Security Whitepaper

Enterprise Security Overview - AI Interview Analyzer

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

Contents

1. Zusammenfassung
2. Dokumentumfang und Ansatz
3. Überblick über die Sicherheitsarchitektur
4. Defense in Depth
5. Netzwerksicherheit
6. Identitäts- und Zugriffsmanagement
7. Anwendungssicherheit
8. Datenschutz
9. Privacy by Design und GDPR
10. Responsible AI und der EU AI Act
11. Sicherer Entwicklungslebenszyklus
12. Kontinuierliche Sicherheitstests
13. Ergebnisse der Sicherheitsaudits
14. Operative Resilienz und geteilte Verantwortung
15. Bedrohungsmodell und OWASP-Mapping
16. Schwachstellenmanagement und Responsible Disclosure
17. Compliance-Mapping
18. Sicherheits-Roadmap
19. Zusammenfassung
Appendix A: Katalog der Sicherheitskontrollen
Appendix B: Häufig gestellte Fragen für Security Reviewer
Appendix C: Glossar
Appendix D: Kontakt und Dokumentenkontrolle

Security Whitepaper

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

Zielgruppe: Enterprise-Sicherheits-, IT- und Beschaffungsteams

Klassifizierung: Öffentlich

1. Zusammenfassung

AI Interview Analyzer ist eine Enterprise-Recruiting-Plattform, die Interviews mit ausdrücklicher Einwilligung der Kandidaten aufzeichnet, transkribiert und strukturiert sowie evidenzbasierte Bewertungsunterstützung für Recruiter bereitstellt. Da die Plattform personenbezogene Daten von Kandidaten verarbeitet und Einstellungsprozesse unterstützt, werden Sicherheit und Datenschutz als primäre Designvorgaben behandelt, nicht als später hinzugefügte Funktionen.

Dieses Whitepaper beschreibt in konkreten und überprüfbaren Begriffen, wie wir Kunden- und Kandidatendaten schützen. Es richtet sich an Personen, die Anbieter prüfen: Sicherheitsingenieure, IT-Administratoren, Datenschutzbeauftragte und Beschaffungsteams. Jede Zahl in diesem Dokument stammt direkt aus unseren eigenen Engineering-Systemen und nicht aus Marketingmaterial.

Die zentrale Botschaft ist einfach: **Wir behaupten nicht nur, dass die Plattform sicher ist, wir testen fortlaufend, dass sie es ist.** Unsere Codebasis enthält **3,171 automatisierte Tests**, darunter eine dedizierte Sicherheitssuite, die Authentifizierung, Autorisierung, organisationsübergreifende Isolation, Schutz vor Injection-Angriffen und Datenlöschung prüft. Darüber hinaus führen wir ein wiederholbares Penetration-Testing-Harness gegen Live-Bereitstellungen aus und erstellen schriftliche Auditberichte. In sieben internen Sicherheitsaudits im März und April 2026 verzeichneten wir **zero critical findings**, wobei unser jüngstes Audit mit dem Urteil **PASS** abgeschlossen wurde. (Die formale Drittzertifizierung dieser Kontrollen befindet sich auf unserer Roadmap; siehe Abschnitt 18.)

Sicherheitsmerkmal	Zusammenfassung
Hosting	Microsoft Azure, nur EU-Regionen
Netzwerkmodell	Private Endpoints, Netzwerksegmentierung mit Default-Deny, keine öffentliche Datenbank
Verschlüsselung	AES-256 im Ruhezustand, TLS 1.2 oder höher bei der Übertragung
Identität	Kurzlebige signierte Tokens, bcrypt-Passwort-Hashing, SSO-Unterstützung
Zugriffskontrolle	Rollenbasierte Zugriffskontrolle mit strikter organisationsbezogener Isolation
Secrets	Zentralisierter Secrets Vault mit Zugriff über Managed Identity
Datenschutz	Ausdrückliche Einwilligung, konfigurierbare Aufbewahrung, Löschung als einzelne Einheit
Responsible AI	Nur Entscheidungsunterstützung, Mensch immer in der Schleife
Nachweis	3,171 automatisierte Tests plus wiederkehrende Penetrationstests und Audits

1.1 Wie dieses Dokument zu lesen ist

Die Abschnitte 3 bis 11 beschreiben die Kontrollen zum Schutz von Daten: Architektur, Netzwerk, Identität, Anwendung, Datenschutz, Privatsphäre und den sicheren Entwicklungslebenszyklus. Die Abschnitte 12 und 13 behandeln unser charakteristisches Programm des kontinuierlichen Testens sowie unsere Audit-Historie. Die Abschnitte 14 bis 17 behandeln Betrieb, Bedrohungsmodellierung, Schwachstellenmanagement und Compliance-Mapping. Die Anhänge enthalten einen Kontrollkatalog, ein FAQ für Reviewer und ein Glossar, das ein Sicherheitsteam direkt während einer Bewertung verwenden

kann.

2. Dokumentumfang und Ansatz

2.1 Was dieses Dokument abdeckt

Dieses Whitepaper behandelt die Sicherheitsarchitektur und -praktiken des AI Interview Analyzer-Services: die Hosting-Umgebung, das Netzwerkdesign, das Identitäts- und Zugriffsmanagement, Kontrollen auf Anwendungsebene, Datenschutz, Datenschutz- und regulatorische Ausrichtung, den sicheren Entwicklungslebenszyklus sowie unser Programm für kontinuierliche Sicherheitstests.

2.2 Was es überprüfbar macht

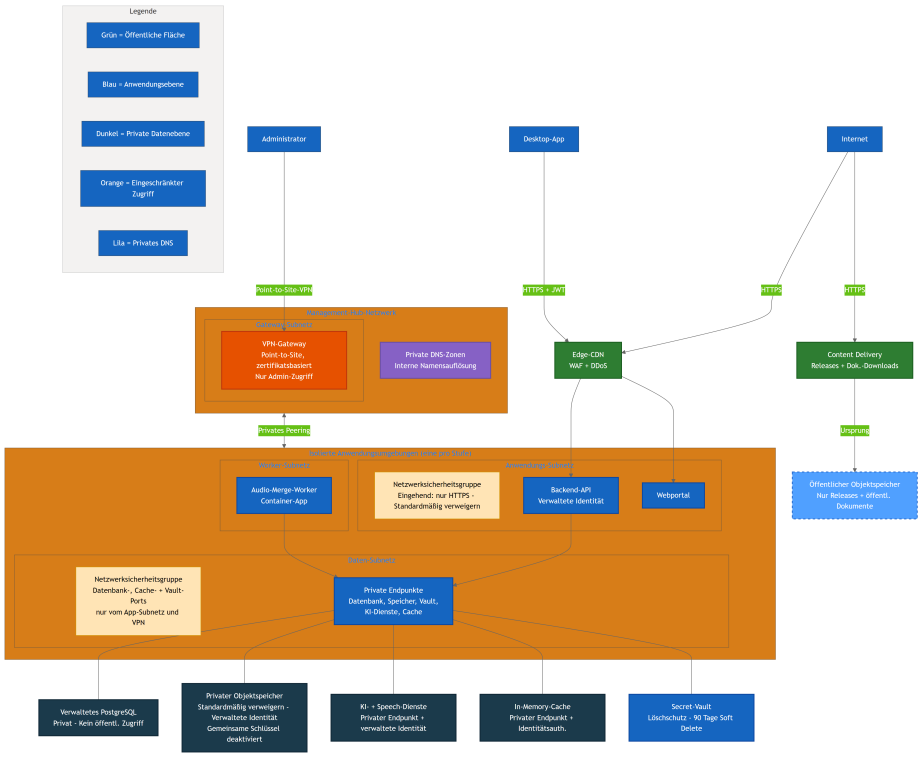
Sicherheitsaussagen von Anbietern sind leicht zu schreiben und schwer zu vertrauen. Deshalb haben wir jede wesentliche Aussage in diesem Dokument mit etwas Konkretem und Zählbarem in unseren Engineering-Systemen verknüpft: einer in Code implementierten Kontrolle, einem Test, der nachweist, dass die Kontrolle funktioniert, einer Infrastrukturdefinition, die sie erzwingt, oder einem Auditbericht, der eine dokumentierte Prüfung festhält. Wo eine Kontrolle Teil unserer zukünftigen Roadmap ist und heute noch nicht produktiv bereitgestellt wurde, sagen wir das ausdrücklich. Wir behaupten lieber zu wenig und werden dafür als vertrauenswürdig wahrgenommen, als zu viel zu behaupten und dabei ertappt zu werden.

2.3 Geteilte Verantwortung

Die Plattform wird als Software-as-a-Service bereitgestellt. Wir betreiben die Infrastruktur, die Anwendung, die AI-Pipeline und die Datenverarbeitung. Der Kunde ist dafür verantwortlich, seine eigenen Benutzerkonten und Rollen zu verwalten, Datenaufbewahrungsfristen entsprechend seiner internen Richtlinie zu konfigurieren und sicherzustellen, dass die Einwilligung des Kandidaten über den von der Plattform bereitgestellten Einwilligungsworkflow eingeholt wird. Abschnitt 14 beschreibt diese Aufteilung ausführlicher.

