Bezpečnostní whitepaper

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Bezpečnostní whitepaper

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

Cílová skupina: Podnikové týmy pro bezpečnost, IT a nákup

Klasifikace: Veřejné

1. Shrnutí pro vedení

AI Interview Analyzer je podniková platforma pro nábor, která se záznamem pohovorů pracuje pouze s výslovným souhlasem kandidáta, převádí je do textu a strukturuje je a poskytuje náborářům podporu hodnocení založenou na důkazech. Protože platforma zpracovává osobní údaje kandidátů a podporuje náborové procesy, jsou bezpečnost a soukromí považovány za primární konstrukční omezení, nikoli za funkce přidané dodatečně.

Tento whitepaper popisuje konkrétním a ověřitelným způsobem, jak chráníme data zákazníků a kandidátů. Je určen lidem, kteří posuzují dodavatele: bezpečnostním inženýrům, IT administrátorům, pověřencům pro ochranu osobních údajů a nákupu. Každý údaj v tomto dokumentu pochází přímo z našich vlastních inženýrských systémů, nikoli z marketingových materiálů.

Ústřední sdělení je jednoduché: **netvrdíme pouze, že je platforma bezpečná, ale průběžně testujeme, že taková skutečně je.** Náš kód obsahuje **3,171 automatizovaných testů**, včetně vyhrazené bezpečnostní sady, která ověřuje autentizaci, autorizaci, izolaci mezi organizacemi, ochranu proti injection útokům a mazání dat. Nad rámec toho provozujeme opakovatelný penetrační testovací rámec proti živým nasazením a vytváříme písemné auditní zprávy. V průběhu sedmi interních bezpečnostních auditů v březnu a dubnu 2026 jsme zaznamenali **zero critical findings**, přičemž náš nejnovější audit byl uzavřen verdiktem **PASS**. (Formální certifikace těchto kontrol třetí stranou je součástí naší roadmapy; viz oddíl 18.)

Bezpečnostní charakteristika	Shrnutí
Hosting	Microsoft Azure, pouze regiony EU
Síťový model	Privátní endpointy, segmentace sítě typu default-deny, žádná veřejná databáze
Šifrování	AES-256 v klidu, TLS 1.2 nebo vyšší při přenosu
Identita	Krátkodobé podepsané tokeny, hashování hesel bcrypt, podpora SSO
Řízení přístupu	Řízení přístupu na základě rolí se striktní izolací po organizacích
Tajné údaje	Centralizovaný vault pro tajné údaje s přístupem přes managed identity
Soukromí	Výslovný souhlas, konfigurovatelná retence, mazání jako jedné jednotky
Odpovědná AI	Pouze podpora rozhodování, člověk je vždy v rozhodovací smyčce
Zajištění	3,171 automatizovaných testů plus opakované penetrační testy a audity

1.1 Jak číst tento dokument

Oddíly 3 až 11 popisují kontroly chránící data: architekturu, síť, identitu, aplikaci, ochranu dat, soukromí a bezpečný životní cyklus vývoje. Oddíly 12 a 13 pokrývají náš charakteristický program průběžného testování a naši historii auditů. Oddíly 14 až 17 pokrývají provoz, threat modeling, správu zranitelností a mapování souladu. Přílohy poskytují katalog kontrol, FAQ pro posuzovatele a glosář, který může bezpečnostní tým přímo použít při hodnocení.

2. Rozsah dokumentu a přístup

2.1 Co tento dokument pokrývá

Tento whitepaper pokrývá bezpečnostní architekturu a postupy služby AI Interview Analyzer: hostingové prostředí, návrh sítě, správu identit a přístupu, kontroly na aplikační úrovni, ochranu dat, soukromí a regulatorní soulad, bezpečný životní cyklus vývoje a náš program průběžného bezpečnostního testování.

2.2 Co jej činí ověřitelným

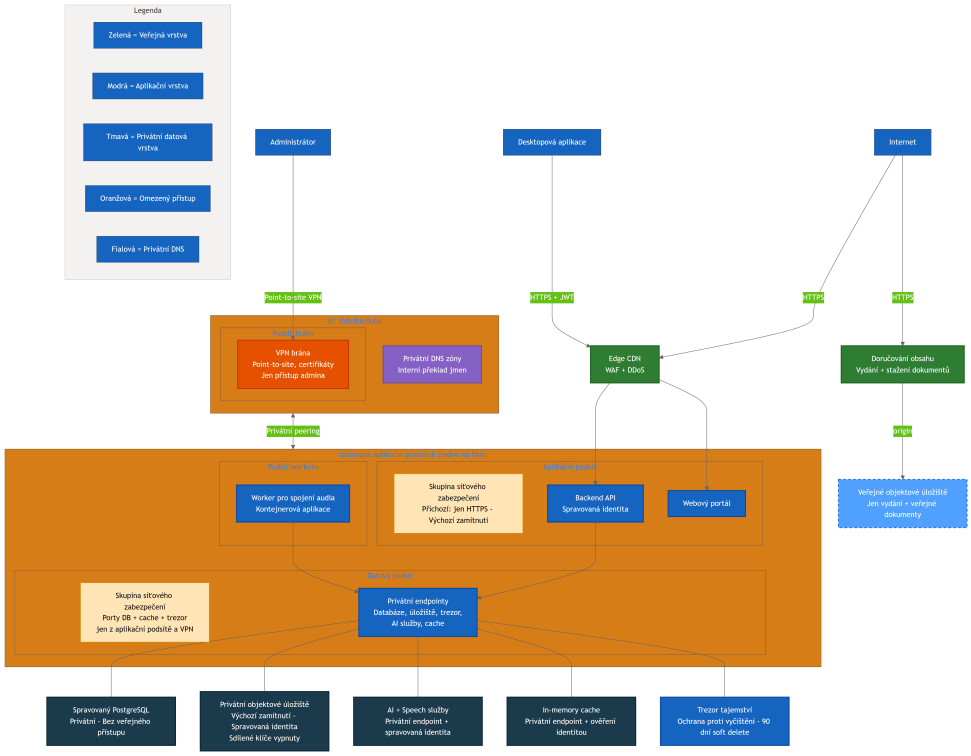
Bezpečnostní tvrzení dodavatelů se snadno píší a obtížně se jim důvěřuje. Každé hlavní tvrzení v tomto dokumentu jsme proto navázali na něco konkrétního a měřitelného v našich inženýrských systémech: kontrolu implementovanou v kódu, test, který prokazuje funkčnost této kontroly, definici infrastruktury, která ji vynucuje, nebo auditní zprávu zaznamenávající zdokumentovanou kontrolu. Pokud je kontrola součástí naší budoucí roadmapy a ještě není dnes nasazena, uvádíme to výslovně. Raději budeme tvrdit méně a budeme důvěryhodní, než tvrdit více a být usvědčeni z nadsázky.

2.3 Sdílená odpovědnost

Platforma je poskytována jako software jako služba. Provozujeme infrastrukturu, aplikaci, AI pipeline a zpracování dat. Zákazník odpovídá za správu vlastních uživatelských účtů a rolí, konfiguraci retenčních lhůt dat tak, aby odpovídaly jeho interní politice, a za zajištění získání souhlasu kandidátů prostřednictvím workflow souhlasu, které platforma poskytuje. Oddíl 14 tuto dělbu odpovědnosti popisuje podrobněji.

3. Přehled bezpečnostní architektury

Platforma je postavena jako malý počet spolupracujících služeb, nikoli jako jeden monolit. Jako klienti fungují desktopová aplikace a webový portál. Centrální backend API spravuje veškerou persistenci, autentizaci, billing, AI pipeline, souhlas, e-mail, práci se soubory a dashboardy. Worker pro slučování audia zpracovává nahrávky asynchronně. Veškerý citlivý stav je umístěn za backend API; klienti nikdy nekomunikují přímo s databází, úložištěm ani AI službami.



