Varnostni dokument

Enterprise Security Overview - AI Interview Analyzer

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

Contents

Varnostni dokument

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

Ciljna publika: ekipe za varnost v podjetjih, IT in nabavo

Klasifikacija: Javno

1. Izvršni povzetek

AI Interview Analyzer je poslovna platforma za zaposlovanje, ki z izrecnim soglasjem kandidata snema intervjuje, jih prepisuje in strukturira ter pripravlja na dokazih temelječo podporo pri ocenjevanju za kadrovike. Ker platforma obdeluje osebne podatke kandidatov in podpira procese zaposlovanja, sta varnost in zasebnost obravnavani kot primarni omejitvi zasnove, ne kot funkcionalnosti, dodane naknadno.

Ta dokument v konkretnih in preverljivih izrazih opisuje, kako varujemo podatke strank in kandidatov. Napisana je za osebe, ki pregledujejo ponudnike: varnostne inženirje, IT skrbnike, pooblaščence za varstvo podatkov in nabavo. Vsaka številka v tem dokumentu izhaja neposredno iz naših lastnih inženirskih sistemov in ne iz trženjskih gradiv.

Osrednje sporočilo je preprosto: **ne trdimo zgolj, da je platforma varna, temveč to neprekinjeno preverjamo.** Naša kodna baza vsebuje **3,171 avtomatiziranih testov**, vključno z namenskim varnostnim sklopom, ki preverja avtentikacijo, avtorizacijo, izolacijo med organizacijami, zaščito pred injekcijami in brisanje podatkov. Poleg tega izvajamo ponovljiv okvir za penetracijsko testiranje nad živimi namestitvami in pripravljamo pisna revizijska poročila. V sedmih internih varnostnih revizijah v marcu in aprilu 2026 smo zabeležili **zero critical findings**, pri čemer se je naša najnovejša revizija zaključila z oceno **PASS**. (Formalna certificiranja teh kontrol s strani tretjih oseb so na našem razvojnem načrtu; glejte Oddelek 18.)

Varnostna značilnost	Povzetek
Gostovanje	Microsoft Azure, samo regije EU
Omrežni model	Zasebne končne točke, omrežna segmentacija s privzeto prepovedjo, brez javne baze podatkov
Šifriranje	AES-256 v mirovanju, TLS 1.2 ali višje med prenosom
Identiteta	Kratkoživi podpisani žetoni, bcrypt zgoščevanje gesel, podpora za SSO
Nadzor dostopa	RBAC s strogo izolacijo po organizacijah
Skrivnosti	Centraliziran trezor skrivnosti z dostopom prek upravljane identitete
Zasebnost	Izrecno soglasje, nastavljiva hramba, brisanje kot enotna celota
Odgovorna raba AI	Samo podpora pri odločanju, človek je vedno v zanki
Zagotovila	3,171 avtomatiziranih testov ter ponavljajoče se penetracijske teste in revizije

1.1 Kako brati ta dokument

Oddelki 3 do 11 opisujejo kontrole, ki varujejo podatke: arhitekturo, omrežje, identiteto, aplikacijo, zaščito podatkov, zasebnost in varen razvojni življenjski cikel. Oddelka 12 in 13 pokrivata naš značilen program neprekinjenega testiranja in zgodovino revizij. Oddelki 14 do 17 obravnavajo delovanje, modeliranje groženj, upravljanje ranljivosti in preslikavo skladnosti. Priloge vsebujejo katalog kontrol, pogosta vprašanja za presojevalce in slovar, ki ga lahko varnostna ekipa neposredno uporabi med presojo.

2. Obseg dokumenta in pristop

2.1 Kaj ta dokument zajema

Ta dokument zajema varnostno arhitekturo in prakse storitve AI Interview Analyzer: gostovalno okolje, zasnovo omrežja, upravljanje identitete in dostopa, kontrole na ravni aplikacije, zaščito podatkov, usklajenost z zasebnostjo in regulativo, varen razvojni življenjski cikel ter naš program neprekinjenega varnostnega testiranja.

2.2 Kaj ga naredi preverljivega

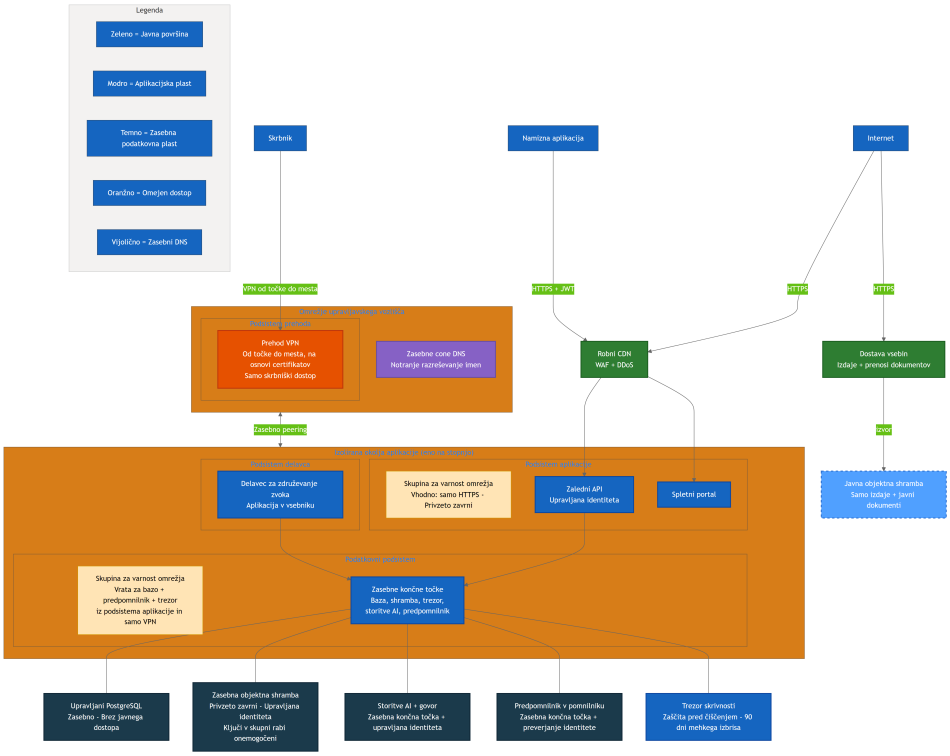
Varnostne trditve ponudnikov je enostavno napisati in težko jim je zaupati. Zato smo vsako glavno trditev v tem dokumentu povezali z nečim konkretnim in merljivim znotraj naših inženirskih sistemov: s kontrolo, implementirano v kodi, s testom, ki dokazuje, da kontrola deluje, z definicijo infrastrukture, ki jo uveljavlja, ali z revizijskim poročilom, ki beleži dokumentirano preverjanje. Kjer je kontrola del našega prihodnjega razvojnega načrta in še ni uvedena danes, to izrecno navedemo. Raje trdimo manj in smo vredni zaupanja, kot da trdimo preveč in smo pri tem ujeti.