3. Überblick über die Sicherheitsarchitektur

Die Plattform ist als kleine Anzahl zusammenarbeitender Services aufgebaut und nicht als einzelner Monolith. Eine Desktop-Anwendung und ein Webportal fungieren als Clients. Eine zentrale Backend-API verwaltet sämtliche Persistenz, Authentifizierung, Abrechnung, die AI-Pipeline, Einwilligungen, E-Mail, Dateiverarbeitung und Dashboards. Ein Audio-Merge-Worker verarbeitet Aufzeichnungen asynchron. Alle sensiblen Zustände befinden sich hinter der Backend-API; Clients sprechen niemals direkt mit der Datenbank, dem Storage oder den AI-Services.



Das obige Diagramm zeigt die Produktionstopologie mit bewusst verallgemeinerten Ressourcennamen. Drei Prinzipien sind darin erkennbar:

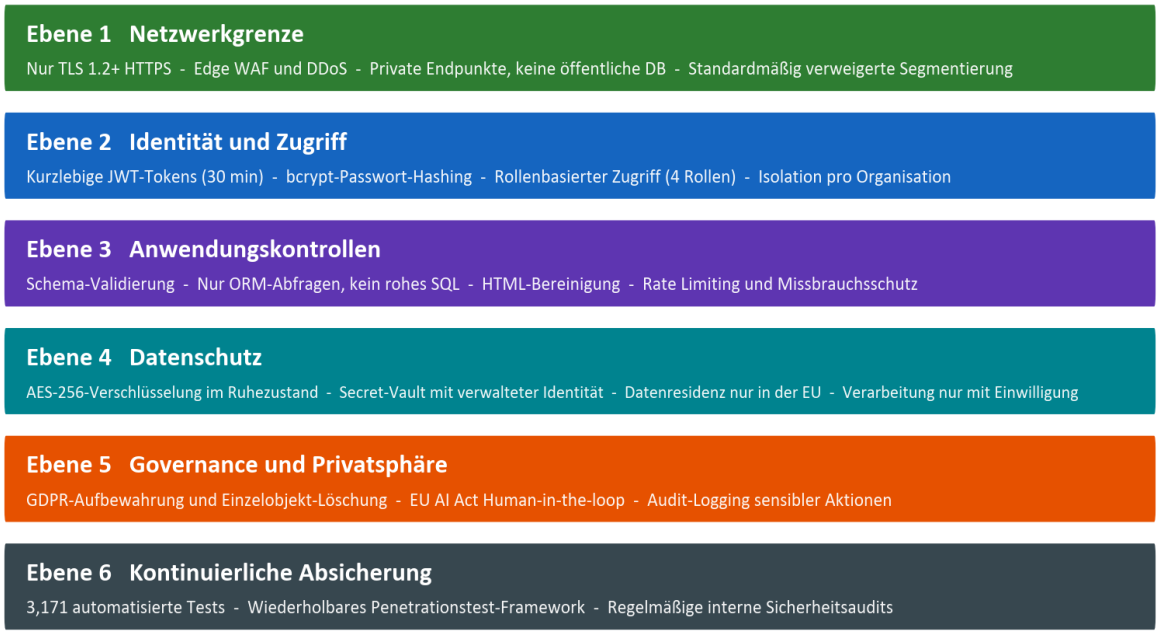
- **Keine direkte Exponierung von Datendiensten.** Die Datenbank, privater Objektspeicher, AI-Services und Cache haben den öffentlichen Netzwerkzugriff deaktiviert und sind nur über Private Endpoints innerhalb eines isolierten virtuellen Netzwerks erreichbar. Der Secrets Vault wird von der Anwendung über einen Private Endpoint erreicht und zusätzlich durch Plattform-Identitätsauthentifizierung sowie Least-Privilege-Zugriffsrichtlinien geschützt, sodass jeder Zugriff unabhängig vom Netzwerkpfad eine gültige, autorisierte Identität erfordert.
- **Eine getrennte öffentliche Oberfläche.** Der einzige öffentliche Objektspeicher enthält Release-Downloads und öffentliche Dokumente. Er enthält niemals Kandidatendaten. Der kundenseitige Anwendungsverkehr läuft über eine Edge-Schicht, die Web application firewall, Schutz vor Distributed-Denial-of-Service und Content Delivery bereitstellt.
- **Administrativer Zugriff ist abgesichert.** Betreiber erreichen interne Ressourcen nur über ein zertifikatbasiertes Point-to-Site VPN in ein Management-Hub-Netzwerk, nicht über das öffentliche Internet.

Jede Bereitstellungsstufe (Entwicklung und Produktion) ist eine vollständig isolierte Umgebung mit eigenem Netzwerk, eigenen Storage-Accounts, eigener Datenbank und eigenen Secrets. Produktionsdaten von Kunden sind niemals in niedrigeren Umgebungen vorhanden. Ein gemeinsamer Management-Hub enthält nur das VPN-Gateway und private DNS und ist privat mit jeder Umgebung verbunden.

4. Defense in Depth

Es wird keiner einzelnen Kontrolle vertraut, jeden Angriff zu stoppen. Die Plattform schichtet unabhängige Kontrollen, sodass das Versagen einer einzelnen Schicht keine Daten offenlegt. Die nachstehenden Schichten sind jeweils implementiert und werden, wie in Abschnitt 12 beschrieben, einzeln getestet.

Mehrschichtiges Sicherheitsmodell: unabhängige Kontrollen auf jeder Ebene



Schicht	Repräsentative Kontrollen
Network Edge	Nur-TLS-Transport, Edge-WAF und DDoS-Schutz, Private Endpoints, Default-Deny-Segmentierung
Identität und Zugriff	Kurzlebige signierte Tokens, bcrypt-Hashing, rollenbasierte Zugriffskontrolle, organisationsbezogene Isolation
Anwendung	Schemavalidierung für alle Eingaben, ausschließlich ORM-basierter Datenzugriff, Output-Encoding, Rate Limiting
Datenschutz	Verschlüsselung im Ruhezustand, Secrets Vault mit Managed Identity, EU-Datenresidenz, einwilligungsbasierte Verarbeitung
Governance und Privatsphäre	Konfigurierbare Aufbewahrung, Löschung als einzelne Einheit, Human-in-the-loop-AI, Audit Logging
Kontinuierlicher Nachweis	Automatisierte Test-Suite, wiederholbare Penetrationstests, wiederkehrende interne Sicherheitsaudits

Der Rest dieses Dokuments erläutert jede Schicht der Reihe nach und beschreibt anschließend, wie wir fortlaufend nachweisen, dass diese Schichten standhalten.

5. Netzwerksicherheit

5.1 Standardmäßig privat

Die Datenschicht ist konstruktionsbedingt privat. Die verwaltete PostgreSQL-Datenbank hat den öffentlichen Netzwerkzugriff deaktiviert und ist nur über einen Private Endpoint erreichbar. Der private Objektspeicher ist so konfiguriert, dass Netzwerkzugriff standardmäßig verweigert wird, deaktiviert Shared Access Keys vollständig und ist nur über Managed Identity aus dem Application-Subnet erreichbar. Der Cache, AI-Services und der Secrets Vault werden ebenso über Private Endpoints mit privater DNS-Auflösung erreicht.

In der Praxis bedeutet dies, dass es keine internetseitige Connection String zur Datenbank und keine öffentliche Storage-URL für Kandidatenaudio gibt: Die Datenbank und der private Storage haben den öffentlichen Netzwerkzugriff vollständig deaktiviert. Der Secrets Vault wird von der Anwendung über einen Private Endpoint erreicht und ist durch Plattform-Identitätsauthentifizierung sowie Least-Privilege-Zugriffsrichtlinien geschützt; Anwendungsidentitäten erhalten schreibgeschützten Zugriff nur auf die Secrets, die sie benötigen, sodass Secrets ohne gültige, autorisierte Identität nicht abgerufen werden können. Die Angriffsfläche, die ein externer Angreifer überhaupt berühren kann, ist auf die HTTPS-Endpunkte der Anwendung hinter der Edge-Schicht beschränkt.

5.2 Netzwerksegmentierung

Jede Umgebung ist in separate Subnets für die Anwendungsschicht, die Datenschicht und den asynchronen Worker unterteilt. Jedes Subnet wird durch eine Network Security Group gesteuert, deren letzte Regel sämtlichen eingehenden Verkehr verweigert. Das Application-Subnet akzeptiert nur eingehendes HTTPS. Das Data-Subnet akzeptiert nur die spezifischen Ports für Datenbank, Cache und Vault und nur aus dem Application-Subnet oder dem administrativen VPN. Das bedeutet, dass selbst ein Angreifer, der somehow die Anwendungsschicht erreicht hätte, nicht frei zur Datenschicht pivotieren kann; die einzigen zulässigen Pfade sind diejenigen, die die Anwendung legitim nutzt.