Výše uvedený diagram zobrazuje produkční topologii se záměrně zobecněnými názvy prostředků. Jsou na něm patrné tři principy:

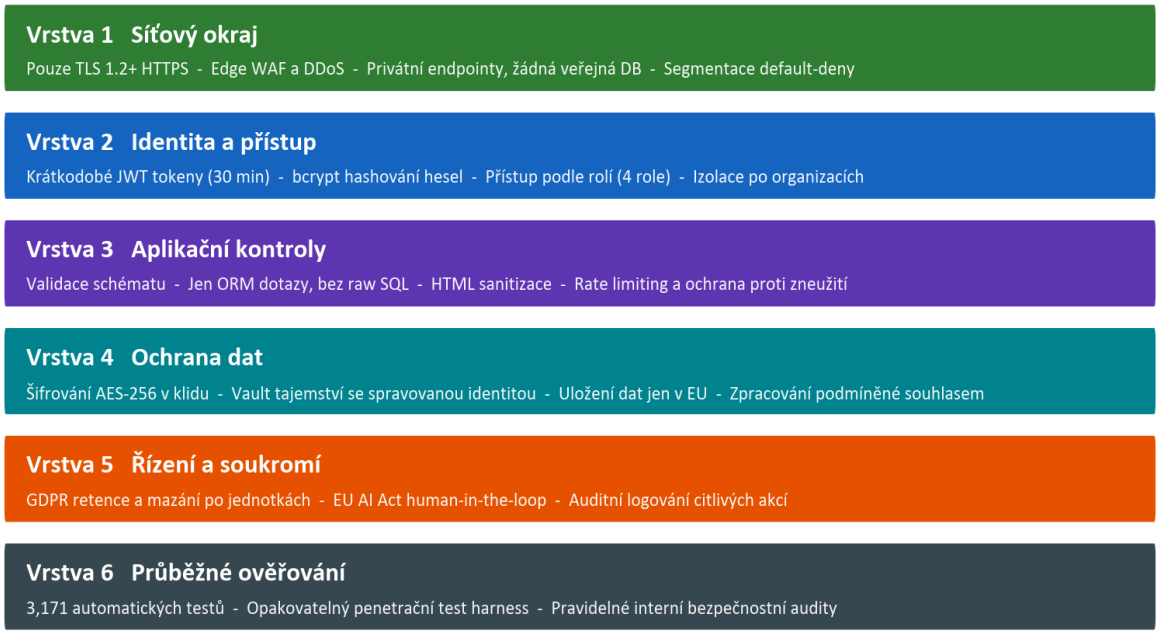
- **Žádné přímé vystavení datových služeb.** Databáze, privátní objektové úložiště, AI služby a cache mají zakázaný veřejný síťový přístup a jsou dosažitelné pouze prostřednictvím privátních endpointů uvnitř izolované virtuální sítě. Vault pro tajné údaje je aplikací dosažen přes privátní endpoint a je navíc chráněn autentizací identity platformy a zásadami přístupu s minimálními oprávněními, takže jakýkoli přístup vyžaduje platnou autorizovanou identitu bez ohledu na síťovou cestu.
- **Oddělená veřejná plocha.** Jediné veřejné objektové úložiště obsahuje instalační balíčky a veřejné dokumenty. Nikdy neobsahuje data kandidátů. Provoz aplikace směrem k zákazníkům prochází přes edge vrstvu, která poskytuje web application firewall, ochranu proti distributed-denial-of-service a distribuci obsahu.
- **Administrativní přístup je řízen.** Operátoři přistupují k interním prostředkům pouze prostřednictvím VPN point-to-site založené na certifikátech do management hub sítě, nikoli přes veřejný internet.

Každá fáze nasazení (vývoj a produkce) je plně izolované prostředí s vlastní sítí, účty úložiště, databází a tajnými údaji. Produkční data zákazníků se nikdy nenacházejí v nižších prostředích. Sdílený management hub obsahuje pouze VPN gateway a privátní DNS, soukromě propojené s každým prostředím.

4. Hloubková obrana

Žádná jednotlivá kontrola není považována za dostačující k zastavení všech útoků. Platforma vrství nezávislé kontroly tak, aby selhání jedné vrstvy nevedlo k vystavení dat. Níže uvedené vrstvy jsou všechny implementovány a, jak je popsáno v oddílu 12, jednotlivě testovány.

Vrstvený bezpečnostní model: nezávislé kontroly v každé vrstvě



Vrstva	Reprezentativní kontroly
Síťový okraj	Pouze TLS přenos, edge WAF a ochrana proti DDoS, privátní endpointy, segmentace typu default-deny
Identita a přístup	Krátkodobé podepsané tokeny, hashování bcrypt, řízení přístupu podle rolí, izolace po organizacích
Aplikace	Validace schémat na všech vstupech, přístup k datům pouze přes ORM, kódování výstupu, rate limiting
Ochrana dat	Šifrování v klidu, vault pro tajné údaje s managed identity, rezidence dat v EU, zpracování podmíněné souhlasem
Governance a soukromí	Konfigurovatelná retence, mazání jako jedné jednotky, AI s člověkem v rozhodovací smyčce, auditní logování
Průběžné zajištění	Automatizovaná sada testů, opakovatelné penetrační testy, pravidelné interní bezpečnostní audity

Zbytek tohoto dokumentu postupně prochází každou vrstvu a poté popisuje, jak průběžně prokazujeme, že tyto vrstvy fungují.

5. Bezpečnost sítě

5.1 Privátní ve výchozím stavu

Datová vrstva je privátní již svou konstrukcí. Spravovaná databáze PostgreSQL má zakázaný veřejný síťový přístup a je dosažitelná pouze přes privátní endpoint. Privátní objektové úložiště je nakonfigurováno tak, aby ve výchozím stavu zakazovalo síťový přístup, zcela vypíná shared access keys a je přístupné pouze přes managed identity z aplikačního subnetu. Cache, AI služby a vault pro tajné údaje jsou obdobně dosažitelné prostřednictvím privátních endpointů s privátním DNS rozlišením.

V praxi to znamená, že pro databázi neexistuje žádný connection string dostupný z internetu a pro audio kandidátů žádné veřejné URL úložiště: databáze i privátní úložiště mají veřejný síťový přístup zcela vypnutý. Vault pro tajné údaje je aplikací dosažen přes privátní endpoint a je chráněn autentizací identity platformy a zásadami přístupu s minimálními oprávněními, přičemž identitám aplikace je udělen přístup pouze pro čtení jen k těm tajným údajům, které potřebují, takže tajné údaje nelze získat bez platné autorizované identity. Plocha útoku, které se externí protivník může vůbec dotknout, je omezena na HTTPS endpointy aplikace za edge vrstvou.

5.2 Segmentace sítě

Každé prostředí je rozděleno do samostatných subnetů pro aplikační vrstvu, datovou vrstvu a asynchronního workera. Každý subnet je řízen network security group, jejíž finální pravidlo zakazuje veškerý příchozí provoz. Aplikační subnet přijímá pouze příchozí HTTPS. Datový subnet přijímá pouze konkrétní porty databáze, cache a vaultu, a to pouze z aplikačního subnetu nebo z administrativní VPN. To znamená, že ani útočník, který by se nějak dostal do aplikační vrstvy, nemůže volně pokračovat do datové vrstvy; povoleny jsou pouze cesty, které aplikace legitimně používá.

5.3 Edge vrstva

Veřejný aplikační provoz je obsluhován přes edge vrstvu poskytující web application firewall, ochranu proti DDoS a content delivery network. Stažení instalačních balíčků a dokumentů jsou obsluhována z vyhrazeného veřejného účtu úložiště přes front door pro doručování obsahu, zcela odděleně od privátního úložiště, které obsahuje data kandidátů. Tyto dvě vrstvy úložiště se nikdy nemíchají: chybná konfigurace ve veřejné vrstvě nemůže odhalit privátní data kandidátů, protože jde o různé účty s různými síťovými pravidly.