2.3 Deljena odgovornost

Platforma se zagotavlja kot programska oprema kot storitev. Mi upravljamo infrastrukturo, aplikacijo, AI cevovod in obdelavo podatkov. Stranka je odgovorna za upravljanje lastnih uporabniških računov in vlog, konfiguracijo obdobij hrambe podatkov v skladu s svojimi internimi politikami ter zagotavljanje, da je soglasje kandidata pridobljeno prek poteka za soglasje, ki ga zagotavlja platforma. Oddelek 14 to razdelitev podrobneje opisuje.

3. Pregled varnostne arhitekture

Platforma je zgrajena kot manjše število sodelujočih storitev in ne kot en sam monolit. Namizna aplikacija in spletni portal delujeta kot odjemalca. Osrednji backend API upravlja vso obstojnost podatkov, avtentikacijo, obračunavanje, AI cevovod, soglasja, e-pošto, delo z datotekami in nadzorne plošče. Delovni proces za združevanje zvoka obdeluje posnetke asinhrono. Vsa občutljiva stanja so za backend API; odjemalci nikoli ne komunicirajo neposredno z bazo podatkov, shrambo ali AI storitvami.



Zgornji diagram prikazuje produkcijsko topologijo z namerno posplošenimi imeni virov. V njem so vidna tri načela:

- **Brez neposredne izpostavljenosti podatkovnih storitev.** Baza podatkov, zasebna objektna shramba, AI storitve in predpomnilnik imajo onemogočen javni omrežni dostop in so dosegljivi le prek zasebnih končnih točk znotraj izoliranega virtualnega omrežja. Trezor skrivnosti aplikacija dosega prek zasebne končne točke, dodatno pa je zaščiten z avtentikacijo platformne identitete in politikami dostopa z najmanjšimi privilegiji, zato vsak dostop zahteva veljavno, avtorizirano identiteto ne glede na omrežno pot.
- **Ločena javna površina.** Edina javna objektna shramba vsebuje prenose izdaj in javne dokumente. Nikoli ne vsebuje podatkov kandidatov. Promet aplikacije, obrnjen proti strankam, poteka prek robne plasti, ki zagotavlja WAF, zaščito pred DDoS in dostavo vsebin.
- **Administrativni dostop je nadzorovan.** Operaterji dosegajo notranje vire samo prek VPN od točke do mesta na osnovi certifikatov v upravljavsko omrežno vozlišče, ne prek javnega interneta.

Vsaka faza namestitve (razvoj in produkcija) je popolnoma izolirano okolje z lastnim omrežjem, računi za shrambo, bazo podatkov in skrivnostmi. Produkcijski podatki strank nikoli niso prisotni v nižjih okoljih. Skupno upravljavsko vozlišče vsebuje le VPN prehod in zasebni DNS, ki je zasebno povezan z vsakim okoljem.

---

4. Večplastna obramba

Nobeni posamezni kontroli ne zaupamo, da bo ustavila vsak napad. Platforma plasti neodvisne kontrole tako, da odpoved katere koli plasti ne razkrije podatkov. Spodnje plasti so vsaka posebej implementirane in, kot je opisano v Oddelku 12, posamezno testirane.

Večplastni varnostni model: neodvisni nadzori na vsaki ravni

Plast	Reprezentativne kontrole
Omrežni rob	Samo TLS prenos, robni WAF in zaščita pred DDoS, zasebne končne točke, segmentacija s privzeto prepovedjo
Identiteta in dostop	Kratkoživi podpisani žetoni, bcrypt zgoščevanje, RBAC, izolacija po organizacijah
Aplikacija	Validacija sheme za vse vnose, dostop do podatkov samo prek ORM, kodiranje izhodov, omejevanje hitrosti
Zaščita podatkov	Šifriranje v mirovanju, trezor skrivnosti z upravljano identiteto, hramba podatkov v EU, obdelava pogojena s soglasjem
Upravljanje in zasebnost	Nastavljiva hramba, brisanje kot enotna celota, AI s človekom v zanki, revizijsko beleženje
Neprekinjena zagotovila	Avtomatiziran testni sklop, ponovljivi penetracijski testi, ponavljajoče se interne varnostne revizije

Preostanek tega dokumenta postopoma obravnava vsako plast, nato pa opisuje, kako neprekinjeno dokazujemo, da plasti držijo.

5. Omrežna varnost

5.1 Privzeto zasebno

Podatkovna plast je zasebna že po zasnovi. Upravljana baza PostgreSQL ima onemogočen javni omrežni dostop in je dosegljiva le prek zasebne končne točke. Zasebna objektna shramba je konfigurirana tako, da privzeto zavrne omrežni dostop, v celoti onemogoča ključe skupnega dostopa in je dosegljiva samo prek upravljane identitete iz podomrežja aplikacije. Predpomnilnik, AI storitve in trezor skrivnosti so prav tako doseženi prek zasebnih končnih točk z zasebnim DNS razreševanjem.

V praksi to pomeni, da ne obstaja javni connection string do baze podatkov in ni javnega URL-ja shrambe za zvočne posnetke kandidatov: javni omrežni dostop do baze podatkov in zasebne shrambe je izrecno onemogočen. Trezor skrivnosti aplikacija dosega prek zasebne končne točke in je zaščiten z avtentikacijo platformne identitete ter politikami dostopa z najmanjšimi privilegiji, pri čemer imajo identitete aplikacije dodeljen samo bralni dostop le do tistih skrivnosti, ki jih potrebujejo, zato skrivnosti ni mogoče pridobiti brez veljavne, avtorizirane identitete. Napadalna površina, ki se je zunanji nasprotnik sploh lahko dotakne, je omejena na HTTPS končne točke aplikacije za robno plastjo.