5.3 Die Edge

Der öffentliche Anwendungsverkehr wird durch eine Edge-Schicht geführt, die eine Web application firewall, DDoS-Schutz und ein Content Delivery Network bereitstellt. Release- und Dokument-Downloads werden aus einem dedizierten öffentlichen Storage-Account über eine Content-Delivery-Front-Door bereitgestellt, vollständig getrennt vom privaten Storage, der Kandidatendaten enthält. Die beiden Storage-Ebenen werden niemals vermischt: Eine Fehlkonfiguration auf der öffentlichen Ebene kann keine privaten Kandidatendaten offenlegen, da es sich um unterschiedliche Accounts mit unterschiedlichen Netzwerkregeln handelt.

5.4 Administrativer Zugriff

Es gibt keinen öffentlichen administrativen Endpunkt in das private Netzwerk. Betreiber verbinden sich über ein Point-to-Site VPN-Gateway mit zertifikatbasierter Authentifizierung. Administrativer Zugriff auf Datenbank und Cache ist nur innerhalb dieses Tunnels möglich, da diese Services den öffentlichen Netzwerkzugriff deaktiviert haben. Dadurch bleiben tägliche Betriebsaktivitäten vollständig außerhalb des öffentlichen Internets.

6. Identitäts- und Zugriffsmanagement

6.1 Authentifizierung

Benutzersitzungen werden mit einem signierten Access Token etabliert, der dreißig Minuten gültig ist, gekoppelt mit einem separaten, opaken, serverseitigen Refresh Token. Access Tokens werden bei jeder Anfrage verifiziert, und der Benutzer wird gegenüber der Datenbank erneut validiert (einschließlich einer Prüfung auf aktives Konto), anstatt sich allein auf den Inhalt des Tokens zu verlassen. Beim Abmelden wird die serverseitige Refresh-Session sofort widerrufen, sodass ein gestohlenes Refresh Token eine Abmeldung nicht überdauern kann.

Passwörter werden niemals im Klartext gespeichert. Sie werden mit bcrypt unter Verwendung eines eindeutigen Salt pro Passwort gehasht. Für Organisationen, die Single Sign-On bevorzugen, unterstützt die Plattform OAuth-Login mit Microsoft und Google; in diesem Fall wird überhaupt kein Passwort gespeichert.

Die Inhaberschaft einer E-Mail-Adresse wird über einen einmalig verwendbaren, zeitlich begrenzten Verifizierungslink bestätigt, bevor ein selbst registriertes Konto als verifiziert behandelt wird, und das erneute Versenden von Verifizierungs-E-Mails ist rate-limitiert, um Missbrauch zu verhindern.

6.2 Rollenbasierte Zugriffskontrolle

Die Autorisierung wird über ein Rollenmodell mit vier Rollen zunehmender Berechtigung erzwungen: Interviewer, Hiring Manager, Recruiter und Administrator. Der Zugriff auf privilegierte Operationen wird durch serverseitige Abhängigkeiten erzwungen, die sowohl die Rolle als auch den Verifizierungsstatus des Aufrufers prüfen. Diese Rollenprüfungen schützen weit über einhundert unterschiedliche API-Operationen.

Rolle	Typische Fähigkeiten
Interviewer	Führt zugewiesene Interviews durch; sieht nur ihm zugewiesene Interviews
Hiring Manager	Verwaltet Recruitments, die ihm gehören oder bei denen er Mitglied ist
Recruiter	Vollständiges Recruitment- und Kandidatenmanagement innerhalb der Organisation
Administrator	Organisationseinstellungen, Abrechnung, Benutzer- und API-Key-Administration

Über grobe Rollenprüfungen hinaus wendet die Plattform Sichtbarkeitsregeln auf Datenebene an. Hiring Manager sehen nur die Recruitments, die sie erstellt haben oder bei denen sie Mitglied sind; Interviewer sehen nur die ihnen zugewiesenen Interviews. Berechtigungen werden daher sowohl auf der Ebene „welche Aktion“ als auch auf der Ebene „welche Datensätze“ erzwungen.

6.3 Organisationsbezogene Isolation

Die Plattform ist Multi-Tenant, und Tenant-Isolation wird als erstklassige Sicherheitskontrolle behandelt. Jede authentifizierte Identität trägt einen Organisationsbezeichner, und Datenabfragen werden auf diese Organisation begrenzt. Fordert ein Benutzer einen Datensatz an, der zu einer anderen Organisation gehört, liefert die Plattform eine „not found“-Antwort zurück, anstatt offenzulegen, dass der Datensatz existiert. Interne Datenbankkennungen werden niemals über die Schnittstelle offengelegt; die API präsentiert Anzeige-IDs und ordnet sie pro Anfrage neu zu, wodurch eine häufige Klasse organisationsübergreifender Enumerationsangriffe entfernt wird.

Dies ist nicht nur eine Designabsicht. Wie in Abschnitt 12 beschrieben, führt unsere automatisierte Suite eine große organisationsübergreifende Matrix aus, die versucht, auf die Daten einer Organisation mit den Zugangsdaten einer anderen Organisation zuzugreifen, und bestätigt, dass jeder solcher Versuch fehlschlägt.

6.4 Programmatischer Zugriff

Für Integrationen können Organisationen in geeigneten Tarifen API Keys ausstellen. Keys verwenden ein erkennbares Präfix, tragen 128 Bits Entropie und werden nur als Hash gespeichert; der Roh-Key wird bei der Erstellung einmal angezeigt und danach nie wieder. Jeder Key trägt einen expliziten Berechtigungsumfang (read, write oder ATS integration), kann auf bestimmte Quellnetzwerke beschränkt werden, kann sofort widerrufen werden und unterliegt pro Key Rate Limits, die aus dem Tarif der Organisation abgeleitet werden. Die Key-Verifizierung verwendet einen timing-sicheren Vergleich, um zu vermeiden, dass Informationen über Antwortzeiten preisgegeben werden.

7. Anwendungssicherheit

Die Anwendung ist so geschrieben, dass ganze Kategorien von Schwachstellen beseitigt werden, anstatt sie von Fall zu Fall zu patchen.

- **Injection.** Der gesamte Datenbankzugriff erfolgt über einen objektrelationalen Mapper mit parameterisierten Abfragen. Die Codebasis enthält kein roh stringformatiertes SQL. Dadurch wird SQL injection strukturell eliminiert.
- **Eingabevalidierung.** Jeder Request-Body wird gegen ein striktes Schema validiert, bevor er die Geschäftslogik erreicht. Zu große Payloads werden abgelehnt, und List-Endpunkte sind paginiert, um den Ressourcenverbrauch zu begrenzen.
- **Output-Encoding und Cross-Site Scripting.** Vom Benutzer bereitgestellter und AI-generierter Text wird als nicht vertrauenswürdig behandelt. Wenn Inhalte als HTML gerendert werden müssen, werden sie beim Schreiben durch einen Allow-List-Sanitizer geleitet, und eine dedizierte Test-Suite bestätigt, dass Script-Tags, Event-Handler und javascript-URLs entfernt werden.
- **Mass Assignment.** Update-Operationen verwenden explizite Schemata, die privilegierte Felder wie Rolle, Organisation und Credit-Saldo ausschließen, sodass ein Client seine Berechtigung nicht durch das Senden zusätzlicher Felder erhöhen kann.
- **Rate Limiting.** Authentifizierungs- und missbrauchsanfällige Endpunkte werden mittels eines langlebigen, datenbankgestützten Limiters rate-limitiert, der Neustarts überlebt und korrekt über mehrere Anwendungsinstanzen hinweg funktioniert. Login, Registrierung, Passwort-Reset und erneutes Versenden von Verifizierungen haben jeweils eigene Limits. Die Auflösung von Client-IP-Adressen ist gegen Spoofing von Forwarding-Headern gehärtet.
- **Webhooks.** Eingehende Webhooks von Zahlungs- und E-Mail-Anbietern werden anhand von Anbietersignaturen auf dem rohen Request-Body verifiziert, bevor sie verarbeitet werden.
- **Datei-Uploads.** Uploads sind größenbegrenzt, werden validiert, unter generierten Bezeichnern statt unter benutzerdefinierten Namen gespeichert und pro Anfrage sowie pro Organisation beschränkt.
- **Security Headers.** In Produktion tragen Antworten Strict-Transport-Security-, Content-Type- und Frame-Options-, eine Referrer Policy und eine restriktive Permissions Policy und unterdrücken Server- und Framework-Banner.

8. Datenschutz

8.1 Verschlüsselung

Alle Daten werden im Ruhezustand mit AES-256 über die Verschlüsselungsschichten für Storage und Datenbank der Azure-Plattform verschlüsselt. Sämtlicher Netzwerkverkehr wird ausschließlich über HTTPS unter Verwendung von TLS 1.2 oder höher bereitgestellt; unverschlüsseltes HTTP wird auf jeder Ebene zu HTTPS umgeleitet. In Produktion geben API und Webportal Strict-Transport-Security-Header zusammen mit einer Reihe von Härtungs-Headern aus und unterdrücken Versionsbanner von Server und Framework.