5.4 Administrativní přístup

Do privátní sítě neexistuje žádný veřejný administrativní endpoint. Operátoři se připojují prostřednictvím VPN gateway point-to-site, která používá autentizaci založenou na certifikátech. Administrativní přístup k databázi a cache je možný pouze uvnitř tohoto tunelu, protože tyto služby mají veřejný síťový přístup vypnutý. To udržuje každodenní provoz zcela mimo veřejný internet.

6. Správa identit a přístupu

6.1 Autentizace

Uživatelské relace jsou navázány pomocí podepsaného access tokenu s platností třicet minut, spárovaného se samostatným neprůhledným refresh tokenem na straně serveru. Access tokeny jsou ověřovány při každém požadavku a uživatel je znovu validován vůči databázi (včetně kontroly aktivního účtu), místo aby se důvěřovalo pouze obsahu tokenu. Odhlášení okamžitě zneplatní refresh relaci na straně serveru, takže odcizený refresh token nepřežije odhlášení.

Hesla nejsou nikdy ukládána v prostém textu. Jsou hashována pomocí bcrypt s jedinečným salt pro každé heslo. Organizace, které preferují single sign-on, mohou využít OAuth přihlášení přes Microsoft a Google; v takovém případě není uloženo žádné heslo.

Vlastnictví e-mailové adresy je ověřováno prostřednictvím jednorázového časově omezeného ověřovacího odkazu, než je samoregistrovaný účet považován za ověřený, a opětovná zaslání ověřovacího e-mailu podléhají rate limiting, aby se zabránilo zneužití.

6.2 Řízení přístupu na základě rolí

Autorizace je vynucována prostřednictvím modelu čtyř rolí se vzrůstající úrovní oprávnění: interviewer, hiring manager, recruiter a administrator. Přístup k privilegovaným operacím je vynucován závislostmi na straně serveru, které kontrolují jak roli, tak stav ověření volajícího. Tyto kontroly rolí chrání výrazně přes sto různých API operací.

Role	Typické schopnosti
Interviewer	Provádí přiřazené pohovory; vidí pouze pohovory přiřazené jemu
Hiring manager	Spravuje nábory, které vlastní nebo jejichž je členem
Recruiter	Plná správa náborů a kandidátů v rámci organizace
Administrator	Nastavení organizace, billing, správa uživatelů a API klíčů

Nad rámec hrubých kontrol rolí platforma uplatňuje pravidla viditelnosti na úrovni dat. Hiring manager vidí pouze nábory, které vytvořil nebo jejichž je členem; interviewer vidí pouze pohovory přiřazené jemu. Oprávnění je tedy vynucováno jak na úrovni „jaká akce“, tak na úrovni „které záznamy“.

6.3 Izolace po organizacích

Platforma je multi-tenant a izolace tenantů je považována za bezpečnostní kontrolu první třídy. Každá autentizovaná identita nese identifikátor organizace a datové dotazy jsou omezeny na tuto organizaci. Když uživatel požádá o záznam patřící jiné organizaci, platforma vrátí odpověď „not found“, místo aby odhalila existenci záznamu. Interní databázové identifikátory nejsou nikdy vystaveny na rozhraní; API prezentuje zobrazované identifikátory a pro každý požadavek je znovu mapuje, čímž odstraňuje běžnou třídu útoků založených na enumeraci mezi tenanty.

Nejde pouze o konstrukční záměr. Jak je popsáno v oddílu 12, naše automatizovaná sada spouští rozsáhlou matici mezi organizacemi, která se pokouší dosáhnout na data jedné organizace pomocí přihlašovacích údajů jiné organizace, a potvrzuje, že každý takový pokus selže.

6.4 Programový přístup

Pro integrace mohou organizace v oprávněných plánech vydávat API klíče. Klíče používají rozpoznatelný prefix, nesou 128 bits entropie a jsou ukládány pouze jako hash; surový klíč je zobrazen jednou při vytvoření a už nikdy znovu. Každý klíč nese explicitní rozsah oprávnění (read, write nebo ATS integration), může být omezen na konkrétní zdrojové sítě, lze jej okamžitě odvolat a podléhá per-key rate limitům odvozeným od úrovně plánu organizace. Ověřování klíčů používá timing-safe porovnání, aby se zabránilo úniku informací prostřednictvím časování odpovědí.

7. Bezpečnost aplikace

Aplikace je psána tak, aby odstraňovala celé kategorie zranitelností, nikoli aby je opravovala případ od případu.

- **Injection.** Veškerý přístup k databázi probíhá přes object-relational mapper s parametrizovanými dotazy. Kódová báze neobsahuje žádné raw SQL formátované jako řetězce. To strukturálně eliminuje SQL injection.
- **Validace vstupu.** Každé tělo požadavku je validováno vůči striktnímu schématu dříve, než se dostane k business logice. Nadměrně velké payloady jsou odmítány a seznamové endpointy jsou stránkovány, aby bylo omezeno využití prostředků.
- **Kódování výstupu a cross-site scripting.** Text dodaný uživatelem i vygenerovaný AI je považován za nedůvěryhodný. Kde musí být obsah vykreslen jako HTML, prochází při zápisu sanitizací založenou na allow-listu a vyhrazená sada testů potvrzuje, že script tagy, event handlery a javascript URL jsou odstraňovány.
- **Mass assignment.** Aktualizační operace používají explicitní schémata, která vylučují privilegovaná pole, jako jsou role, organizace a zůstatek kreditů, takže klient nemůže eskalovat oprávnění odesláním dodatečných polí.
- **Rate limiting.** Endpointy pro autentizaci a endpointy náchylné ke zneužití jsou omezeny pomocí odolného limiteru založeného na databázi, který přežije restarty a funguje správně napříč více instancemi aplikace. Přihlášení, registrace, reset hesla a opětovné zaslání ověření mají každé vlastní limity. Rozlišování IP adres klienta je zpevněno proti spoofingu forwarding headers.
- **Webhooky.** Příchozí webhooky od poskytovatelů plateb a e-mailu jsou před zpracováním ověřovány vůči podpisům poskytovatele na raw request body.
- **Nahrávání souborů.** Uploady mají omezenou velikost, jsou validovány, ukládány pod generovanými identifikátory namísto názvů dodaných uživatelem a omezeny na úroveň požadavku i organizace.
- **Bezpečnostní hlavičky.** V produkci odpovědi nesou strict transport security, volby content-type a frame, referrer policy a restriktivní permissions policy a potlačují bannery serveru a frameworku.

8. Ochrana dat

8.1 Šifrování

Všechna data jsou šifrována v klidu pomocí AES-256 prostřednictvím platforem Azure pro šifrování úložiště a databáze. Veškerý síťový provoz je obsluhován výhradně přes HTTPS s použitím TLS 1.2 nebo vyšší; prostý HTTP je na všech vrstvách přesměrován na HTTPS. V produkci API a webový portál vysílají hlavičky strict transport security spolu se sadou hardening hlaviček a potlačují bannery verzí serveru a frameworku.

8.2 Správa tajných údajů

Tajné údaje aplikace jsou uloženy v centralizovaném vaultu pro tajné údaje s aktivovanou purge protection a devadesátidenním soft-delete oknem. Aplikace se autentizují k prostředkům Azure pomocí system-assigned managed identities namísto dlouhodobých klíčů; například privátní úložiště má shared access keys zcela vypnuté, takže přístup je možný pouze prostřednictvím přiřazení rolí založených na identitě, omezených na konkrétní prostředek. Přístupové politiky vaultu udělují aplikačním principálům pouze oprávnění ke čtení konkrétních tajných údajů, které potřebují, v souladu se zásadou minimálních oprávnění.

8.3 Rezidence dat

Všechna data zákazníků a kandidátů jsou ukládána a zpracovávána v rámci Evropské unie. Hosting aplikace, databáze, úložiště, cache a tajné údaje se nacházejí ve West Europe a AI zpracování běží v regionech EU. Poskytovatel AI nepoužívá zákaznická data k trénování svých modelů.