5.2 Omrežna segmentacija

Vsako okolje je razdeljeno na ločena podomrežja za aplikacijsko plast, podatkovno plast in asinhronega delavca. Vsako podomrežje upravlja NSG, katerega zadnje pravilo zavrne ves dohodni promet. Podomrežje aplikacije sprejema le dohodni HTTPS. Podomrežje podatkov sprejema le specifična vrata baze podatkov, predpomnilnika in trezorja, in to samo iz podomrežja aplikacije ali administrativnega VPN. To pomeni, da tudi napadalec, ki bi nekako dosegel aplikacijsko plast, ne more prosto prehajati v podatkovno plast; dovoljene so le poti, ki jih aplikacija legitimno uporablja.

5.3 Rob

Javni promet aplikacije je postavljen za robno plastjo, ki zagotavlja WAF, zaščito pred DDoS in CDN. Prenosi izdaj in dokumentov se strežejo iz namenskega javnega računa za shrambo prek sprednjih vrat za dostavo vsebin, povsem ločeno od zasebne shrambe, ki hrani podatke kandidatov. Obe ravnini shrambe se nikoli ne mešata: napačna konfiguracija v javni ravnini ne more razkriti zasebnih podatkov kandidatov, ker gre za različna računa z različnimi omrežnimi pravili.

5.4 Administrativni dostop

V zasebno omrežje ne obstaja nobena javna administrativna končna točka. Operaterji se povezujejo prek VPN prehoda od točke do mesta, ki uporablja avtentikacijo na osnovi certifikatov. Administrativni dostop do baze podatkov in predpomnilnika je mogoč le znotraj tega tunela, saj imajo te storitve onemogočen javni omrežni dostop. To pomeni, da je vsakodnevno delovanje v celoti odmaknjeno od javnega interneta.

6. Upravljanje identitete in dostopa

6.1 Avtentikacija

Uporabniške seje se vzpostavijo s podpisanim dostopnim žetonom, veljavnim trideset minut, v paru z ločenim, neprosojnim osvežitvenim žetonom na strani strežnika. Dostopni žetoni se preverjajo pri vsaki zahtevi, uporabnik pa se ponovno preveri v bazi podatkov (vključno s preverjanjem aktivnega računa), namesto da bi zaupali zgolj vsebini žetona. Odjava takoj prekliče osvežitveno sejo na strani strežnika, zato ukradeni osvežitveni žeton ne more preživeti odjave.

Gesla niso nikoli shranjena v navadnem besedilu. Zgoščena so z bcrypt z uporabo enkratne soli za vsako geslo. Za organizacije, ki imajo raje enotno prijavo, platforma podpira OAuth prijavo z Microsoft in Google, v tem primeru pa geslo sploh ni shranjeno.

Lastništvo e-poštnega naslova se preveri prek enkratne, časovno omejene povezave za verifikacijo, preden se samoregistriran račun obravnava kot preverjen, ponovno pošiljanje verifikacijskih e-poštnih sporočil pa je omejeno s hitrostnimi omejitvami za preprečevanje zlorab.

6.2 RBAC

Avtorizacija se uveljavlja prek modela vlog s štirimi vlogami naraščajočih privilegijev: izvajalec intervjuja, vodja zaposlovanja, kadrovik in administrator. Dostop do privilegiranih operacij se uveljavlja s strežniškimi odvisnostmi, ki preverjajo tako vlogo kot status verifikacije klicatelja. Ta preverjanja vlog varujejo precej več kot sto različnih API operacij.

Vloga	Tipične zmožnosti
Izvajalec intervjuja	Izvaja dodeljene intervjuje; vidi samo intervjuje, ki so mu dodeljeni
Vodja zaposlovanja	Upravlja zaposlovanja, ki jih ima v lasti ali katerih član je
Kadrovik	Popolno upravljanje zaposlovanj in kandidatov znotraj organizacije
Administrator	Nastavitve organizacije, obračunavanje, upravljanje uporabnikov in API ključev

Poleg grobih preverjanj vlog platforma uporablja pravila vidnosti na ravni podatkov. Vodje zaposlovanja vidijo le zaposlovanja, ki so jih ustvarili ali katerih člani so; izvajalci intervjujev vidijo le intervjuje, ki so jim dodeljeni. Privilegiji se zato uveljavljajo tako na ravni »katero dejanje« kot na ravni »katere zapise«.

6.3 Izolacija po organizacijah

Platforma je večnajemniška, izolacija najemnikov pa se obravnava kot prvovrstna varnostna kontrola. Vsaka avtenticirana identiteta nosi identifikator organizacije, poizvedbe po podatkih pa so omejene na to organizacijo. Ko uporabnik zahteva zapis, ki pripada drugi organizaciji, platforma vrne odgovor »ni najdeno«, namesto da bi razkrila, da zapis obstaja. Notranji identifikatorji baze podatkov niso nikoli izpostavljeni prek omrežja; API prikazuje identifikatorje za prikaz in jih za vsako zahtevo ponovno preslika, kar odstranjuje pogost razred napadov naštevanja med najemniki.

To ni zgolj namen zasnove. Kot je opisano v Oddelku 12, naš avtomatiziran sklop izvaja obsežno matriko med organizacijami, ki poskuša doseči podatke ene organizacije s poverilnicami druge organizacije in potrjuje, da vsak tak poskus spodleti.

6.4 Programski dostop

Za integracije lahko organizacije na ustreznih paketih izdajo API ključe. Ključi uporabljajo prepoznaven prefiks, nosijo 128 bitov entropije in so shranjeni samo kot zgoščena vrednost; surovi ključ je prikazan enkrat ob ustvarjanju in nikoli več. Vsak ključ ima izrecno področje dovoljenj (read, write ali ATS integration), lahko je omejen na določena izvorna omrežja, ga je mogoče takoj preklicati in zanj veljajo omejitve hitrosti na ključ, izpeljane iz ravni paketa organizacije. Preverjanje ključa uporablja časovno varno primerjavo, da se prepreči razkrivanje informacij prek odzivnega časa.

7. Varnost aplikacije

Aplikacija je napisana tako, da odstrani celotne kategorije ranljivosti, namesto da bi jih popravljali za vsak primer posebej.

• **Injekcije.** Ves dostop do baze podatkov poteka prek object-relational mapper z uporabo parametriziranih poizvedb. Kodna baza ne vsebuje surovega SQL, formatiranega z nizi. To strukturno odpravlja SQL injection.

• **Validacija vhodov.** Vsako telo zahteve se pred vstopom v poslovno logiko preveri glede na strogo shemo. Preveliki tovori se zavrnejo, končne točke s seznami pa uporabljajo straničenje za omejitev porabe virov.