8.2 Secrets Management

Application-Secrets werden in einem zentralisierten Secrets Vault mit aktivierter Purge Protection und einem Soft-Delete-Fenster von neunzig Tagen gespeichert. Anwendungen authentifizieren sich gegenüber Azure-Ressourcen mittels systemzugewiesener Managed Identities anstatt langlebiger Keys; beispielsweise hat privater Storage Shared Access Keys vollständig deaktiviert, sodass Zugriff nur über identitätsbasierte Rollenzuweisungen möglich ist, die auf die einzelne Ressource beschränkt sind. Vault-Zugriffsrichtlinien gewähren Anwendungsprinzipalen schreibgeschützten Zugriff nur auf die spezifischen Secrets, die sie benötigen, gemäß dem Least-Privilege-Prinzip.

8.3 Datenresidenz

Alle Kunden- und Kandidatendaten werden innerhalb der Europäischen Union gespeichert und verarbeitet. Anwendungshosting, Datenbank, Storage, Cache und Secrets befinden sich in West Europe, und die AI-Verarbeitung läuft in EU-Regionen. Der AI-Anbieter verwendet Kundendaten nicht zum Training seiner Modelle.

8.4 Der Lebensweg eines einzelnen Interviews

Der klarste Weg, die Datenschutzkontrollen zu verstehen, besteht darin, ein einzelnes Interview von Anfang bis Ende nachzuverfolgen. Die Einwilligung wird erfasst und protokolliert, bevor irgendetwas verarbeitet wird. Der Upload wird bei der Übertragung verschlüsselt. Transkription und Analyse laufen innerhalb von EU-Rechenzentren. Ergebnisse werden in verschlüsseltem Storage gespeichert. Jeder Datensatz unterliegt anschließend einer einzelnen Aufbewahrungsuhr, die mit einer protokollierten, kaskadierenden Löschung endet. Zu jedem Zeitpunkt können Kandidatenrechte wie Widerruf, Löschung, Auskunft oder Datenübertragbarkeit diesen Ablauf unterbrechen.

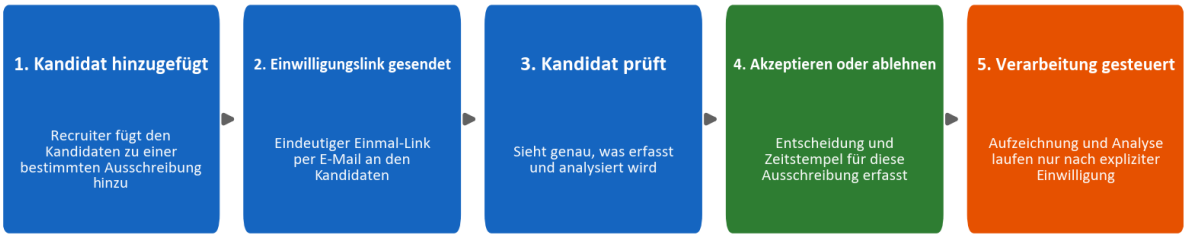
9. Privacy by Design und GDPR

Datenschutz ist in das Datenmodell und den Workflow eingebaut und nicht nur über Richtlinien nachträglich ergänzt.

9.1 Einwilligung

Kein Interview wird ohne ausdrückliche Einwilligung des Kandidaten aufgezeichnet oder analysiert. Wenn ein Kandidat zu einem Recruitment hinzugefügt wird, versendet die Plattform per E-Mail einen eindeutigen, einmal verwendbaren Einwilligungslink. Der Kandidat prüft, was geschehen wird, und akzeptiert oder lehnt ab. Der Einwilligungsstatus, einschließlich des Zeitpunkts der Antwort, wird für dieses konkrete Recruitment protokolliert, sodass eine Einwilligung stets auf einen konkreten Einstellungsprozess bezogen ist und nicht global erteilt wird.

Kandidaten-Einwilligung: explizit und vor jeder Verarbeitung erfasst

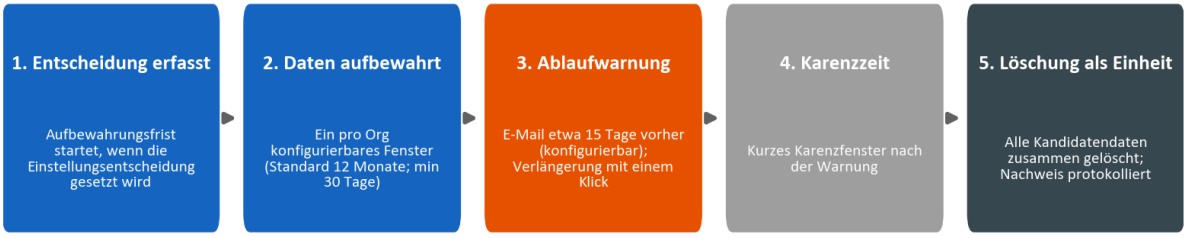


9.2 Aufbewahrung und Löschung

Die Datenaufbewahrung ist pro Organisation konfigurierbar, mit einem Standardwert von zwölf Monaten und einem konfigurierbaren Minimum von dreißig Tagen, und kann pro Kandidat überschrieben werden. Es gibt eine einzige Aufbewahrungsuhr für die Daten eines Kandidaten, keinen separaten Timer pro Artefakt. Die Uhr startet, wenn eine Einstellungsentscheidung protokolliert wird. Bevor Daten ablaufen, sendet die Plattform eine Warnung (standardmäßig etwa fünfzehn Tage im Voraus) und bietet eine Verlängerung mit einem Klick an. Wenn Daten gelöscht werden, werden sie als einzelne Einheit gelöscht: der Kandidatendatensatz, Interviews, Transkripte, Audioaufzeichnungen, Dokumente und Vergleiche werden alle gemeinsam entfernt, und die Löschung wird in einem Audit-Log protokolliert. Es bleibt kein teilweiser oder verwaister Restbestand zurück.

Der folgende Lebenszyklus zeigt diese einzelne Uhr und wie sie in einer einzigen kaskadierenden Löschung mit protokolliertem Löschungsnachweis zusammenläuft.

Datenaufbewahrung: eine Frist pro Kandidat, Löschung als Einheit



9.3 Rechte betroffener Personen und Sub-Processors

Die Plattform unterstützt die unter der GDPR erforderlichen Rechte betroffener Personen, einschließlich Auskunft, Löschung, Übertragbarkeit, Widerspruch und Erläuterung. Die Verarbeitung erfolgt unter einem Data Processing Agreement, dem Kunden bei der Registrierung zustimmen und das pro Organisation versioniert wird. Unsere Sub-Processors und ihre Rollen, sämtlich innerhalb der EU oder unter geeigneten Schutzmaßnahmen, sind in dieser Vereinbarung offengelegt, und Kunden erhalten im Voraus eine Benachrichtigung über jede Änderung. Abschnitt 17 enthält das Sub-Processor-Register und das artikelweise Compliance-Mapping.

10. Responsible AI und der EU AI Act

Die Plattform fällt in die Hochrisikokategorie des EU AI Act, weil sie Beschäftigungsentscheidungen unterstützt, und wir nehmen diese Einstufung ernst.

Die definierende Regel des Produkts ist, dass **die AI Entscheidungsunterstützung ist, nicht Entscheidungsträger.** Das System akzeptiert oder lehnt einen Kandidaten niemals automatisch ab. Es transkribiert Sprache, strukturiert Fragen und Antworten, bewertet Antworten anhand von Kriterien, die der Recruiter definiert hat, und erstellt Entwürfe für Feedback; ein Mensch überprüft jede Ausgabe, bevor sie verwendet wird. Dadurch bleibt ein Mensch fest in der Schleife.

Ebenso wichtig ist, was die AI nicht tut. Sie bewertet weder Persönlichkeit, „cultural fit“, emotionalen Zustand, Tonfall, Akzent, Geschlecht, Alter, ethnische Zugehörigkeit, Erscheinungsbild noch Körpersprache. Die Bewertung ist an Evidenz aus dem Transkript und an vom Recruiter definierte Kriterien gebunden, und Kandidatennamen werden von den Eingaben für die Bewertung ausgeschlossen, um Bias zu reduzieren. Wir veröffentlichen eine Transparency Card, Benutzerdokumentation und eine Declaration of Conformity, die das System, seine Grenzen und seine Schutzmaßnahmen beschreibt.

Responsible-AI-Kontrolle	Funktionsweise
Human in the loop	Jeder Score und jedes Feedback wird vor der Nutzung von einem Recruiter überprüft
Keine automatisierten Entscheidungen	Das System akzeptiert oder lehnt einen Kandidaten niemals automatisch ab
Evidenzbasierte Bewertung	Scores verweisen auf unterstützende Evidenz aus dem Transkript
Anti-Bias-Design	Namen von der Bewertung ausgeschlossen; Inhalt wird höher gewichtet als Stil
Bereichsgrenzen	Persönlichkeit, Emotion, Akzent und geschützte Merkmale werden niemals bewertet
Sicherheit von Kandidatenfeedback	Privates Kandidatenfeedback durchläuft eine Sicherheitsleitplanke für Generierung und Validierung

Diese Einschränkungen sind nicht nur in der Dokumentation festgehalten; sie sind in der AI-Prompt-Schicht kodiert und werden durch ein dediziertes AI-Sicherheits-Testprogramm geprüft, das in Abschnitt 12.3 beschrieben ist.

11. Sicherer Entwicklungslebenszyklus

Sicherheit wird in der Art und Weise durchgesetzt, wie wir Software entwickeln und ausliefern, nicht nur im laufenden System.