8.4 Život jednoho pohovoru

Nejjasnějším způsobem, jak porozumět kontrolám ochrany dat, je sledovat jeden pohovor od začátku do konce. Souhlas je získán a zaznamenán před jakýmkoli zpracováním. Upload je při přenosu šifrován. Přepis a analýza probíhají v datových centrech EU. Výsledky jsou zapisovány do šifrovaného úložiště. Každý záznam je poté řízen jedinými retenčními hodinami, které končí zaznamenaným kaskádovým smazáním. Práva kandidáta, jako je odvolání souhlasu, smazání, přístup nebo přenositelnost, mohou tento tok kdykoli přerušit.

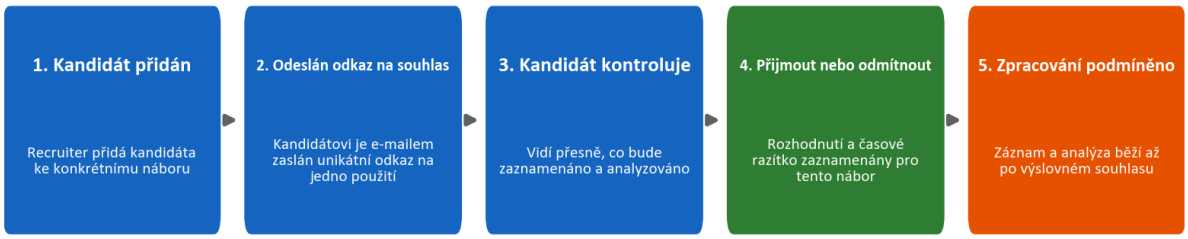
9. Soukromí by design a GDPR

Soukromí je zabudováno do datového modelu a workflow, nikoli pouze doplněno politikou.

9.1 Souhlas

Žádný pohovor není zaznamenán ani analyzován bez výslovného souhlasu kandidáta. Když je kandidát přidán do náboru, platforma zašle e-mailem jedinečný jednorázový odkaz pro udělení souhlasu. Kandidát si prostuduje, co se bude dít, a buď souhlasí, nebo odmítne. Stav souhlasu, včetně času odpovědi, je zaznamenán k danému konkrétnímu náboru, takže souhlas je vždy vztažen ke konkrétnímu náborovému procesu, nikoli udělen globálně.

Souhlas kandidáta: výslovný a zaznamenaný před jakýmkoli zpracováním

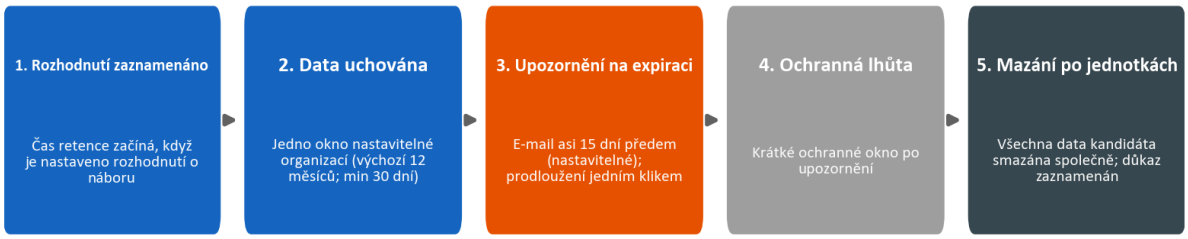


9.2 Retence a výmaz

Retence dat je konfigurovatelná pro každou organizaci, s výchozí hodnotou dvanáct měsíců a konfigurovatelným minimem třiceti dnů, a lze ji přepsat pro jednotlivého kandidáta. Pro data kandidáta existují jedny retenční hodiny, nikoli samostatný časovač pro každý artefakt. Hodiny se spouštějí při zaznamenání rozhodnutí o náboru. Před vypršením dat platforma odešle upozornění (ve výchozím nastavení přibližně patnáct dní předem) a nabídne prodloužení jedním kliknutím. Když jsou data smazána, jsou smazána jako jedna jednotka: záznam kandidáta, pohovory, přepisy, audio nahrávky, dokumenty a porovnání jsou odstraněny společně a smazání je zaznamenáno do auditního logu. Neexistují žádné částečné ani osiřelé zbytky.

Níže uvedený životní cyklus ukazuje tyto jedny hodiny a způsob, jak se sbíhají do jednoho kaskádového smazání s protokolovaným důkazem výmazu.

Retence dat: jedny hodiny na kandidáta, mazání po jednotkách



9.3 Práva subjektu údajů a sub-processors

Platforma podporuje práva subjektů údajů vyžadovaná podle GDPR, včetně přístupu, smazání, přenositelnosti, námitky a vysvětlení. Zpracování probíhá na základě dohody o zpracování osobních údajů, kterou zákazníci přijímají při registraci a která je verzována pro každou organizaci. Naši sub-processors a jejich role, všechny v rámci EU nebo při použití odpovídajících záruk, jsou

v této dohodě zveřejněni a zákazníci dostávají předběžné oznámení o jakékoli změně. Oddíl 17 obsahuje registr sub-processorů a mapování souladu po jednotlivých článcích.

10. Odpovědná AI a EU AI Act

Platforma spadá do kategorie high-risk podle EU AI Act, protože podporuje rozhodování v oblasti zaměstnání, a k této klasifikaci přistupujeme vážně.

Definující pravidlo produktu je, že **AI je podpora rozhodování, nikoli činitel rozhodnutí.** Systém nikdy automaticky nepřijme ani neodmítne kandidáta. Přepisuje řeč, strukturuje otázky a odpovědi, boduje odpovědi podle kritérií definovaných náborářem a připravuje návrh zpětné vazby, přičemž každý výstup před použitím zkontroluje člověk. Tím je člověk pevně udržen v rozhodovací smyčce.

Stejně důležité je i to, co AI nedělá. Nehodnotí osobnost, „kulturní soulad“, emoční stav, tón hlasu, přízvuk, pohlaví, věk, etnicitu, vzhled ani řeč těla. Bodování je ukotveno k důkazům z přepisu a ke kritériím definovaným náborářem a jména kandidátů jsou z hodnoticího vstupu vyloučena, aby se snížila zaujatost. Zveřejňujeme kartu transparentnosti, uživatelskou dokumentaci a prohlášení o shodě popisující systém, jeho omezení a ochranná opatření.

Kontrola odpovědné AI	Jak funguje
Člověk v rozhodovací smyčce	Každé skóre a každý kus zpětné vazby je před použitím zkontrolován náborářem
Žádná automatizovaná rozhodnutí	Systém nikdy kandidáta automaticky nepřijme ani automaticky neodmítne
Hodnocení založené na důkazech	Skóre odkazují na podpůrné důkazy z přepisu
Návrh proti bias	Jména jsou z hodnocení vyloučena; upřednostňuje se obsah před stylem
Omezení rozsahu	Osobnost, emoce, přízvuk a chráněné charakteristiky nejsou nikdy hodnoceny
Bezpečnost zpětné vazby kandidátovi	Soukromá zpětná vazba kandidátovi prochází bezpečnostním zábradlím generation-and-validation

Tato omezení nejsou uvedena pouze v dokumentaci; jsou zakódována ve vrstvě promptů AI a ověřována vyhrazeným programem AI-safety testů popsaným v oddílu 12.3.

11. Bezpečný životní cyklus vývoje

Bezpečnost je vynucována způsobem, jakým software vytváříme a vydáváme, nejen v běžícím systému.