• **Kodiranje izhodov in cross-site scripting.** Besedilo, ki ga vnese uporabnik ali ustvari AI, se obravnava kot nezaupljivo. Kjer je treba vsebino prikazati kot HTML, ta ob zapisu preide skozi sanitizer z dovoljenim seznamom, namenski testni sklop pa potrjuje, da se script oznake, event handlerji in javascript URL-ji odstranijo.

• **Mass assignment.** Operacije posodabljanja uporabljajo izrecne sheme, ki izključujejo privilegirana polja, kot so vloga, organizacija in stanje kreditov, zato odjemalec ne more povišati privilegijev z objavo dodatnih polj.

• **Omejevanje hitrosti.** Končne točke za avtentikacijo in točke, nagnjene k zlorabam, so omejene s trajnim omejevalnikom na osnovi baze podatkov, ki preživi ponovne zagone in deluje pravilno v več primerkih aplikacije. Prijava, registracija, ponastavitev gesla in ponovno pošiljanje verifikacije imajo vsak svoje omejitve. Razreševanje IP naslovov odjemalcev je utrjeno proti ponarejanju posredovalnih glav.

• **Webhooki.** Dohodni webhooki ponudnikov plačil in e-pošte se pred obdelavo preverijo glede na podpise ponudnika na surovem telesu zahteve.

• **Prenosi datotek.** Prenosi imajo omejeno velikost, se validirajo, shranjujejo pod ustvarjenimi identifikatorji in ne pod uporabniško podanimi imeni ter so omejeni na zahtevo in na organizacijo.

• **Varnostne glave.** V produkciji odgovori vsebujejo strogo transportno varnost, možnosti za content-type in frame, politiko referrer ter restriktivno permissions policy, hkrati pa skrivajo oznake strežnika in ogrodja.

8. Zaščita podatkov

8.1 Šifriranje

Vsi podatki so šifrirani v mirovanju z AES-256 prek platformnih plasti šifriranja shrambe in baze podatkov v Azure. Ves omrežni promet se zagotavlja izključno prek HTTPS z uporabo TLS 1.2 ali višje; nešifrirani HTTP je na vseh ravneh preusmerjen na HTTPS. V produkciji API in spletni portal pošiljata stroge glave za transportno varnost skupaj s sklopom utrditvenih glav ter skrivata oznake različic strežnika in ogrodja.

8.2 Upravljanje skrivnosti

Skrivnosti aplikacije se hranijo v centraliziranem trezorju skrivnosti z omogočeno zaščito pred trajnim izbrisom in devetdesetdnevnim obdobjem soft-delete. Aplikacije se do virov Azure avtenticirajo z uporabo sistemsko dodeljenih upravljanih identitet namesto dolgoživih ključev; na primer, zasebna shramba ima ključe skupnega dostopa v celoti onemogočene, zato je dostop mogoč le prek dodelitev vlog na podlagi identitete, omejenih na posamezni vir. Politike dostopa do trezorja aplikacijskim principalom dodeljujejo samo bralni dostop do točno določenih skrivnosti, ki jih potrebujejo, v skladu z načelom najmanjših privilegijev.

8.3 Hramba podatkov v regiji

Vsi podatki strank in kandidatov se shranjujejo in obdelujejo znotraj Evropske unije. Gostovanje aplikacije, baza podatkov, shramba, predpomnilnik in skrivnosti se nahajajo v West Europe, obdelava z AI pa poteka v regijah EU. Ponudnik AI podatkov strank ne uporablja za učenje svojih modelov.

8.4 Življenjski cikel posameznega intervjuja

Najbolj jasen način za razumevanje kontrol zaščite podatkov je sledenje enemu intervjuju od začetka do konca. Soglasje se zajame in zabeleži, preden se karkoli obdela. Prenos je med prenosom šifriran. Prepis in analiza potekata v podatkovnih centrih EU. Rezultati se zapišejo v šifrirano shrambo. Vsak zapis nato upravlja enotna ura hrambe, ki se zaključi z zabeleženim kaskadnim izbrisom. V katerem koli trenutku lahko pravice kandidata, kot so umik soglasja, izbris, dostop ali prenosljivost, prekinejo ta tok.

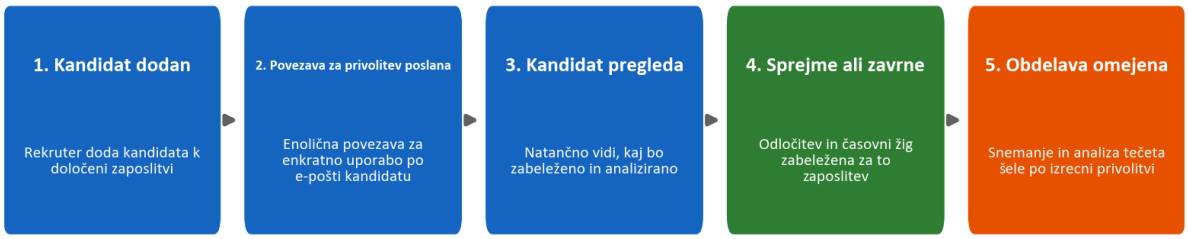
9. Zasebnost po zasnovi in GDPR

Zasebnost je vgrajena v podatkovni model in delovni tok, ne pa naknadno dodana le s politiko.

9.1 Soglasje

Noben intervju se ne snema ali analizira brez izrecnega soglasja kandidata. Ko je kandidat dodan v zaposlitveni postopek, platforma po e-pošti pošlje enkratno, unikatno povezavo za soglasje. Kandidat pregleda, kaj se bo zgodilo, in soglasje sprejme ali zavrne. Stanje soglasja, vključno s časom odgovora, se zabeleži pri tem konkretnem zaposlitvenem postopku, tako da je soglasje vedno omejeno na konkreten proces zaposlovanja in ni dano globalno.

