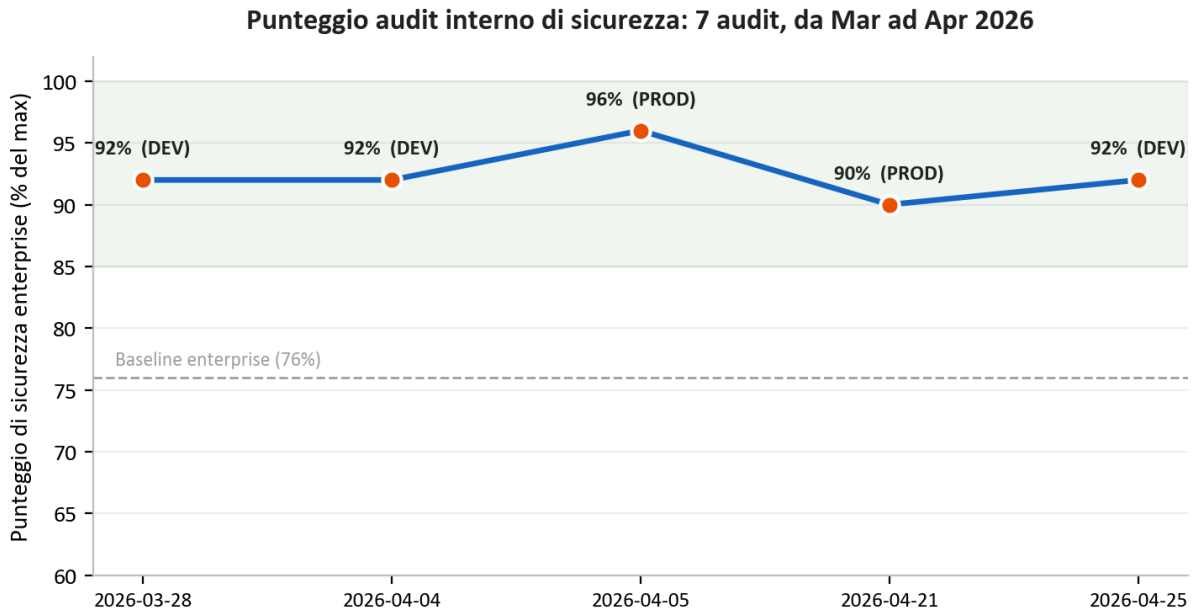
12.3 Test di Sicurezza del Feedback al Candidato

Poiché la piattaforma può generare feedback privato di sviluppo per i candidati, eseguiamo un programma di sicurezza avversariale separato su questa funzionalità. Alimenta deliberatamente il sistema con note dei recruiter dure e ostili e conferma che l'output rivolto al candidato non contenga mai volgarità, non riveli né attribuisca mai l'identità o l'opinione privata di un recruiter e non applichi mai etichette giudicanti sulla personalità. Questo protegge sia il candidato, che dovrebbe ricevere feedback costruttivo e rispettoso, sia il cliente, che non dovrebbe mai vedere una opinione interna trapelare verso l'esterno.