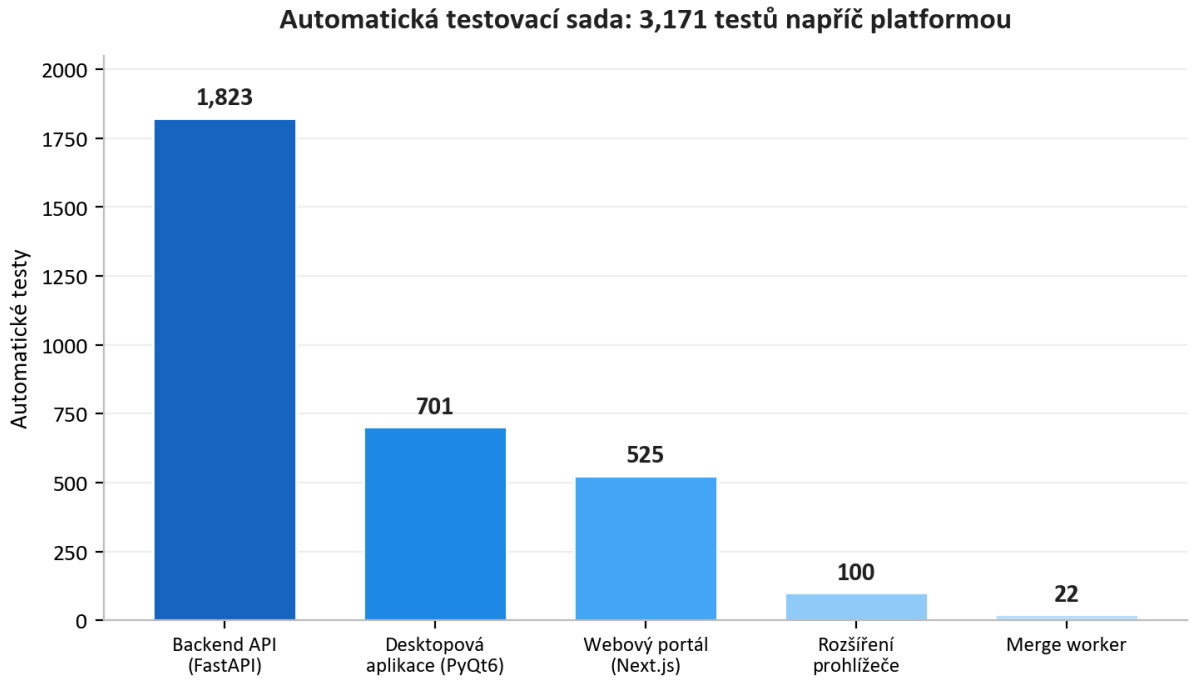
- **Oddělení prostředí.** Vývoj a produkce jsou plně odděleny, každé s vlastní infrastrukturou, účty úložiště, databází, tajnými údaji a subdoménami. Neexistuje žádný sdílený stav.
- **Infrastruktura jako kód.** Celé cloudové prostředí je definováno jako kód a kontrolováno jako kód, což činí bezpečnostní nastavení auditovatelným a reprodukovatelným. Posuzovatel může přesně zjistit, které porty jsou otevřené, které prostředky jsou privátní a které identity mají jaká oprávnění.
- **Připnutá a řízená nasazení.** Každý krok v CI/CD pipeline je připnut k přesné neměnné verzi. Produkční nasazení jsou založena na tagech, probíhají pouze prostřednictvím chráněné produkční pipeline a jsou podmíněna povinným schválením. Automatizovaná sada testů funguje jako uvolňovací brána: pokud testy selžou, nasazení nelze vydat.
- **Hygiena závislostí.** Automatizované sledování závislostí navrhuje aktualizace každý týden napříč backendem, desktopem, webem, infrastrukturou a definicemi pipeline a audity závislostí jsou součástí našich periodických bezpečnostních kontrol.
- **Podepsané artefakty.** Desktopové instalátory jsou code-signed, takže zákazníci mohou ověřit, že software, který instalují, skutečně pochází od nás.
- **Disciplína pro tajné údaje.** Tajné údaje jsou uloženy ve vaultu a v chráněných tajných údajích pipeline, nikdy ne ve zdrojovém kódu.

12. Průběžné bezpečnostní testování

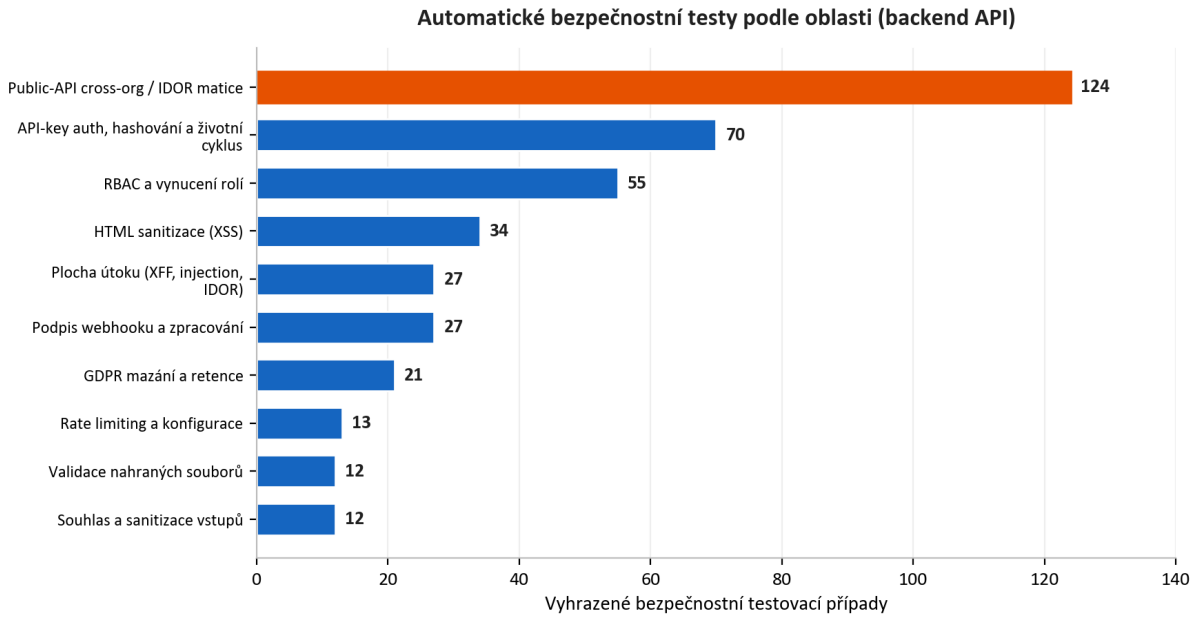
To je jádro našeho příběhu o zajištění a část, kterou většina dodavatelů nedokáže ukázat. Bezpečnost považujeme za něco, co se má průběžně měřit pomocí spustitelných kontrol, nikoli za něco, co se jednou prohlásí.

12.1 Automatizovaná sada testů

Platforma je pokryta **3,171 automatizovanými testy**, které zahrnují backend API, desktopovou aplikaci, webový portál, rozšíření prohlížeče a workera pro slučování audia.



Nejde pouze o funkční testy. Významná vyhrazená bezpečnostní sada ověřuje kontroly popsané dříve v tomto dokumentu. Níže uvedený graf rozděluje bezpečnostně specifické testy v backend API podle domény.



Mimo mnoha dalších tato sada zahrnuje rozsáhlou matici veřejného API, která spouští každý endpoint jako legitimní uživatel, jako vlastní API klíč organizace a jako API klíč konkurenční organizace a potvrzuje, že každý pokus mezi organizacemi je blokován. Obsahuje desítky adversariálních testů útočné plochy pro spoofing forwarding headers, header injection a únik identifikátorů, cílenou HTML-sanitizační sadu pro cross-site scripting, testy vynucení rolí pro celý model rolí a testy prokazující, že data kandidáta jsou skutečně smazána jako jedna jednotka. Protože se tyto testy spouštějí jako release gate, regrese oslabující kteroukoli z těchto kontrol by zastavila vydání místo toho, aby se dostala k zákazníkům.