Privolitev kandidata: izrecna in zabeležena pred vsako obdelavo

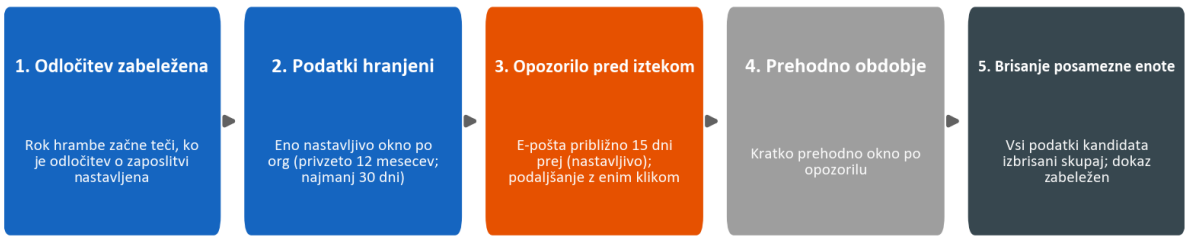


9.2 Hramba in izbris

Hramba podatkov je nastavljiva na organizacijo, s privzeto vrednostjo dvanajstih mesecev in nastavljivim minimumom tridesetih dni, ter jo je mogoče preglasiti na kandidata. Za podatke kandidata obstaja ena sama ura hrambe, ne ločen časovnik za vsak artefakt. Ura začne teči, ko je zabeležena odločitev o zaposlitvi. Pred iztekom podatkov platforma pošlje opozorilo (privzeto približno petnajst dni vnaprej) in ponudi podaljšanje z enim klikom. Ko se podatki izbrišejo, se izbrišejo kot enotna celota: zapis kandidata, intervjuji, prepisi, zvočni posnetki, dokumenti in primerjave se odstranijo skupaj, izbris pa se zabeleži v revizijski dnevnik. Delnih ali osirotelih ostankov ni.

Spodnji življenjski cikel prikazuje to enotno uro in kako se steka v en sam kaskadni izbris z zabeleženim dokazom o izbrisu.

Hramba podatkov: ena ura na kandidata, brisanje posamezne enote



9.3 Pravice posameznikov in podobdelovalci

Platforma podpira pravice posameznikov, ki jih zahteva GDPR, vključno z dostopom, izbrisom, prenosljivostjo, ugovorom in pojasnilom. Obdelava poteka na podlagi DPA, ki ga stranke sprejmejo ob registraciji in je verzioniran po organizaciji. Naši podobdelovalci in njihove vloge, vsi znotraj EU ali pod ustreznimi zaščitnimi ukrepi, so razkriti v tem sporazumu, stranke pa prejmejo predhodno obvestilo o vsaki spremembi. Oddelek 17 vsebuje register podobdelovalcev in preslikavo skladnosti po

členih.

10. Odgovorna raba AI in EU AI Act

Platforma spada v kategorijo visokega tveganja po EU AI Act, ker podpira odločitve o zaposlovanju, in to klasifikacijo jemljemo resno.

Določilno pravilo izdelka je, da **je AI podpora pri odločanju, ne odločevalec.** Sistem nikoli avtomatično ne sprejme ali zavrne kandidata. Prepisuje govor, strukturira vprašanja in odgovore, ocenjuje odgovore glede na merila, ki jih določi kadrovik, ter pripravlja osnutke povratnih informacij, človek pa pregleda vsak izhod, preden se uporabi. To ohranja človeka trdno v zanki.

Enako pomembno je, česa AI ne počne. Ne ocenjuje osebnosti, »kulturnega ujemanja«, čustvenega stanja, tona glasu, naglasa, spola, starosti, etnične pripadnosti, videza ali govorice telesa. Točkovanje je zasidrano v dokazih iz prepisa in v merilih, ki jih določi kadrovik, imena kandidatov pa so izključena iz vhodnih podatkov za ocenjevanje, da se zmanjša pristranskost. Objavljamo kartico transparentnosti, uporabniško dokumentacijo in izjavo o skladnosti, ki opisujejo sistem, njegove omejitve in zaščitne ukrepe.

Kontrola odgovorne rabe AI	Kako deluje
Človek v zanki	Vsako oceno in vsak del povratne informacije pred uporabo pregleda kadrovik
Brez avtomatiziranih odločitev	Sistem nikoli samodejno ne sprejme ali zavrne kandidata
Ocenjevanje na podlagi dokazov	Ocene se sklicujejo na podporne dokaze iz prepisa
Zasnova proti pristranskosti	Imena so izključena iz ocenjevanja; vsebina se ocenjuje pred slogom
Omejitve obsega	Osebnost, čustva, naglas in zaščitene značilnosti se nikoli ne ocenjujejo
Varnost povratnih informacij za kandidate	Zasebne povratne informacije za kandidate prehajajo skozi varnostno ograjo ustvarjanja in validacije

Te omejitve niso zapisane le v dokumentaciji; kodirane so v prompt plasti AI in preverjane z namenskim programom testiranja varnosti AI, opisanim v Oddelku 12.3.

11. Varen razvojni življenjski cikel

Varnost se uveljavlja v načinu, kako gradimo in dostavljamo programsko opremo, ne le v delujočem sistemu.