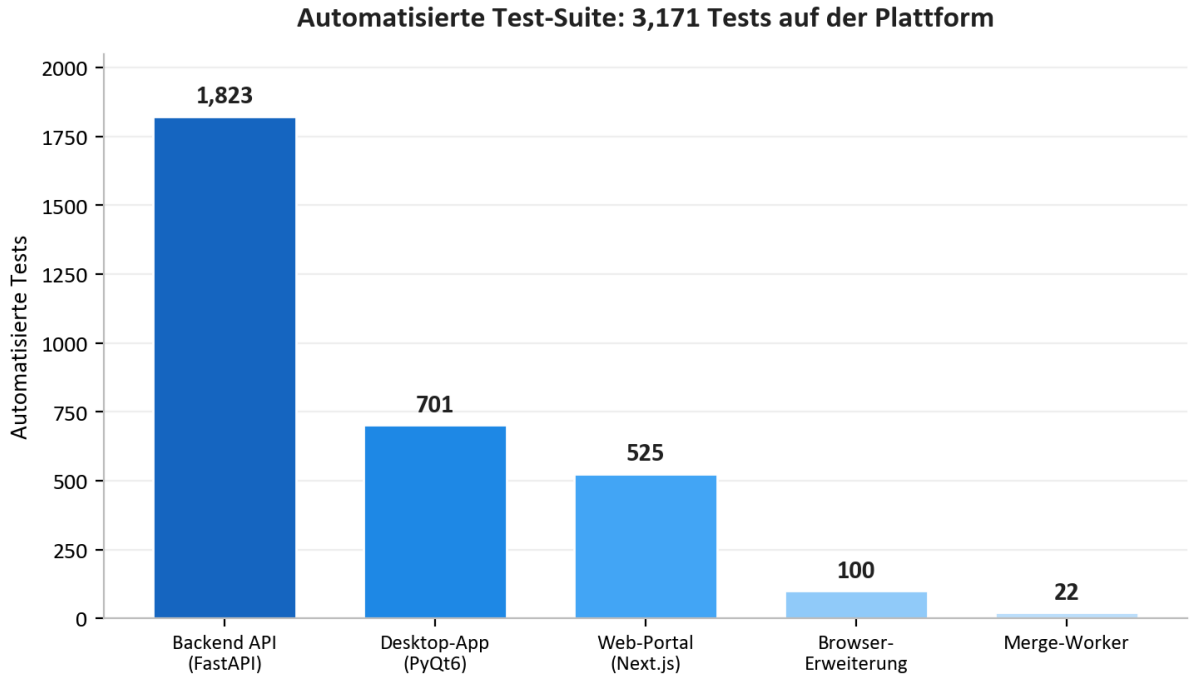
- **Umgebungstrennung.** Entwicklung und Produktion sind vollständig getrennt, jeweils mit eigener Infrastruktur, eigenen Storage-Accounts, eigener Datenbank, eigenen Secrets und eigenen Subdomains. Es gibt keinen gemeinsamen Zustand.
- **Infrastructure as code.** Die gesamte Cloud-Umgebung ist als Code definiert und wird als Code geprüft, wodurch die Sicherheitslage auditierbar und reproduzierbar wird. Ein Reviewer kann exakt nachlesen, welche Ports offen sind, welche Ressourcen privat sind und welche Identitäten welche Berechtigungen haben.
- **Fixierte, kontrollierte Deployments.** Jeder Schritt in der Continuous-Integration-Pipeline ist auf eine exakte, unveränderliche Version fixiert. Produktionsdeployments sind tag-basiert, laufen nur über die geschützte Produktionspipeline und sind durch erforderliche Freigaben abgesichert. Die automatisierte Test-Suite läuft als Release-Gate: Ein Deployment kann nicht ausgeliefert werden, wenn Tests fehlschlagen.
- **Dependency-Hygiene.** Automatisiertes Dependency-Monitoring schlägt wöchentlich Updates für Backend, Desktop, Web, Infrastruktur und Pipelinedefinitionen vor, und Dependency-Audits sind Teil unserer regelmäßigen Sicherheitsprüfung.
- **Signierte Artefakte.** Desktop-Installer sind code-signiert, sodass Kunden prüfen können, dass die von ihnen installierte Software tatsächlich von uns stammt.
- **Disziplin bei Secrets.** Secrets befinden sich im Vault und in geschützten Pipeline-Secrets, niemals im Source Code.

12. Kontinuierliche Sicherheitstests

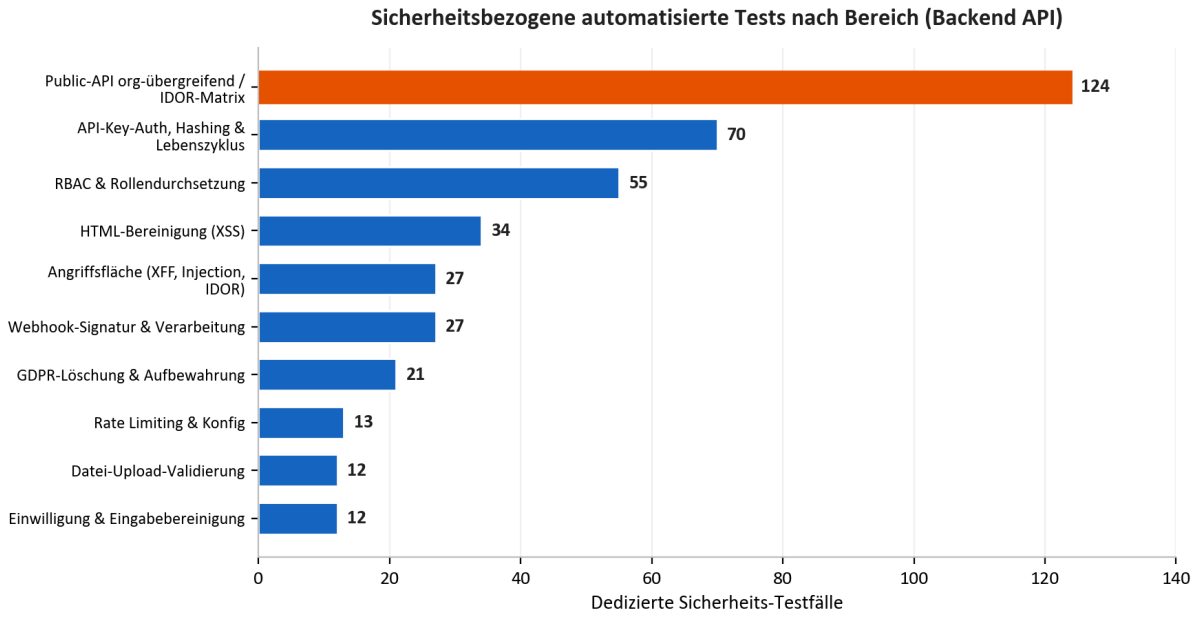
Dies ist das Herzstück unserer Nachweisführung und der Teil, den die meisten Anbieter nicht zeigen können. Wir behandeln Sicherheit als etwas, das kontinuierlich mit ausführbaren Prüfungen gemessen wird, statt einmalig behauptet zu werden.

12.1 Die automatisierte Test-Suite

Die Plattform wird durch **3,171 automatisierte Tests** abgedeckt, die die Backend-API, die Desktop-Anwendung, das Webportal, die Browser-Erweiterung und den Audio-Merge-Worker umfassen.



Dies sind nicht nur Funktionstests. Eine umfangreiche, dedizierte Sicherheitssuite prüft die zuvor in diesem Dokument beschriebenen Kontrollen. Das folgende Diagramm zeigt die sicherheitsspezifischen Tests in der Backend-API nach Bereich.



Unter vielen anderen umfasst diese Suite eine große Public-API-Matrix, die jeden Endpunkt als legitimer Benutzer, mit dem eigenen API Key der Organisation und mit dem API Key einer konkurrierenden Organisation ausführt und bestätigt, dass jeder organisationsübergreifende Versuch blockiert wird. Sie umfasst Dutzende adversarialer Tests der Angriffsoberfläche für Forwarding-Header-Spoofing, Header-Injection und Identifier-Leakage, eine fokussierte HTML-Sanitization-Suite für Cross-Site Scripting, Rollendurchsetzungstests für das vollständige Rollenmodell sowie Tests, die nachweisen, dass Kandidatendaten tatsächlich als Einheit gelöscht werden. Da diese Tests als Release-Gate ausgeführt werden, würde eine Regression, die eine dieser Kontrollen schwächt, die Veröffentlichung stoppen, anstatt Kunden zu erreichen.