12.2 Živé penetrační testování

Automatizované unit testy prokazují, že kontroly fungují správně izolovaně. Abychom prokázali, že obstojí dohromady v reálném nasazení, udržujeme opakovatelnou metodologii penetračního testování, která spouští skutečné útočné skripty proti živému prostředí. Je organizována do šesti fází:

Fáze	Zaměření	Příklady toho, co je ověřováno
1. Statická analýza	Zdrojový kód	Tajné údaje, vzory injection, nebezpečné funkce, chybějící auth, nebezpečné HTML
2. Kontrola architektury	Infrastruktura	Privátní endpointy, segmentace, TLS, konfigurace tajných údajů
3. Analýza vektorů útoku	Source control a cloud	Ochrana větví, rozsah identit, veřejné vystavení
4. Živé penetrační testování	Běžící prostředí	Průzkum bez autentizace, přístup mezi organizacemi, injection, manipulace s tokeny, SSRF, bursty proti rate limitům
5. Podnikové skórování	Vyspělost	Šestnáct bezpečnostních kategorií hodnocených vůči podnikovému základu
6. Závislosti a dodavatelský řetězec	Riziko třetích stran	Audit CVE závislostí, připnuté akce pipeline, integrita lock souborů

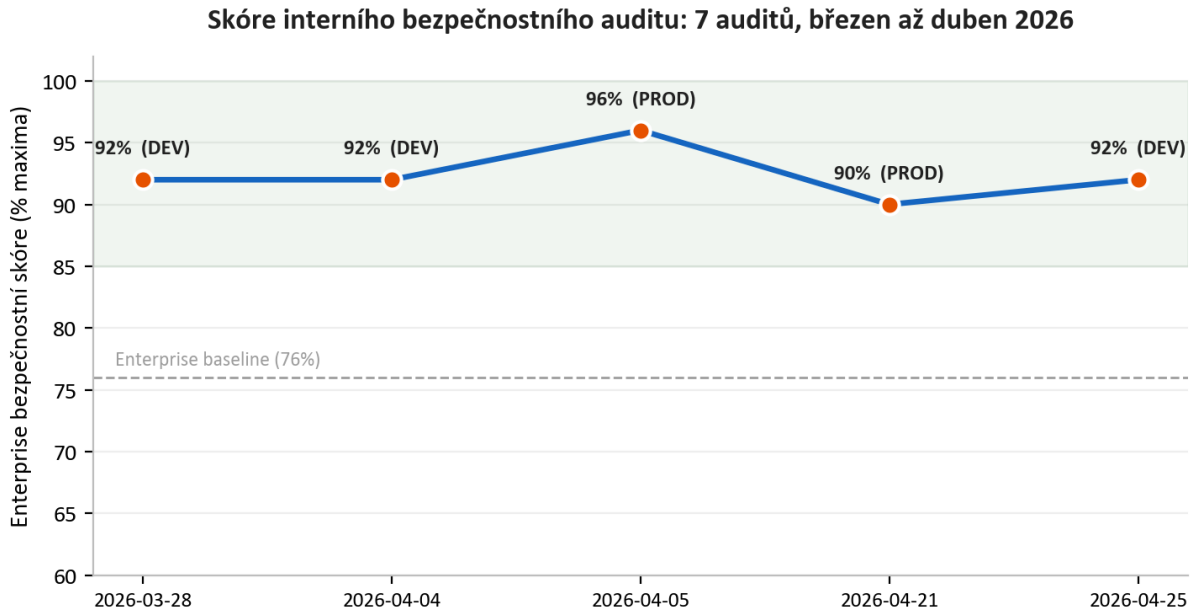
Fáze 4 představuje skutečné adversariální testování nasazeného systému, nikoli checklist. Zkoumá chráněné endpointy bez přihlašovacích údajů a potvrzuje, že odmítají přístup; registruje dvě organizace a pokouší se dosáhnout na záznamy jedné organizace pomocí účtu druhé; vkládá payloady cross-site-scripting a server-side-template a potvrzuje, že jsou zneškodněny; manipuluje s autentizačními tokeny a potvrzuje jejich odmítnutí; pokouší se o server-side request forgery proti cloud metadata endpointům; a zatěžuje autentizační endpointy dávkami požadavků, aby potvrdila, že se rate limiting skutečně aktivuje v živém prostředí, nejen teoreticky.

12.3 Bezpečnostní testování zpětné vazby kandidátům

Protože platforma může generovat soukromou rozvojovou zpětnou vazbu pro kandidáty, provozujeme proti této funkci samostatný adversariální bezpečnostní program. Záměrně systému předkládá tvrdé a nepřátelské poznámky náborářů a potvrzuje, že výstup určený kandidátovi nikdy neobsahuje vulgarity, nikdy neodhaluje ani nepřipisuje identitu náboráře nebo jeho soukromý názor a nikdy nepoužívá hodnoticí nálepky osobnosti. To chrání jak kandidáta, který má dostávat konstruktivní a respektující zpětnou vazbu, tak zákazníka, jehož interní názory by se nikdy neměly dostat navenek.

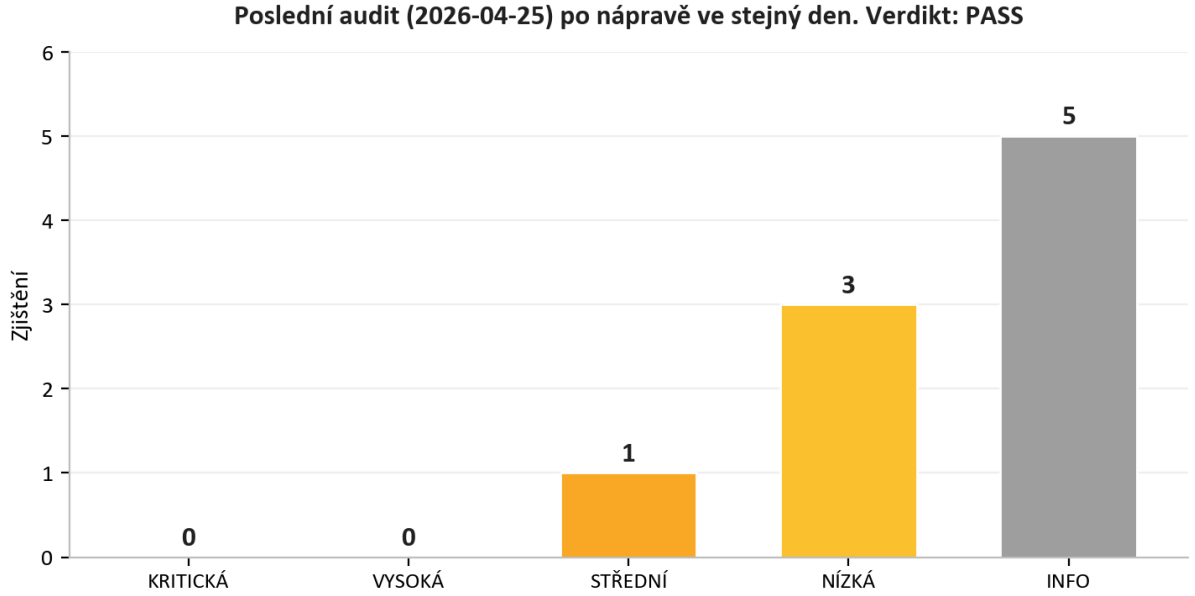
13. Výsledky bezpečnostních auditů

Provádíme pravidelné bezpečnostní audity s použitím strukturované, opakovatelné metodologie penetračního testování a každý z nich zpracováváme do datované zprávy se zjištěními hodnocenými podle závažnosti, důkazy a nápravou. Jde o interní audity prováděné naším vlastním bezpečnostním procesem; formální certifikace stejných kontrol třetí stranou je součástí naší roadmapy. Mezi koncem března a koncem dubna 2026 jsme dokončili **seven such audits** napříč vývojem a produkcí.



Výsledek, který je pro potenciálního zákazníka nejdůležitější, je konzistence: **across all seven audits there were zero critical findings.** Ve vzácných případech, kdy se objevila závažnější otázka, byla rychle napravena, často ještě tentýž den, a znovu ověřena. Bodovací rubrika byla v tomto období záměrně zpřísněna (maximální možné skóre bylo zvýšeno, jak jsme přidávali další hodnocené kategorie), což je důvod, proč linie normalizovaného skóre zůstává vysoko, i když se laťka posouvala výše.

Náš nejnovější audit z 25 April 2026 ilustruje, jak proces funguje v praxi. Byly identifikovány dvě závažnější otázky, obě byly tentýž den opraveny a znovu ověřeny a audit byl uzavřen verdiktem **PASS** bez zbývajících problémů připravených ke zneužití v rámci aktuálního threat modelu.