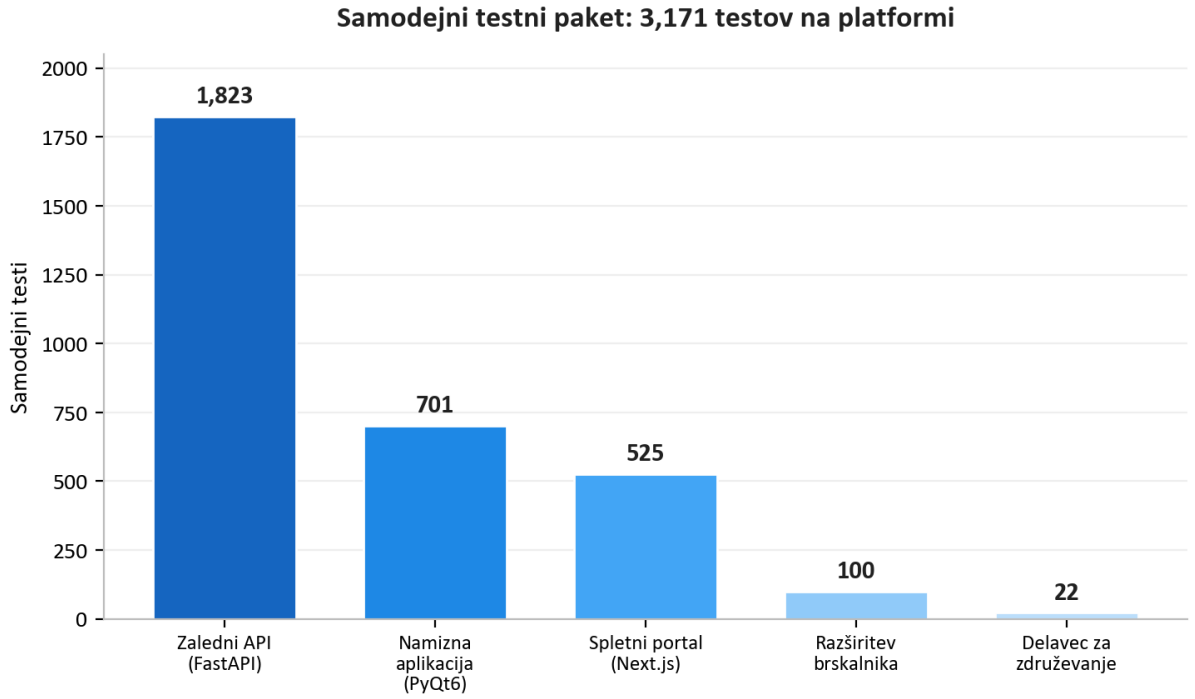
- **Ločevanje okolij.** Razvoj in produkcija sta popolnoma ločena, vsak s svojo infrastrukturo, računi za shrambo, bazo podatkov, skrivnostmi in poddomenami. Skupnega stanja ni.
- **Infrastruktura kot koda.** Celotno okolje v oblaku je definirano kot koda in pregledovano kot koda, kar pomeni, da je varnostna drža revidirljiva in ponovljiva. Presojevalec lahko natančno prebere, katera vrata so odprta, kateri viri so zasebni in katere identitete imajo katera dovoljenja.
- **Pripete in nadzorovane namestitve.** Vsak korak v CI/CD cevovodu je pripet na natančno, nespremenljivo različico. Produkcijske namestitve temeljijo na oznakah, potekajo samo prek zaščitenega produkcijskega cevovoda in so zavarovane z obvezno odobritvijo. Avtomatiziran testni sklop deluje kot pogoj za izdajo: namestitev ne more biti izvedena, če testi ne uspejo.
- **Higiena odvisnosti.** Avtomatizirano spremljanje odvisnosti tedensko predlaga posodobitve za backend, namizno aplikacijo, splet, infrastrukturo in definicije cevovodov, revizije odvisnosti pa so del našega periodičnega varnostnega pregleda.
- **Podpisani artefakti.** Namestitveni programi za namizno aplikacijo so digitalno podpisani, tako da lahko stranke preverijo, da programska oprema, ki jo nameščajo, dejansko prihaja od nas.
- **Disciplina skrivnosti.** Skrivnosti se nahajajo v trezorju in v zaščitenih skrivnostih cevovoda, nikoli v izvorni kodi.

12. Neprekinjeno varnostno testiranje

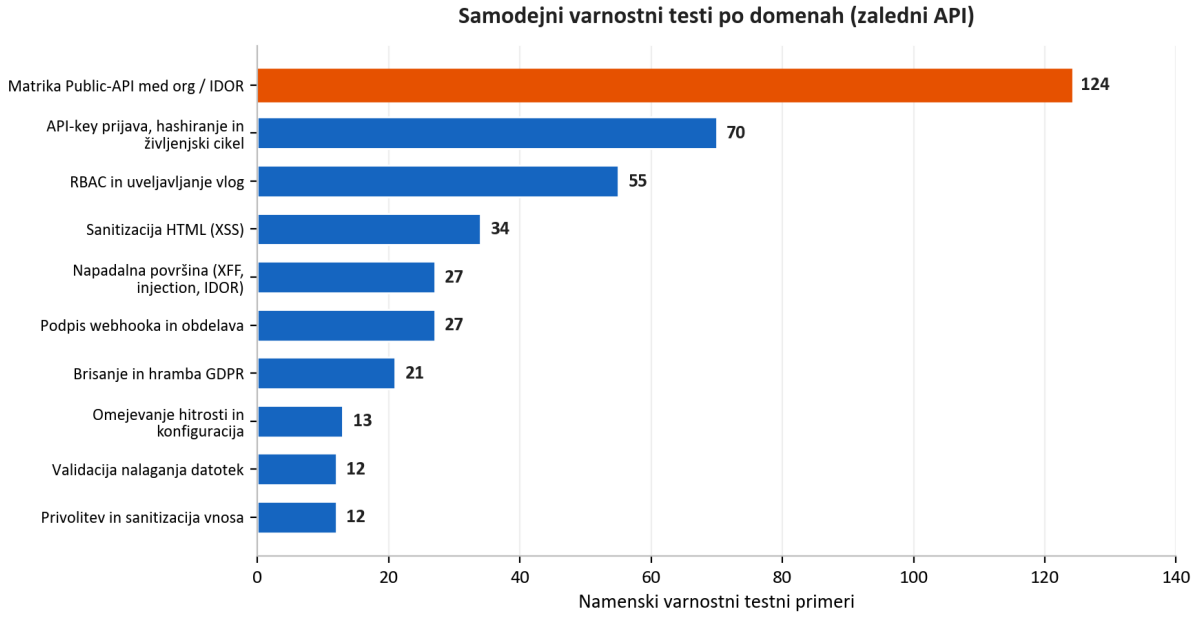
To je jedro naše zgodbe o zagotovilih in del, ki ga večina ponudnikov ne more pokazati. Varnost obravnavamo kot nekaj, kar je treba neprekinjeno meriti z izvršljivimi preverjanji, ne pa kot nekaj, kar se enkrat zgolj zatrdi.

12.1 Avtomatiziran testni sklop

Platformo pokriva **3,171 avtomatiziranih testov**, ki zajemajo backend API, namizno aplikacijo, spletni portal, razširitev za brskalnik in delavca za združevanje zvoka.



To niso le funkcionalni testi. Obsežen namenski varnostni sklop preverja kontrole, opisane prej v tem dokumentu. Spodnji graf prikazuje razčlenitev varnostno specifičnih testov v backend API po domenah.



Med številnimi drugimi ta sklop vključuje veliko matriko javnega API, ki vsako končno točko izvaja kot legitimni uporabnik, kot lastni API ključ organizacije in kot API ključ konkurenčne organizacije ter potrjuje, da je vsak poskus dostopa med organizacijami blokiran. Vključuje več deset adversarialnih testov napadalne površine za ponarejanje posredovalnih glav, injiciranje glav in uhajanje identifikatorjev, osredotočen HTML-sanitization sklop za cross-site scripting, teste uveljavljanja vlog za celoten model vlog in teste, ki dokazujejo, da so podatki kandidata resnično izbrisani kot enotna celota. Ker se ti testi izvajajo kot pogoj za izdajo, bi regresija, ki oslabi katero koli od teh kontrol, ustavila izdajo, namesto da bi dosegla stranke.