---

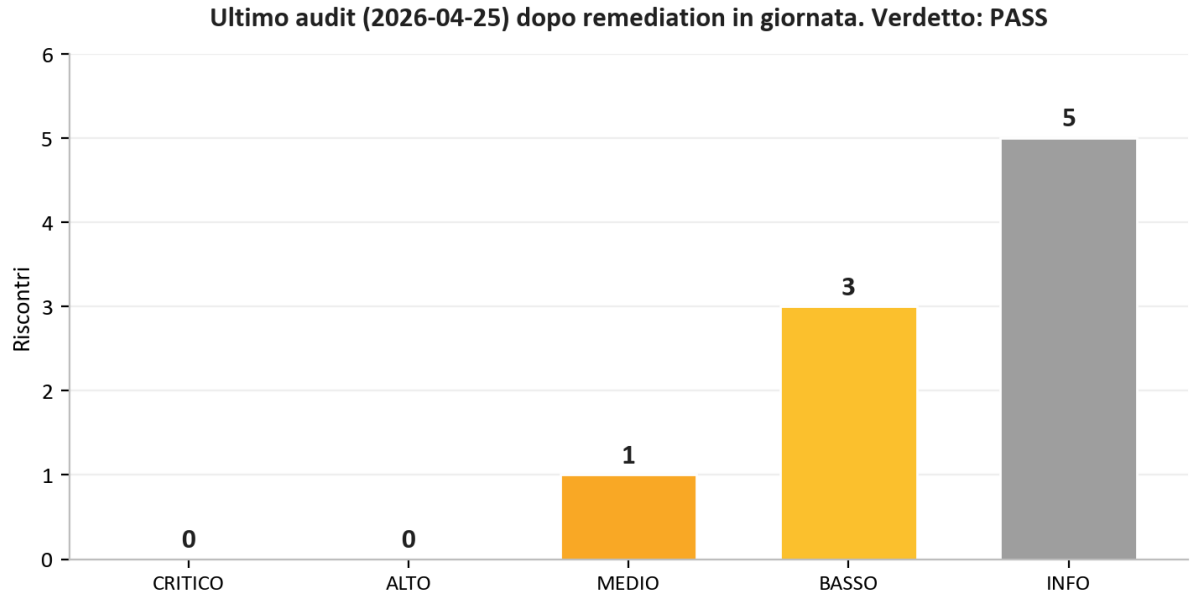
13. Risultati degli Audit di Sicurezza

Conduciamo audit di sicurezza ricorrenti usando una metodologia strutturata e ripetibile di penetration testing, e documentiamo ciascuno di essi in un report datato con finding classificati per severità, evidenze e remediation. Si tratta di audit interni eseguiti dal nostro stesso processo di sicurezza; la certificazione formale di terze parti degli stessi controlli è nella nostra roadmap. Tra la fine di marzo e la fine di aprile 2026 abbiamo completato **sette di tali audit** tra development e production.



Il risultato che conta di più per un potenziale cliente è la coerenza: **in tutti e sette gli audit si sono registrati zero critical findings.** Nelle rare occasioni in cui è emerso un problema di severità più alta, esso è stato corretto rapidamente, spesso nello stesso giorno, e nuovamente verificato. La rubric di scoring è stata deliberatamente resa più rigorosa durante questo periodo (il punteggio massimo possibile è stato aumentato man mano che aggiungevamo più categorie da valutare), motivo per cui la linea del punteggio normalizzato rimane elevata anche se l'asticella si è alzata.

Il nostro audit più recente, del 25 April 2026, illustra come il processo funzioni nella pratica. Sono stati identificati due problemi di severità più alta, entrambi corretti e nuovamente verificati nello stesso giorno, e l'audit si è chiuso con un verdetto di **PASS** senza problemi pronti allo sfruttamento residui nell'attuale threat model.



Audit	Ambiente	Critical	Verdetto
2026-03-28	Development	0	Pronto per la produzione
2026-04-04	Development	0	Pronto per l'enterprise
2026-04-05	Production	0	Pronto per l'enterprise
2026-04-20	Development	0	Pronto per la produzione, note
2026-04-20	Development	0	Superato con note
2026-04-21	Production	0	Sicuro, nessun finding sfruttabile
2026-04-25	Development	0	Superato

Il pattern osservato in questi audit è la prova più onesta che possiamo offrire: i problemi vengono trovati, perché li cerchiamo con impegno, e vengono chiusi rapidamente, perché il processo è costruito per chiuderli. Un fornitore che non riporta mai un finding è di solito un fornitore che non sta cercando.

---

14. Resilienza Operativa e Responsabilità Condivisa

14.1 Monitoraggio e Logging

La telemetria dell'applicazione e della piattaforma confluisce in un workspace centralizzato di log analytics e in un servizio di application monitoring, fornendoci visibilità su disponibilità e comportamento. Le azioni sensibili come cancellazione dei dati, accettazione di accordi legali e invocazioni AI sono registrate in tabelle di audit dedicate, così da avere una registrazione durevole di chi ha fatto cosa ai dati importanti.

14.2 Backup e Recovery

Il database gestito conserva backup automatizzati, e lo storage privato è protetto da retention di soft-delete sia sui blob sia sui container, in modo che una cancellazione accidentale o malevola possa essere recuperata entro la finestra di retention. L'infrastruttura critica dispone di deletion lock per prevenire la rimozione accidentale delle risorse di produzione.