Audit	Prostředí	Critical	Verdikt
2026-03-28	Vývoj	0	Připraveno pro produkci
2026-04-04	Vývoj	0	Připraveno pro enterprise
2026-04-05	Produkce	0	Připraveno pro enterprise
2026-04-20	Vývoj	0	Připraveno pro produkci, poznámky
2026-04-20	Vývoj	0	Pass with notes
2026-04-21	Produkce	0	Bezpečné, žádná zneužitelná zjištění
2026-04-25	Vývoj	0	Pass

Vzorec napříč těmito audity je nejpoctivějším důkazem, který můžeme nabídnout: problémy jsou nalézány, protože je důsledně hledáme, a jsou rychle uzavírány, protože proces je navržen tak, aby je uzavíral. Dodavatel, který nikdy nevykazuje žádné zjištění, je obvykle dodavatel, který je nehledá.

---

14. Provozní odolnost a sdílená odpovědnost

14.1 Monitoring a logování

Telemetrie aplikace a platformy proudí do centralizovaného pracovního prostoru log analytics a služby pro monitoring aplikací, což nám poskytuje přehled o dostupnosti a chování. Citlivé akce, jako je mazání dat, přijetí právních ujednání a AI invokace, jsou zaznamenávány do vyhrazených auditních tabulek, takže existuje trvalý záznam o tom, kdo co udělal s důležitými daty.

14.2 Zálohování a obnova

Spravovaná databáze uchovává automatizované zálohy a privátní úložiště je chráněno soft-delete retencí jak pro blobs, tak pro kontejnery, takže náhodné nebo škodlivé smazání lze obnovit v rámci retenčního okna. Kritická infrastruktura je opatřena deletion locky, aby se zabránilo náhodnému odstranění produkčních prostředků.

14.3 Přehled sdílené odpovědnosti

Oblast	AI Interview Analyzer	Zákazník
Infrastruktura, síť, patching	Ano	-
Bezpečnost aplikace a AI pipeline	Ano	-
Šifrování, tajné údaje, rezidence dat	Ano	-
Správa uživatelů a rolí	Poskytuje kontroly	Spravuje uživatele a role
Konfigurace retenční politiky	Poskytuje kontroly	Nastavuje retenční okno
Souhlas kandidáta	Poskytuje workflow	Zajišťuje jeho používání
Silné koncové přihlašovací údaje a SSO	Podporuje SSO a politiku	Vynucuje interní politiku

15. Threat model a mapování na OWASP

Navrhujeme obranu proti konkrétní sadě protivníků: externí útočník bez přihlašovacích údajů, zvědavý nebo škodlivý autentizovaný uživatel jedné organizace, který se snaží dosáhnout na data jiné organizace, kompromitovaná závislost a chyba insidera. Níže uvedená tabulka mapuje široce používané kategorie rizik OWASP Top 10 na konkrétní kontroly, které je v této platformě řeší, přičemž každá z nich je ověřována testováním popsaným v oddílu 12.

Riziko OWASP	Jak jej platforma zmírňuje
Broken access control	Řízení přístupu podle rolí na každém privilegovaném endpointu; scope po organizacích; „not found“ při přístupu mezi organizacemi; remapping identifikátorů; testovací matice mezi organizacemi
Cryptographic failures	TLS 1.2+ při přenosu; AES-256 v klidu; hashování hesel bcrypt; tajné údaje ve spravovaném vaultu
Injection	Pouze ORM parametrizované dotazy; striktní validace schémat; HTML sanitizace při zápisu
Insecure design	Vrstvená hloubková obrana; threat modeling a kontrola architektury v každém auditu
Security misconfiguration	Infrastruktura jako kód; síťové skupiny typu default-deny; bezpečnostní hlavičky; vypnuté shared storage keys; API schema není v produkci vystavena
Vulnerable components	Týdenní automatizované sledování závislostí; CVE audity závislostí v periodických kontrolách
Identification and authentication failures	Krátkodobé tokeny; přihlášení s rate limiting; ověřování e-mailu; podpora SSO; žádná hesla v prostém textu
Software and data integrity failures	Připnuté neměnné kroky pipeline; podepsané desktopové instalátory; ověřování podpisu webhooků; produkční deploye řízené tagy
Security logging and monitoring failures	Centralizovaná telemetrie; vyhrazené auditní tabulky pro citlivé akce
Server-side request forgery	Odchozí volání omezena na důvěryhodné endpointy; SSRF testy v rámci penetračního testovacího rámce

Toto mapování je páteří našeho argumentu o zajištění: pro každou známou třídu útoku existuje pojmenovaná kontrola a pro každou pojmenovanou kontrolu existuje test.

16. Správa zranitelností a odpovědné oznamování

Bezpečnost není nikdy hotová, proto provozujeme průběžnou smyčku objevování a nápravy.

- **Objevování.** Zranitelnosti jsou identifikovány ze čtyř zdrojů: automatizované sady testů, opakovaných auditů penetračního testování, automatizovaného monitoringu závislostí a hlášení od zákazníků nebo výzkumníků.
- **Triage.** Každému zjištění je přiřazena závažnost (critical, high, medium, low nebo informational) spolu s důkazy a vlastníkem nápravy, přesně jak je zaznamenáno v našich auditních zprávách.
- **Cíle nápravy.** Zjištění critical a high jsou prioritizována k okamžité nápravě; v historii našich auditů byla zjištění vyšší závažnosti typicky vyřešena a znovu ověřena ještě tentýž den. Zjištění medium a nižší jsou plánována do běžného cyklu údržby.
- **Ověření.** Opravy jsou znovu testovány a tam, kde je to relevantní, je proti nasazenému prostředí provedena živá kontrola, aby se potvrdilo, že je problém skutečně uzavřen, nikoli pouze uzavřen v kódu.
- **Oznamování.** Bezpečnostní obavy nám lze nahlásit přímo. Přijetí hlášení potvrdíme, prošetříme jej a budeme oznamovatele informovat až do vyřešení.

17. Mapování souladu

17.1 GDPR

Oblast GDPR	Implementace v platformě
Právní základ (Art. 6)	Výslovný souhlas kandidáta získaný před zpracováním
Minimalizace dat a omezení uložení (Art. 5)	Zpracovávají se pouze data relevantní pro pohovor; konfigurovatelná retence s automatickým mazáním
Právo na výmaz (Art. 17)	Smazání všech dat kandidáta jako jedné jednotky s protokolovaným důkazem výmazu
Práva subjektu údajů (Art. 15 to 20)	Podporovány jsou přístup, smazání, přenositelnost a námitka
Povinnosti zpracovatele (Art. 28)	Dohoda o zpracování osobních údajů přijatá při registraci a verzovaná pro každou organizaci
Bezpečnost zpracování (Art. 32)	Šifrování, řízení přístupu, izolace a průběžné testování, jak je popsáno v tomto dokumentu
Transparentnost sub-processorů	Zveřejněno v dohodě o zpracování osobních údajů s předběžným oznámením změn

17.2 EU AI Act

Platforma je považována za high-risk AI systém podporující rozhodování v oblasti zaměstnání a udržujeme dokumentaci v souladu s regulací, včetně karty transparentnosti, uživatelské dokumentace a prohlášení o shodě. Klíčová ochranná opatření, lidský dohled, transparentnost, hodnocení založené na důkazech a přísná omezení rozsahu toho, co AI hodnotí, jsou popsána v oddílu 10. Jak postupuje implementační harmonogram regulace, nadále rozvíjíme naši formální dokumentaci shody.

17.3 Hostingové certifikace

Platforma běží plně na Microsoft Azure, jehož datová centra mají nezávislé certifikace včetně ISO 27001 a SOC 2. Tyto certifikace pokrývají fyzické a platformní vrstvy pod naší aplikací; kontroly na aplikační vrstvě jsou popsány v celém tomto dokumentu.