12.2 Penetracijsko testiranje v živo

Avtomatizirani enotni testi dokazujejo, da se kontrole pravilno obnašajo v izolaciji. Da dokažemo, da skupaj vzdržijo v resnični namestitvi, vzdržujemo ponovljivo metodologijo penetracijskega testiranja, ki izvaja resnične napadalne skripte proti živemu okolju. Organizirana je v šest faz:

Faza	Fokus	Primeri tega, kar se preverja
1. Statična analiza	Izvorna koda	Skrivnosti, vzorci injekcij, nevarne funkcije, manjkajoča avtentikacija, nevaren HTML
2. Pregled arhitekture	Infrastruktura	Zasebne končne točke, segmentacija, TLS, konfiguracija skrivnosti
3. Analiza napadalnih vektorjev	Nadzor izvorne kode in oblak	Zaščita vej, obseg identitete, javna izpostavljenost
4. Penetracijsko testiranje v živo	Delujoče okolje	Poizvedovanje brez avtentikacije, medorganizacijski dostop, injekcije, poseganje v žetone, SSRF, sunki omejevanja hitrosti
5. Ocenjevanje za podjetja	Zrelost	Šestnajst varnostnih kategorij, ocenjenih glede na poslovno izhodišče
6. Odvisnosti in dobavna veriga	Tveganje tretjih oseb	Revizija CVE odvisnosti, pripete akcije cevovoda, integriteta lock datotek

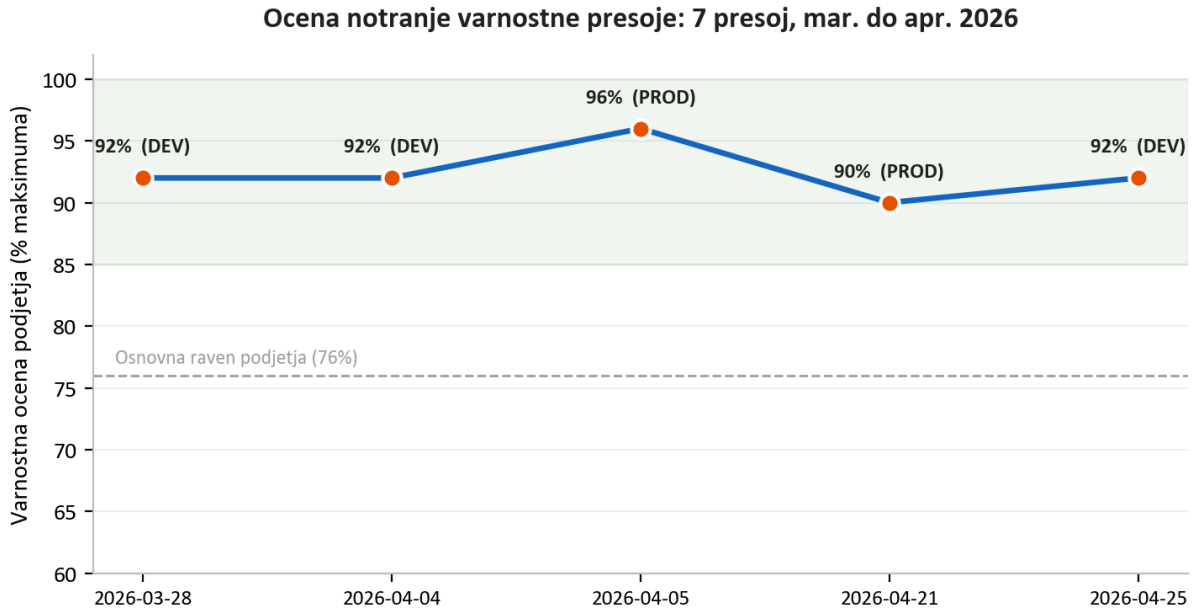
Faza 4 je resnično adversarialno testiranje proti nameščenemu sistemu, ne kontrolni seznam. Preizkuša zaščitene končne točke brez poverilnic in potrjuje, da zavrnejo dostop; registrira dve organizaciji in poskuša doseči zapise ene organizacije z računom druge; vbrizga payload-e za cross-site-scripting in server-side-template ter potrjuje, da so nevtralizirani; posega v avtentikacijske žetone in potrjuje, da so zavrnjeni; poskuša SSRF proti končnim točkam metapodatkov v oblaku; ter izvaja sunke proti avtentikacijskim končnim točkam, da potrdi, da se omejevanje hitrosti dejansko sproži v živem okolju, ne le teoretično.

12.3 Testiranje varnosti povratnih informacij za kandidate

Ker platforma lahko ustvarja zasebne razvojne povratne informacije za kandidate, nad to funkcionalnostjo izvajamo ločen adversarialni varnostni program. Sistem namenoma oskrbi z ostrimi in sovražnimi zapiski kadrovikov ter potrdi, da izhod, namenjen kandidatu, nikoli ne vsebuje vulgarnosti, nikoli ne razkrije ali pripiše identitete kadrovika ali njegovega zasebnega mnenja in nikoli ne uporablja obsojajočih oznak osebnosti. To ščiti tako kandidata, ki bi moral prejeti konstruktivne in spoštljive povratne informacije, kot tudi stranko, pri kateri interno mnenje nikoli ne sme uiti navzven.