14.3 Sintesi della Responsabilità Condivisa

Area	AI Interview Analyzer	Cliente
Infrastruttura, rete, patching	Sì	-
Sicurezza applicativa e pipeline AI	Sì	-
Crittografia, secrets, residenza dei dati	Sì	-
Amministrazione di utenti e ruoli	Fornisce i controlli	Gestisce utenti e ruoli
Configurazione della retention policy	Fornisce i controlli	Imposta la finestra di retention
Consenso del candidato	Fornisce il workflow	Ne garantisce l'utilizzo
Credenziali forti degli utenti finali e SSO	Supporta SSO e policy	Applica la policy interna

15. Threat Model e Mappatura OWASP

Progettiamo contro un insieme concreto di avversari: un attaccante esterno senza credenziali, un utente autenticato curioso o malevolo di un'organizzazione che tenta di raggiungere i dati di un'altra organizzazione, una dipendenza compromessa e un errore interno. La tabella seguente mappa le categorie di rischio comunemente usate dell'OWASP Top 10 ai controlli specifici che le affrontano in questa piattaforma, ciascuno dei quali è verificato dai test descritti nella Sezione 12.

Rischio OWASP	Come la piattaforma lo mitiga
Broken access control	Controllo degli accessi basato sui ruoli su ogni endpoint privilegiato; scoping per organizzazione; "not found" su accesso cross-org; rimappatura degli identificatori; matrice di test cross-org
Cryptographic failures	TLS 1.2+ in transito; AES-256 at rest; hashing delle password con bcrypt; secrets in un vault gestito
Injection	Query parametrizzate solo tramite ORM; rigorosa validazione dello schema; sanitizzazione HTML in fase di scrittura
Insecure design	Defense in depth stratificata; threat modeling e revisione dell'architettura in ogni audit
Security misconfiguration	Infrastructure as code; gruppi di rete default-deny; header di sicurezza; shared storage keys disabilitate; schema API non esposto in produzione
Vulnerable components	Monitoraggio automatizzato settimanale delle dipendenze; audit CVE delle dipendenze nella revisione periodica
Identification and authentication failures	Token a breve durata; login con rate limiting; verifica email; supporto SSO; nessuna password in chiaro
Software and data integrity failures	Fasi della pipeline pinned e immutabili; installer desktop firmati; verifica della firma dei webhook; deployment di produzione protetti da tag
Security logging and monitoring failures	Telemetria centralizzata; tabelle di audit dedicate per azioni sensibili
Server-side request forgery	Chiamate in uscita limitate a endpoint fidati; probe SSRF nel framework di penetration test

Questa mappatura è la spina dorsale del nostro argomento di assurance: per ogni classe nota di attacco esiste un controllo nominato, e per ogni controllo nominato esiste un test.

16. Gestione delle Vulnerabilità e Responsible Disclosure

La sicurezza non è mai conclusa, quindi eseguiamo un ciclo continuo di scoperta e remediation.

- **Scoperta.** Le vulnerabilità emergono da quattro fonti: la suite di test automatizzati, gli audit ricorrenti di penetration test, il monitoraggio automatizzato delle dipendenze e le segnalazioni di clienti o ricercatori.
- **Triage.** A ogni finding viene assegnata una severità (critical, high, medium, low o informational) con evidenze e un responsabile della remediation, esattamente come registrato nei nostri report di audit.
- **Obiettivi di remediation.** I finding critical e high hanno priorità per una remediation immediata; nella nostra cronologia di audit, i finding di severità più elevata sono stati tipicamente risolti e nuovamente verificati nello stesso giorno. I finding medium e inferiori vengono pianificati nel normale ciclo di manutenzione.
- **Verifica.** Le correzioni vengono ritestate e, ove rilevante, viene eseguito un controllo live contro l'ambiente distribuito per confermare che il problema sia realmente chiuso, non solo chiuso nel codice.
- **Disclosure.** I problemi di sicurezza possono esserci segnalati direttamente. Confermiamo la ricezione delle segnalazioni, indaghiamo e teniamo informato il segnalante fino alla risoluzione.

17. Mappatura di Compliance

17.1 GDPR

Area GDPR	Implementazione della piattaforma
Base giuridica (Art. 6)	Consenso esplicito del candidato acquisito prima del trattamento
Minimizzazione dei dati e limitazione della conservazione (Art. 5)	Vengono trattati solo dati rilevanti per il colloquio; retention configurabile con cancellazione automatica
Diritto alla cancellazione (Art. 17)	Cancellazione come unità singola di tutti i dati del candidato, con prova registrata di cancellazione
Diritti dell'interessato (Art. 15 to 20)	Sono supportati accesso, cancellazione, portabilità e opposizione
Obblighi del responsabile del trattamento (Art. 28)	Data processing agreement accettato alla registrazione e versionato per organizzazione
Sicurezza del trattamento (Art. 32)	Crittografia, controllo degli accessi, isolamento e test continui come descritto in questo documento
Trasparenza sui sub-processor	Divulgati nel data processing agreement con preavviso di modifica

17.2 EU AI Act

La piattaforma è trattata come un sistema AI high-risk che supporta decisioni occupazionali, e manteniamo documentazione allineata al regolamento, inclusi una transparency card, documentazione utente e una dichiarazione di conformità. Le salvaguardie fondamentali, la supervisione umana, la trasparenza, il punteggio basato su evidenze e i rigorosi limiti di ambito su ciò che l'AI valuta, sono descritti nella Sezione 10. Continuiamo a maturare la nostra documentazione formale di conformità man mano che avanza la timeline di implementazione del regolamento.