17.4 Registr sub-processorů

Sub-processor	Účel	Region
Microsoft Azure	Hosting, AI a speech processing, úložiště, transakční e-mail	EU (West Europe, Sweden Central)
Stripe	Zpracování předplatného a plateb	EU (Ireland)
Fakturownia	Fakturace	EU (Poland)
ATS connector (optional)	Integrace se systémem pro správu uchazečů, povoleno pouze na vyžádání	EU

18. Bezpečnostní roadmapa

Bezpečnost chápeme jako program neustálého zlepšování. Mezi aktuální iniciativy v naší roadmapě patří posílení možností multi-factor authentication pro administrativní účty, rozšíření centralizovaného auditního logování přístupu k datům, pokračující zpřísňování aktuálnosti závislostí v pravidelném rytmu a postup k formální certifikaci kontrol popsaných v tomto dokumentu třetí stranou. Žádná z těchto položek nepředstavuje mezeru, která by dnes vystavovala zákaznická data; každá je vylepšením již vrstveného bezpečnostního postoje.

19. Shrnutí

AI Interview Analyzer chrání data kandidátů a zákazníků prostřednictvím vrstvené architektury: sítě privátní ve výchozím stavu bez veřejných datových služeb, silné identity a izolace po organizacích, aplikačního kódu, který konstrukčně odstraňuje celé třídy zranitelností, šifrování a rezidence dat v EU a kontrol soukromí zabudovaných do datového modelu. To, co platformu odlišuje, jsou důkazy za těmito tvrzeními. Díky 3,171 automatizovaným testům, opakovatelné metodologii živého penetračního testování, vyhrazenému programu AI-safety a historii sedmi interních bezpečnostních auditů s zero critical findings můžeme ukázat, nejen tvrdit, že je platforma bezpečná.

Příloha A: Katalog bezpečnostních kontrol

Kondenzovaný přehled primárních kontrol a důkazů, které každou z nich podporují.

Kontrola	Mechanismus	Důkaz
Šifrování přenosu	Pouze HTTPS, TLS 1.2+, přesměrování HTTP	Infrastruktura jako kód; audit architektury
Šifrování v klidu	Platformní šifrování AES-256 na úložišti a databázi	Konfigurace platformy; audit architektury
Ochrana hesel	bcrypt se salt pro každé heslo	Source control; autentizační testy
Správa relací	30-minute podepsané tokeny, odvolatelný refresh na straně serveru	Source control; autentizační testy
Autorizace	Řízení přístupu se čtyřmi rolemi na privilegovaných endpointech	Sada testů vynucení rolí
Izolace tenantů	Scope dotazů po organizacích; 404 při přístupu mezi organizacemi	Testovací matice mezi organizacemi
Bezpečnost API klíčů	Uložení jako hash, rozsahy oprávnění, per-key rate limity	Sada testů API klíčů
Ochrana proti injection	Pouze ORM parametrizované dotazy	Statická analýza; injection testy
Ochrana proti cross-site scripting	HTML sanitizace při zápisu	HTML-sanitization test suite
Rate limiting	Odolný limiter založený na databázi na auth endpointech	Rate-limit testy; živé burst kontroly
Integrita webhooků	Ověřování podpisu poskytovatele na raw body	Sada testů webhooků
Správa tajných údajů	Managed vault, purge protection, managed identity	Infrastruktura jako kód; audit architektury
Izolace sítě	Privátní endpointy; segmentace typu default-deny	Infrastruktura jako kód; audit architektury
Mazání dat	Kaskádové mazání jako jedné jednotky s auditním logem	GDPR deletion test suite
Dodavatelský řetězec	Připnuté kroky pipeline; týdenní monitoring závislostí	Konfigurace pipeline; audit závislostí

Příloha B: Často kladené otázky pro bezpečnostní posuzovatele

Kde jsou naše data uložena? Výhradně v Evropské unii, na Microsoft Azure, ve West Europe s AI zpracováním v regionech EU. Data kandidátů nikdy neopouštějí EU.

Používají se naše data k trénování AI modelů? Ne. Poskytovatel AI nepoužívá zákaznická data pro trénování.

Je databáze dosažitelná z internetu? Ne. Veřejný síťový přístup je zakázán a databáze je dosažitelná pouze prostřednictvím privátního endpointu uvnitř virtuální sítě.

Může jeden zákazník vidět data jiného zákazníka? Ne. Každý dotaz je omezen na organizaci volajícího, přístup mezi organizacemi vrací „not found“ a automatizovaná matice tuto izolaci průběžně testuje.

Jak jsou ukládána hesla? Hashována pomocí bcrypt a jedinečného salt pro každé heslo. Je podporováno single sign-on s Microsoft a Google, v takovém případě není ukládáno žádné heslo.

Podporujete single sign-on? Ano, prostřednictvím Microsoft a Google OAuth.

Jak dlouho jsou platné access tokeny? Třicet minut, spárované s odvolatelnou refresh relací na straně serveru, která je při odhlášení zneplatněna.

Jak je zpracováván souhlas kandidáta? Každý kandidát obdrží jedinečný jednorázový odkaz pro souhlas a musí jej přijmout před jakýmkoli záznamem nebo analýzou. Souhlas je zaznamenán ke konkrétnímu náborovému procesu.

Jak jsou data mazána? Jako jedna jednotka zahrnující záznam kandidáta, pohovory, přepisy, audio, dokumenty a porovnání, podle konfigurovatelného retenčního plánu, s protokolovaným důkazem výmazu. Kandidáti mohou také požádat o smazání přímo.

Máte dohodu o zpracování osobních údajů? Ano, je přijímána při registraci a verzována pro každou organizaci, včetně registru sub-processorů.

Provádí AI rozhodnutí o náboru? Ne. Poskytuje pouze podporu rozhodování; člověk kontroluje každý výstup a činí všechna rozhodnutí.

Jak prokazujete svá bezpečnostní tvrzení? Prostřednictvím 3,171 automatizovaných testů včetně vyhrazené bezpečnostní sady, opakovatelné šestifázové metodologie penetračního testování provozované proti živým prostředím, programu AI-safety testů a pravidelných písemných auditních zpráv.

Co se stane, když naleznete zranitelnost? Je jí přiřazena závažnost s důkazy a vlastníkem, je napravena podle prioritního harmonogramu, znovu ověřena včetně živých kontrol tam, kde je to relevantní, a zaznamenána v auditní zprávě.

Můžeme provést vlastní penetrační test? Bezpečnostní hodnocení lze sjednat prostřednictvím vašeho account representative při odpovídajícím rozsahu a harmonogramu.

Příloha C: Glosář

Termín	Význam
AES-256	Silný standard symetrického šifrování používaný k ochraně dat v klidu
bcrypt	Účelově vytvořená funkce pro hashování hesel se salt pro každé heslo
Managed identity	Identita vydaná platformou, která službě umožňuje autentizaci bez uložených klíčů
Private endpoint	Privátní síťová adresa, která drží cloudovou službu mimo veřejný internet
Network security group	Sada pravidel povolení a zákazu, která filtrují síťový provoz do subnetu
RBAC	Řízení přístupu na základě rolí, udělující oprávnění podle role uživatele
IDOR	Insecure direct object reference, chyba řízení přístupu, proti níž se platforma brání
SSRF	Server-side request forgery, třída útoků testovaná v našich penetračních testech
Web application firewall	Edge kontrola, která filtruje škodlivý webový provoz
Data processing agreement	Smlouva upravující, jak zpracovatel nakládá s osobními údaji jménem správce

Příloha D: Kontakt a správa dokumentu

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Pro bezpečnostní posouzení, kopii naší dohody o zpracování osobních údajů nebo naši dokumentaci shody s EU AI Act kontaktujte prosím svého account representative.

Tento dokument popisuje bezpečnostní nastavení služby AI Interview Analyzer k datu generování uvedenému v zápatí. Je poskytován pro účely hodnocení a netvoří součást žádné smlouvy. Konkrétní smluvní bezpečnostní závazky jsou uvedeny v příslušné smlouvě a dohodě o zpracování osobních údajů.