12.2 Live-Penetrationstests

Automatisierte Unit-Tests beweisen, dass Kontrollen isoliert korrekt funktionieren. Um nachzuweisen, dass sie in einer realen Bereitstellung zusammenhalten, pflegen wir eine wiederholbare Penetration-Testing-Methodik, die echte Angriffsskripte gegen eine Live-Umgebung ausführt. Sie ist in sechs Phasen organisiert:

Phase	Fokus	Beispiele dafür, was geprüft wird
1. Statische Analyse	Source Code	Secrets, Injection-Muster, gefährliche Funktionen, fehlende Auth, unsicheres HTML
2. Architekturprüfung	Infrastruktur	Private Endpoints, Segmentierung, TLS, Secrets-Konfiguration
3. Analyse von Angriffsvektoren	Source Control und Cloud	Branch Protection, Identity Scope, öffentliche Exponierung
4. Live-Penetrationstests	Laufende Umgebung	Unauthentifiziertes Probing, organisationsübergreifender Zugriff, Injection, Token-Manipulation, SSRF, Rate-Limit-Bursts
5. Enterprise-Bewertung	Reifegrad	Sechzehn Sicherheitskategorien anhand einer Enterprise-Baseline bewertet
6. Dependency- und Supply-Chain	Third-Party-Risiko	Dependency-CVE-Audit, fixierte Pipeline-Actions, Lock-File-Integrität

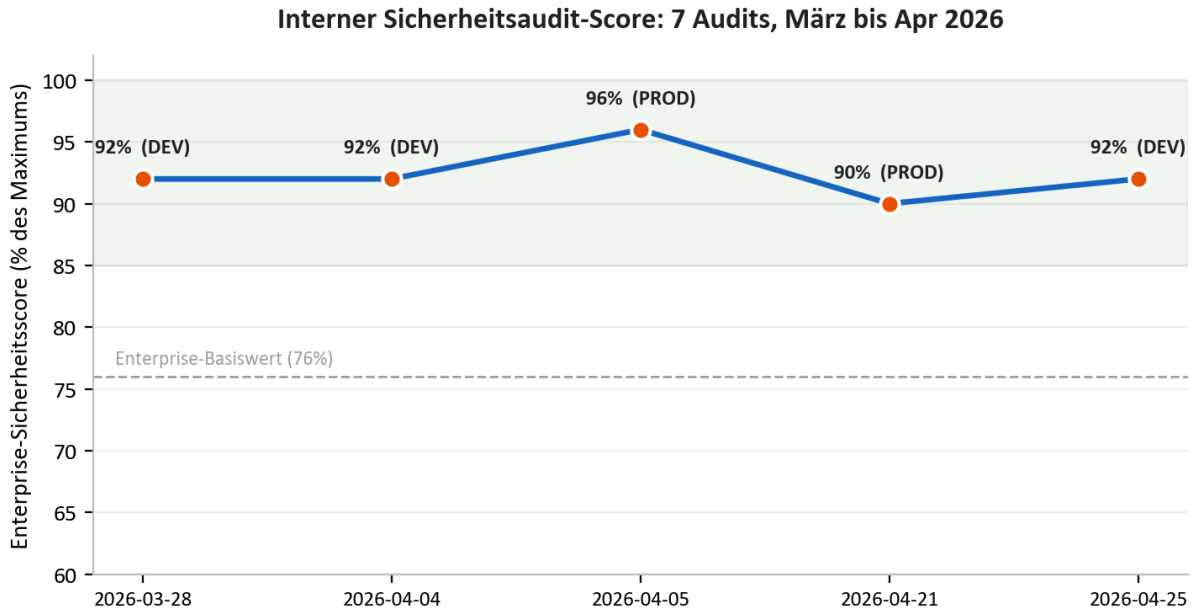
Phase 4 ist echtes adversariales Testen gegen ein bereitgestelltes System, keine Checkliste. Sie prüft geschützte Endpunkte ohne Zugangsdaten und bestätigt, dass sie den Zugriff verweigern; sie registriert zwei Organisationen und versucht, mit dem Konto der einen Organisation auf die Datensätze der anderen zuzugreifen; sie injiziert Cross-Site-Scripting- und Server-Side-Template-Payloads und bestätigt, dass sie neutralisiert werden; sie manipuliert Authentifizierungstokens und bestätigt, dass diese abgelehnt werden; sie versucht Server-Side Request Forgery gegen Cloud-Metadatenendpunkte; und sie setzt Authentifizierungsendpunkte Burst-Last aus, um zu bestätigen, dass Rate Limiting in der Live-Umgebung tatsächlich auslöst und nicht nur theoretisch vorhanden ist.

12.3 Sicherheitstests für Kandidatenfeedback

Da die Plattform privates Entwicklungsfeedback für Kandidaten generieren kann, führen wir ein separates adversariales Sicherheitsprogramm gegen diese Funktion aus. Es speist dem System absichtlich harte und feindselige Recruiter-Notizen ein und bestätigt, dass die kandidatenseitige Ausgabe niemals Vulgarität enthält, niemals die Identität oder private Meinung eines Recruiters offenlegt oder zuordnet und niemals wertende Persönlichkeitslabels verwendet. Dies schützt sowohl den Kandidaten, der konstruktives und respektvolles Feedback erhalten soll, als auch den Kunden, dessen interne Meinung niemals nach außen dringen sollte.

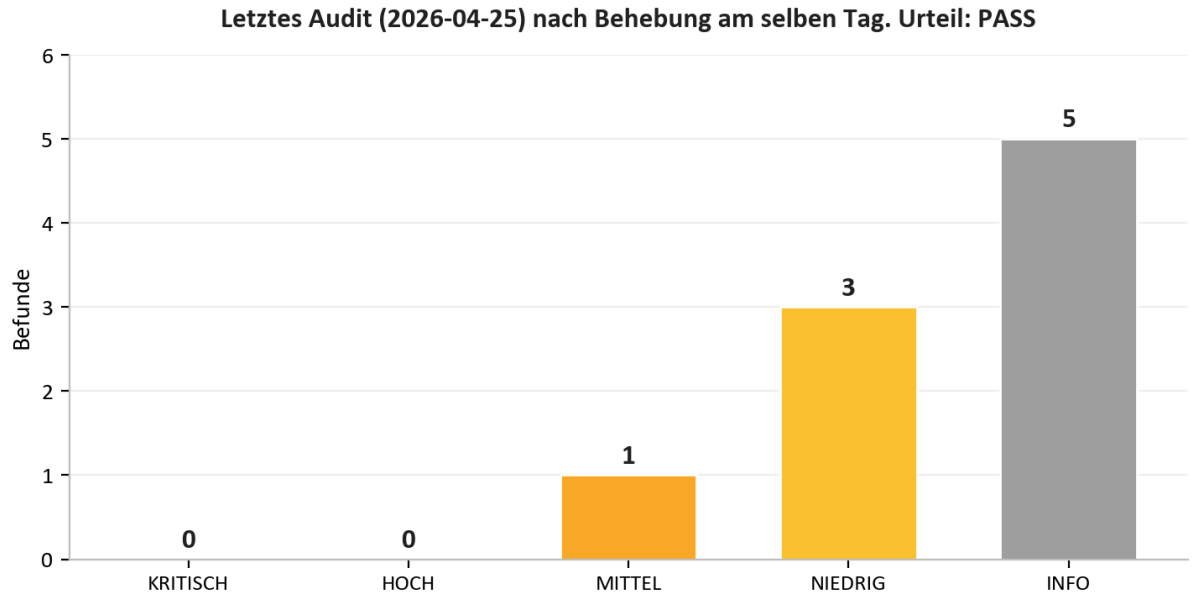
13. Ergebnisse der Sicherheitsaudits

Wir führen wiederkehrende Sicherheitsaudits mit einer strukturierten, wiederholbaren Penetration-Testing-Methodik durch und dokumentieren jedes Audit als datierten Bericht mit nach Schweregrad bewerteten Feststellungen, Evidenz und Abhilfemaßnahmen. Dabei handelt es sich um interne Audits, die durch unseren eigenen Sicherheitsprozess durchgeführt werden; die formale Drittzertifizierung derselben Kontrollen befindet sich auf unserer Roadmap. Zwischen Ende März und Ende April 2026 haben wir **seven such audits** in Entwicklung und Produktion abgeschlossen.



Das für einen potenziellen Kunden wichtigste Ergebnis ist die Konsistenz: **across all seven audits there were zero critical findings.** In den seltenen Fällen, in denen ein Problem mit höherem Schweregrad auftrat, wurde es schnell behoben, häufig noch am selben Tag, und erneut verifiziert. Die Bewertungsrubrik wurde in diesem Zeitraum bewusst verschärft (die maximal mögliche Punktzahl wurde erhöht, als wir zusätzliche Kategorien zur Bewertung hinzugefügt haben), weshalb die normalisierte Bewertungsreihe hoch bleibt, obwohl die Messlatte angehoben wurde.

Unser jüngstes Audit am 25 April 2026 veranschaulicht, wie der Prozess in der Praxis funktioniert. Zwei Probleme mit höherem Schweregrad wurden identifiziert, beide noch am selben Tag behoben und erneut verifiziert, und das Audit wurde mit dem Urteil **PASS** geschlossen, ohne dass im aktuellen Bedrohungsmodell ausnutzbare Probleme verblieben.