17.3 Certificazioni dell'Hosting

La piattaforma opera interamente su Microsoft Azure, i cui data center dispongono di certificazioni indipendenti, tra cui ISO 27001 e SOC 2. Tali certificazioni coprono i livelli fisici e di piattaforma sottostanti alla nostra applicazione; i controlli a livello applicativo sono quelli descritti in tutto questo documento.

17.4 Registro dei Sub-processor

Sub-processor	Finalità	Regione
Microsoft Azure	Hosting, elaborazione AI e speech, storage, email transazionali	EU (West Europe, Sweden Central)
Stripe	Gestione di abbonamenti e pagamenti	EU (Ireland)
Fakturownia	Fatturazione	EU (Poland)
ATS connector (optional)	Integrazione applicant-tracking, abilitata solo su richiesta	EU

18. Roadmap della Sicurezza

Trattiamo la sicurezza come un programma di miglioramento continuo. Le iniziative attualmente presenti nella nostra roadmap includono il rafforzamento delle opzioni di autenticazione multi-factor per gli account amministrativi, l'espansione dell'audit logging centralizzato degli accessi ai dati, il continuo irrigidimento dell'aggiornamento delle dipendenze con una cadenza regolare e il progresso verso la certificazione formale di terze parti dei controlli descritti in questo documento. Nessuno di questi aspetti rappresenta oggi una lacuna che espone i dati dei clienti; ciascuno è un miglioramento di una postura già stratificata.

19. Sintesi

AI Interview Analyzer protegge i dati dei candidati e dei clienti tramite un'architettura stratificata: una rete privata per impostazione predefinita senza servizi dati pubblici, identità forti e isolamento per organizzazione, codice applicativo che elimina intere classi di vulnerabilità, crittografia e residenza dei dati nell'UE, e controlli di privacy incorporati nel modello dei dati. Ciò che distingue la piattaforma è l'evidenza a supporto di queste affermazioni. Con 3,171 test automatizzati, una metodologia ripetibile di live penetration testing, un programma dedicato di sicurezza AI e una cronologia di sette audit di sicurezza interni con zero critical findings, possiamo mostrare, non solo dichiarare, che la piattaforma è sicura.

Appendix A: Catalogo dei Controlli di Sicurezza

Un riferimento sintetico dei controlli principali e delle evidenze che supportano ciascuno di essi.

Controllo	Meccanismo	Evidenza
Crittografia del trasporto	Solo HTTPS, TLS 1.2+, HTTP reindirizzato	Infrastructure as code; audit dell'architettura
Crittografia at rest	Crittografia di piattaforma AES-256 su storage e database	Configurazione della piattaforma; audit dell'architettura
Protezione delle password	bcrypt con salt per password	Source control; test di autenticazione
Gestione delle sessioni	Token firmati di 30 minuti, refresh lato server revocabile	Source control; test di autenticazione
Autorizzazione	Controllo degli accessi a quattro ruoli sugli endpoint privilegiati	Suite di test di enforcement dei ruoli
Isolamento dei tenant	Scoping delle query per organizzazione; 404 su cross-org	Matrice di test cross-organization
Sicurezza delle API key	Storage come hash, permessi scoped, limiti di frequenza per chiave	Suite di test delle API key
Difesa dalle injection	Query parametrizzate solo tramite ORM	Analisi statica; test di injection
Difesa dal cross-site scripting	Sanitizzazione HTML in fase di scrittura	Suite di test di sanitizzazione HTML
Rate limiting	Limiter durevole supportato dal database sugli endpoint auth	Test di rate limit; controlli live di burst
Integrità dei webhook	Verifica della firma del provider sul body grezzo	Suite di test dei webhook
Gestione dei secrets	Vault gestito, purge protection, managed identity	Infrastructure as code; audit dell'architettura
Isolamento di rete	Endpoint privati; segmentazione default-deny	Infrastructure as code; audit dell'architettura
Cancellazione dei dati	Cancellazione a cascata come unità singola con audit log	Suite di test di cancellazione GDPR
Supply chain	Fasi della pipeline pinned; monitoraggio settimanale delle dipendenze	Configurazione della pipeline; audit delle dipendenze

Appendix B: Domande Frequenti per i Revisori della Sicurezza

Dove sono archiviati i nostri dati? Interamente all'interno dell'Unione Europea, su Microsoft Azure, in West Europe con elaborazione AI in regioni UE. I dati dei candidati non lasciano mai l'UE.