Audit	Umgebung	Kritisch	Urteil
2026-03-28	Entwicklung	0	Bereit für Produktion
2026-04-04	Entwicklung	0	Enterprise-ready
2026-04-05	Produktion	0	Enterprise-ready
2026-04-20	Entwicklung	0	Produktionsbereit, Hinweise
2026-04-20	Entwicklung	0	Bestanden mit Hinweisen
2026-04-21	Produktion	0	Sicher, keine ausnutzbaren Findings
2026-04-25	Entwicklung	0	Bestanden

Das Muster über diese Audits hinweg ist die ehrlichste Evidenz, die wir anbieten können: Probleme werden gefunden, weil wir intensiv nach ihnen suchen, und sie werden schnell geschlossen, weil der Prozess darauf ausgelegt ist, sie zu schließen. Ein Anbieter, der nie ein Finding meldet, ist in der Regel ein Anbieter, der nicht sucht.

---

14. Operative Resilienz und geteilte Verantwortung

14.1 Monitoring und Logging

Anwendungs- und Plattformtelemetrie fließen in einen zentralisierten Log-Analytics-Workspace und einen Anwendungs-Monitoring-Service, wodurch wir Sichtbarkeit in Verfügbarkeit und Verhalten erhalten. Sensible Aktionen wie Datenlöschung, Annahme rechtlicher Vereinbarungen und AI-Aufrufe werden in dedizierten Audit-Tabellen protokolliert, sodass ein belastbarer Nachweis darüber besteht, wer was mit wichtigen Daten getan hat.

14.2 Backup und Wiederherstellung

Die verwaltete Datenbank bewahrt automatisierte Backups auf, und privater Storage ist durch Soft-Delete-Aufbewahrung sowohl für Blobs als auch für Container geschützt, sodass versehentliche oder böswillige Löschung innerhalb des Aufbewahrungsfensters wiederhergestellt werden kann. Kritische Infrastruktur ist mit Deletion Locks versehen, um eine versehentliche Entfernung von Produktionsressourcen zu verhindern.

14.3 Zusammenfassung der geteilten Verantwortung

Bereich	AI Interview Analyzer	Kunde
Infrastruktur, Netzwerk, Patching	Ja	-
Anwendungssicherheit und AI-Pipeline	Ja	-
Verschlüsselung, Secrets, Datenresidenz	Ja	-
Benutzer- und Rollenverwaltung	Stellt die Kontrollen bereit	Verwaltet Benutzer und Rollen
Konfiguration der Aufbewahrungsrichtlinie	Stellt die Kontrollen bereit	Legt das Aufbewahrungsfenster fest
Einwilligung der Kandidaten	Stellt den Workflow bereit	Stellt sicher, dass er verwendet wird
Starke Endbenutzer-Zugangsdaten und SSO	Unterstützt SSO und Richtlinien	Erzwingt interne Richtlinien

15. Bedrohungsmodell und OWASP-Mapping

Wir entwerfen gegen ein konkretes Set von Angreifern: einen externen Angreifer ohne Zugangsdaten, einen neugierigen oder böswilligen authentifizierten Benutzer einer Organisation, der versucht, auf die Daten einer anderen Organisation zuzugreifen, eine kompromittierte Dependency und einen internen Fehler. Die folgende Tabelle ordnet die weit verbreiteten OWASP Top 10-Risikokategorien den spezifischen Kontrollen zu, die sie in dieser Plattform adressieren und die jeweils durch die in Abschnitt 12 beschriebenen Tests geprüft werden.

OWASP-Risiko	Wie die Plattform es mindert
Broken access control	Rollenbasierte Zugriffskontrolle auf jedem privilegierten Endpunkt; organisationsbezogene Begrenzung; „not found“ bei organisationsübergreifendem Zugriff; Identifier-Remapping; organisationsübergreifende Testmatrix
Cryptographic failures	TLS 1.2+ bei der Übertragung; AES-256 im Ruhezustand; bcrypt-Passwort-Hashing; Secrets in einem Managed Vault
Injection	Ausschließlich ORM-basierte parametrisierte Abfragen; strikte Schemavalidierung; HTML-Sanitization beim Schreiben
Insecure design	Mehrschichtige Defense in Depth; Bedrohungsmodellierung und Architekturprüfung in jedem Audit
Security misconfiguration	Infrastructure as code; Default-Deny-Netzwerkgruppen; Security Headers; deaktivierte Shared Storage Keys; API-Schema in Produktion nicht exponiert
Vulnerable components	Wöchentliches automatisiertes Dependency-Monitoring; Dependency-CVE-Audits in regelmäßigen Reviews
Identification and authentication failures	Kurzlebige Tokens; rate-limitierter Login; E-Mail-Verifizierung; SSO-Unterstützung; keine Klartextpasswörter
Software and data integrity failures	Fixierte, unveränderliche Pipeline-Schritte; signierte Desktop-Installer; Verifizierung von Webhook-Signaturen; tag-gesteuerte Produktionsdeployments
Security logging and monitoring failures	Zentralisierte Telemetrie; dedizierte Audit-Tabellen für sensible Aktionen
Server-side request forgery	Ausgehende Aufrufe auf vertrauenswürdige Endpunkte beschränkt; SSRF-Prüfungen im Penetration-Test-Harness

Dieses Mapping ist das Rückgrat unserer Nachweisführung: Für jede bekannte Angriffsklasse gibt es eine benannte Kontrolle, und für jede benannte Kontrolle gibt es einen Test.

16. Schwachstellenmanagement und Responsible Disclosure

Sicherheit ist niemals abgeschlossen, daher betreiben wir einen kontinuierlichen Zyklus aus Erkennung und Behebung.

- **Erkennung.** Schwachstellen werden aus vier Quellen sichtbar: der automatisierten Test-Suite, den wiederkehrenden Penetration-Test-Audits, automatisiertem Dependency-Monitoring und Meldungen von Kunden oder Forschern.
- **Triage.** Jedem Finding wird ein Schweregrad (critical, high, medium, low oder informational) mit Evidenz und einem Verantwortlichen für die Behebung zugewiesen, genau wie in unseren Auditberichten festgehalten.
- **Ziele für die Behebung.** Critical- und High-Findings werden für eine sofortige Behebung priorisiert; in unserer Audit-Historie wurden Findings höheren Schweregrads typischerweise noch am selben Tag behoben und erneut verifiziert. Medium- und niedrigere Findings werden in den regulären Wartungszyklus eingeplant.
- **Verifizierung.** Fixes werden erneut getestet, und sofern relevant wird eine Live-Prüfung gegen die bereitgestellte Umgebung ausgeführt, um zu bestätigen, dass das Problem tatsächlich geschlossen ist und nicht nur im Code.
- **Offenlegung.** Sicherheitsbedenken können uns direkt gemeldet werden. Wir bestätigen den Eingang von Meldungen, untersuchen sie und halten die meldende Person bis zur Behebung auf dem Laufenden.

17. Compliance-Mapping

17.1 GDPR

GDPR-Bereich	Plattformimplementierung
Rechtsgrundlage (Art. 6)	Ausdrückliche Einwilligung des Kandidaten vor der Verarbeitung erfasst
Datenminimierung und Speicherbegrenzung (Art. 5)	Es werden nur interviewrelevante Daten verarbeitet; konfigurierbare Aufbewahrung mit automatischer Löschung
Recht auf Löschung (Art. 17)	Löschung aller Kandidatendaten als einzelne Einheit, mit protokolliertem Löschungsnachweis
Rechte betroffener Personen (Art. 15 bis 20)	Auskunft, Löschung, Übertragbarkeit und Widerspruch werden unterstützt
Pflichten des Auftragsverarbeiters (Art. 28)	Data Processing Agreement wird bei der Registrierung akzeptiert und pro Organisation versioniert
Sicherheit der Verarbeitung (Art. 32)	Verschlüsselung, Zugriffskontrolle, Isolation und kontinuierliche Tests wie in diesem Dokument beschrieben
Transparenz bei Sub-Processors	Im Data Processing Agreement mit Vorankündigung von Änderungen offengelegt

17.2 EU AI Act

Die Plattform wird als Hochrisiko-AI-System behandelt, das Beschäftigungsentscheidungen unterstützt, und wir pflegen an der Verordnung ausgerichtete Dokumentation, darunter eine Transparency Card, Benutzerdokumentation und eine Declaration of Conformity. Die zentralen Schutzmaßnahmen, menschliche Aufsicht, Transparenz, evidenzbasierte Bewertung und strikte Bereichsgrenzen dessen, was die AI bewertet, sind in Abschnitt 10 beschrieben. Wir entwickeln unsere formale Konformitätsdokumentation weiter, während der Umsetzungszeitplan der Verordnung voranschreitet.

17.3 Hosting-Zertifizierungen

Die Plattform läuft vollständig auf Microsoft Azure, dessen Rechenzentren unabhängige Zertifizierungen einschließlich ISO 27001 und SOC 2 tragen. Diese Zertifizierungen decken die physischen und Plattformschichten unterhalb unserer Anwendung ab; die Kontrollen auf Anwendungsebene sind diejenigen, die in diesem Dokument beschrieben werden.

17.4 Sub-Processor-Register

Sub-Processor	Zweck	Region
Microsoft Azure	Hosting, AI- und Sprachverarbeitung, Storage, transaktionale E-Mail	EU (West Europe, Sweden Central)
Stripe	Abonnement- und Zahlungsabwicklung	EU (Ireland)
Fakturownia	Rechnungsstellung	EU (Poland)
ATS connector (optional)	Applicant-Tracking-Integration, nur auf Anfrage aktiviert	EU

18. Sicherheits-Roadmap

Wir behandeln Sicherheit als ein Programm kontinuierlicher Verbesserung. Zu den aktuellen Initiativen auf unserer Roadmap gehören die Stärkung der Optionen für Multi-Factor Authentication bei administrativen Konten, der Ausbau zentralisierten Audit Loggings von Datenzugriffen, die weitere regelmäßige Straffung der Aktualität von Dependencies sowie die Fortschreibung der formalen Drittzertifizierung der in diesem Dokument beschriebenen Kontrollen. Keines dieser Themen ist eine Lücke, die heute Kundendaten exponiert; jedes davon ist eine Verbesserung einer bereits mehrschichtigen Sicherheitslage.

19. Zusammenfassung

AI Interview Analyzer schützt Kandidaten- und Kundendaten durch eine mehrschichtige Architektur: ein standardmäßig privates Netzwerk ohne öffentliche Datendienste, starke Identität und organisationsbezogene Isolation, Anwendungscode, der ganze Schwachstellenklassen aus dem Design entfernt, Verschlüsselung und EU-Datenresidenz sowie Datenschutzkontrollen, die in das Datenmodell eingebaut sind. Was die Plattform auszeichnet, ist die Evidenz hinter diesen Aussagen. Mit 3,171 automatisierten Tests, einer wiederholbaren Methodik für Live-Penetrationstests, einem dedizierten AI-Sicherheitsprogramm und einer Historie von sieben internen Sicherheitsaudits mit zero critical findings können wir zeigen und nicht nur sagen, dass die Plattform sicher ist.

Appendix A: Katalog der Sicherheitskontrollen

Eine komprimierte Referenz der primären Kontrollen und der Evidenz, die jede einzelne stützt.

Kontrolle	Mechanismus	Evidenz
Transportverschlüsselung	Nur HTTPS, TLS 1.2+, HTTP umgeleitet	Infrastructure as code; Architekturaudit
Verschlüsselung im Ruhezustand	AES-256-Plattformverschlüsselung für Storage und Datenbank	Plattformkonfiguration; Architekturaudit
Passwortschutz	bcrypt mit Salt pro Passwort	Source Control; Authentifizierungstests
Sitzungsmanagement	30-minütige signierte Tokens, widerrufbare serverseitige Refreshes	Source Control; Authentifizierungstests
Autorisierung	Zugriffskontrolle mit vier Rollen auf privilegierten Endpunkten	Rollendurchsetzungs-Test-Suite
Tenant-Isolation	Organisationsbezogene Begrenzung von Abfragen; 404 organisationsübergreifend	Organisationsübergreifende Testmatrix
API-Key-Sicherheit	Gehashte Speicherung, begrenzte Berechtigungen, Rate Limits pro Key	API-Key-Test-Suite
Schutz vor Injection	Ausschließlich ORM-basierte parametrisierte Abfragen	Statische Analyse; Injection-Tests
Schutz vor Cross-Site Scripting	HTML-Sanitization beim Schreiben	HTML-Sanitization-Test-Suite
Rate Limiting	Langlebiger datenbankgestützter Limiter auf Auth-Endpunkten	Rate-Limit-Tests; Live-Burst-Prüfungen
Webhook-Integrität	Verifizierung der Anbietersignatur auf dem rohen Body	Webhook-Test-Suite
Secrets Management	Managed Vault, Purge Protection, Managed Identity	Infrastructure as code; Architekturaudit
Netzwerkisolation	Private Endpoints; Default-Deny-Segmentierung	Infrastructure as code; Architekturaudit
Datenlöschung	Kaskadierende Löschung als einzelne Einheit mit Audit Log	GDPR-Löschtest-Suite
Supply Chain	Fixierte Pipeline-Schritte; wöchentliches Dependency-Monitoring	Pipeline-Konfiguration; Dependency-Audit

Appendix B: Häufig gestellte Fragen für Security Reviewer

Wo werden unsere Daten gespeichert? Vollständig innerhalb der Europäischen Union, auf Microsoft Azure, in West Europe mit AI-Verarbeitung in EU-Regionen. Kandidatendaten verlassen niemals die EU.

Werden unsere Daten zum Training von AI-Modellen verwendet? Nein. Der AI-Anbieter verwendet Kundendaten nicht für das Training.

Ist die Datenbank aus dem Internet erreichbar? Nein. Der öffentliche Netzwerkzugriff ist deaktiviert, und die Datenbank ist nur über einen Private Endpoint innerhalb des virtuellen Netzwerks erreichbar.

Kann ein Kunde die Daten eines anderen Kunden sehen? Nein. Jede Abfrage ist auf die Organisation des Aufrufers begrenzt, organisationsübergreifender Zugriff liefert „not found“ zurück, und eine automatisierte Matrix testet diese Isolation fortlaufend.

Wie werden Passwörter gespeichert? Gehasht mit bcrypt und einem eindeutigen Salt pro Passwort. Single Sign-On mit Microsoft und Google wird unterstützt; in diesem Fall wird kein Passwort gespeichert.

Unterstützen Sie Single Sign-On? Ja, über Microsoft und Google OAuth.

Wie lange sind Access Tokens gültig? Dreißig Minuten, gekoppelt mit einer widerrufbaren serverseitigen Refresh-Session, die beim Logout ungültig gemacht wird.

Wie wird die Einwilligung von Kandidaten behandelt? Jeder Kandidat erhält einen eindeutigen, einmal verwendbaren Einwilligungslink und muss zustimmen, bevor eine Aufzeichnung oder Analyse erfolgt. Die Einwilligung wird gegen den spezifischen Einstellungsprozess protokolliert.

Wie werden Daten gelöscht? Als einzelne Einheit, die den Kandidatendatensatz, Interviews, Transkripte, Audio, Dokumente und Vergleiche umfasst, nach einem konfigurierbaren Aufbewahrungsplan, mit einem protokollierten Löschungsnachweis. Kandidaten können die Löschung auch direkt anfordern.

Haben Sie ein Data Processing Agreement? Ja, es wird bei der Registrierung akzeptiert und pro Organisation versioniert, einschließlich des Sub-Processor-Registers.

Trifft die AI Einstellungsentscheidungen? Nein. Sie bietet nur Entscheidungsunterstützung; ein Mensch überprüft jede Ausgabe und trifft alle Entscheidungen.

Wie weisen Sie Ihre Sicherheitsbehauptungen nach? Durch 3,171 automatisierte Tests einschließlich einer dedizierten Sicherheitssuite, eine wiederholbare sechsstufige Penetration-Testing-Methodik, die gegen Live-Umgebungen ausgeführt wird, ein AI-Sicherheits-Testprogramm und wiederkehrende schriftliche Auditberichte.

Was passiert, wenn Sie eine Schwachstelle finden? Sie erhält einen Schweregrad mit Evidenz und einem Verantwortlichen, wird nach Priorität behoben, erneut verifiziert einschließlich Live-Prüfungen, sofern relevant, und in einem Auditbericht dokumentiert.

Können wir unseren eigenen Penetrationstest durchführen? Sicherheitsbewertungen können über Ihren Ansprechpartner unter angemessener Festlegung von Umfang und Zeitplanung vereinbart werden.

Appendix C: Glossar

Begriff	Bedeutung
AES-256	Ein starker symmetrischer Verschlüsselungsstandard zum Schutz von Daten im Ruhezustand
bcrypt	Eine speziell entwickelte Passwort-Hashing-Funktion mit Salt pro Passwort
Managed identity	Eine von der Plattform ausgegebene Identität, mit der sich ein Service ohne gespeicherte Keys authentifizieren kann
Private endpoint	Eine private Netzwerkadresse, die einen Cloud-Service vom öffentlichen Internet fernhält
Network security group	Eine Menge von Allow- und Deny-Regeln, die den Netzwerkverkehr zu einem Subnet filtern
RBAC	Rollenbasierte Zugriffskontrolle, die Berechtigungen entsprechend der Rolle eines Benutzers gewährt
IDOR	Insecure direct object reference, eine Zugriffskontrollschwachstelle, gegen die sich die Plattform schützt
SSRF	Server-side request forgery, eine Angriffsklasse, die in unseren Penetrationstests geprüft wird
Web application firewall	Eine Edge-Kontrolle, die bösartigen Webverkehr filtert
Data processing agreement	Der Vertrag, der regelt, wie ein Auftragsverarbeiter personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet

Appendix D: Kontakt und Dokumentenkontrolle

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Für eine Sicherheitsprüfung, eine Kopie unseres Data Processing Agreement oder unsere EU AI Act-Konformitätsdokumentation wenden Sie sich bitte an Ihren Ansprechpartner.

Dieses Dokument beschreibt die Sicherheitslage des AI Interview Analyzer-Services zum im Footer angegebenen Erstellungsdatum. Es wird zu Bewertungszwecken bereitgestellt und ist nicht Bestandteil eines Vertrags. Konkrete vertragliche Sicherheitszusagen sind in der anwendbaren Vereinbarung und im Data Processing Agreement festgelegt.