I nostri dati vengono usati per addestrare modelli AI? No. Il provider AI non utilizza i dati dei clienti per l'addestramento.

Il database è raggiungibile da Internet? No. L'accesso alla rete pubblica è disabilitato e il database è raggiungibile solo tramite un endpoint privato all'interno della virtual network.

Un cliente può vedere i dati di un altro cliente? No. Ogni query è limitata all'organizzazione del chiamante, l'accesso cross-organization restituisce "not found" e una matrice automatizzata verifica continuamente questo isolamento.

Come vengono archiviate le password? Sottoposte ad hashing con bcrypt e un salt univoco per password. È supportato il single sign-on con Microsoft e Google, nel qual caso non viene archiviata alcuna password.

Supportate il single sign-on? Sì, tramite Microsoft e Google OAuth.

Per quanto tempo sono validi gli access token? Trenta minuti, abbinati a una sessione di refresh lato server revocabile che viene invalidata al logout.

Come viene gestito il consenso del candidato? Ogni candidato riceve un link di consenso univoco e monouso e deve accettare prima di qualsiasi registrazione o analisi. Il consenso viene registrato rispetto allo specifico processo di assunzione.

Come vengono cancellati i dati? Come unità singola comprendente il record del candidato, i colloqui, le trascrizioni, l'audio, i documenti e i confronti, secondo una retention schedule configurabile, con una prova registrata di cancellazione. I candidati possono anche richiedere direttamente la cancellazione.

Avete un data processing agreement? Sì, accettato alla registrazione e versionato per organizzazione, incluso il registro dei sub-processor.

L'AI prende decisioni di assunzione? No. Fornisce solo supporto decisionale; un essere umano esamina ogni output e prende tutte le decisioni.

Come dimostrate le vostre affermazioni sulla sicurezza? Tramite 3,171 test automatizzati inclusa una suite di sicurezza dedicata, una metodologia ripetibile di penetration testing in sei fasi eseguita contro ambienti live, un programma di test di sicurezza AI e report di audit scritti ricorrenti.

Cosa succede quando trovate una vulnerabilità? Le viene assegnata una severità con evidenze e un responsabile, viene corretta secondo una schedule prioritaria, nuovamente verificata includendo controlli live ove rilevanti e registrata in un report di audit.

Possiamo eseguire il nostro penetration test? Le valutazioni di sicurezza possono essere organizzate tramite il vostro account representative con ambito e pianificazione appropriati.

Appendix C: Glossario

Termine	Significato
AES-256	Un solido standard di crittografia simmetrica usato per proteggere i dati at rest
bcrypt	Una funzione di hashing delle password progettata appositamente con salting per password
Managed identity	Un'identità emessa dalla piattaforma che consente a un servizio di autenticarsi senza chiavi archiviate
Private endpoint	Un indirizzo di rete privato che mantiene un servizio cloud fuori da Internet pubblico
Network security group	Un insieme di regole allow e deny che filtrano il traffico di rete verso una subnet
RBAC	Controllo degli accessi basato sui ruoli, che concede permessi in base al ruolo dell'utente
IDOR	Insecure direct object reference, una falla di controllo degli accessi da cui la piattaforma si difende
SSRF	Server-side request forgery, una classe di attacco verificata nei nostri penetration test
Web application firewall	Un controllo edge che filtra il traffico web malevolo
Data processing agreement	Il contratto che disciplina come un responsabile del trattamento gestisce dati personali per conto di un titolare

Appendix D: Contatto e Controllo del Documento

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Per una security review, una copia del nostro data processing agreement o la nostra documentazione di conformità al EU AI Act, contattare il proprio account representative.

Questo documento descrive la postura di sicurezza del servizio AI Interview Analyzer alla data di generazione indicata nel piè di pagina. È fornito a fini di valutazione e non costituisce parte di alcun contratto. Gli specifici impegni contrattuali di sicurezza sono stabiliti nell'accordo applicabile e nel data processing agreement.