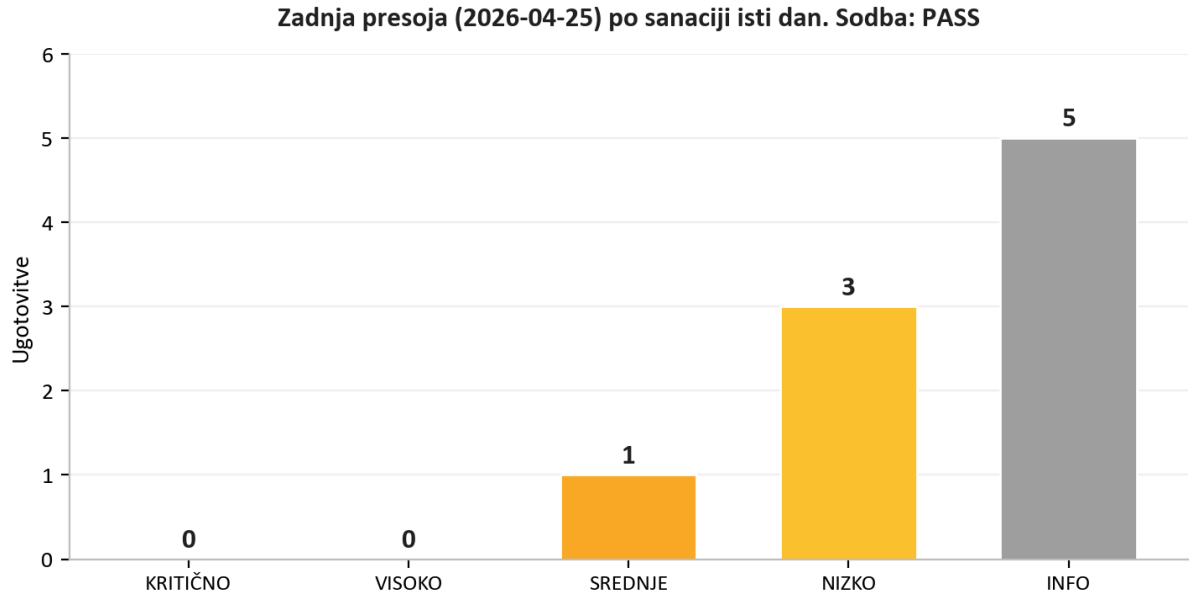
13. Rezultati varnostnih revizij

Izvajamo ponavljajoče se varnostne revizije z uporabo strukturirane, ponovljive metodologije penetracijskega testiranja in vsako pripravimo kot datirano poročilo z ugotovitvami po resnosti, dokazi in odpravo. Gre za interne revizije, izvedene v okviru našega lastnega varnostnega procesa; formalno certificiranje istih kontrol s strani tretjih oseb je na našem razvojnem načrtu. Med koncem marca in koncem aprila 2026 smo izvedli **seven such audits** v razvoju in produkciji.



Rezultat, ki je za potencialno stranko najpomembnejši, je doslednost: **v vseh sedmih revizijah je bilo zero critical findings.** Ko se je redko pojavila težava višje resnosti, je bila hitro odpravljena, pogosto še isti dan, in ponovno preverjena. Ocenjevalna lestvica je bila v tem obdobju namerno zaostrena (najvišja možna ocena je bila zvišana, ko smo dodajali več kategorij za presojo), zato normalizirana črta ocene ostaja visoka, tudi ko se je letvica dvigovala.

Naša najnovejša revizija, 25 April 2026, ponazarja, kako postopek deluje v praksi. Identificirani sta bili dve težavi višje resnosti, obe sta bili isti dan odpravljeni in ponovno preverjeni, revizija pa se je zaključila z oceno **PASS**, brez preostalih za izrabo pripravljenih težav v trenutnem modelu groženj.



Revizija	Okolje	Critical	Presoja
2026-03-28	Razvoj	0	Pripravljeno za produkcijo
2026-04-04	Razvoj	0	Pripravljeno za podjetja
2026-04-05	Produkcija	0	Pripravljeno za podjetja
2026-04-20	Razvoj	0	Pripravljeno za produkcijo, opombe
2026-04-20	Razvoj	0	Uspešno z opombami
2026-04-21	Produkcija	0	Varno, brez izrabljivih ugotovitev
2026-04-25	Razvoj	0	Uspešno

Vzorec v teh revizijah je najbolj iskren dokaz, ki ga lahko ponudimo: težave so odkrite, ker jih aktivno iščemo, in hitro zaprte, ker je proces zasnovan za njihovo zapiranje. Ponudnik, ki nikoli ne poroča o ugotovitvah, je običajno ponudnik, ki jih ne išče.

14. Operativna odpornost in deljena odgovornost

14.1 Spremljanje in beleženje

Telemetrija aplikacije in platforme teče v centraliziran delovni prostor za log analytics in storitev za spremljanje aplikacij, kar nam daje vidnost nad razpoložljivostjo in obnašanjem. Občutljiva dejanja, kot so brisanje podatkov, sprejem pravnih sporazumov in klici AI, se beležijo v namenskih revizijskih tabelah, zato obstaja trajen zapis o tem, kdo je kaj storil s pomembnimi podatki.

14.2 Varnostne kopije in obnova

Upravljana baza podatkov hrani avtomatizirane varnostne kopije, zasebna shramba pa je zaščitena s soft-delete hrambo tako za blob-e kot vsebnike, zato je mogoče nenameren ali zlonameren izbris obnoviti znotraj obdobja hrambe. Kritična infrastruktura vsebuje zaklepe za brisanje, ki preprečujejo nenamerno odstranitev produkcijskih virov.

14.3 Povzetek deljene odgovornosti

Področje	AI Interview Analyzer	Stranka
Infrastruktura, omrežje, nameščanje popravkov	Da	-
Varnost aplikacije in AI cevovod	Da	-
Šifriranje, skrivnosti, hramba podatkov v regiji	Da	-
Upravljanje uporabnikov in vlog	Zagotavlja kontrole	Upravlja uporabnike in vloge
Konfiguracija politike hrambe	Zagotavlja kontrole	Nastavlja obdobje hrambe
Soglasje kandidata	Zagotavlja potek	Zagotavlja, da se uporablja
Močne poverilnice končnih uporabnikov in SSO	Podpira SSO in politiko	Uveljavlja interno politiko

15. Model groženj in preslikava OWASP

Načrtujemo proti konkretnemu naboru nasprotnikov: zunanjemu napadalcu brez poverilnic, radovednemu ali zlonamernemu avtenticiranemu uporabniku ene organizacije, ki skuša doseči podatke druge organizacije, kompromitirani odvisnosti in interni napaki. Spodnja tabela preslika široko uporabljene kategorije tveganj OWASP Top 10 na konkretne kontrole, ki jih obravnavajo na tej platformi, pri čemer se vsaka preverja s testiranjem, opisanim v Oddelku 12.

Tveganje OWASP	Kako ga platforma zmanjšuje
Broken access control	RBAC na vsaki privilegirani končni točki; omejevanje po organizaciji; »ni najdeno« pri medorganizacijskem dostopu; preslikava identifikatorjev; medorganizacijska testna matrika
Cryptographic failures	TLS 1.2+ med prenosom; AES-256 v mirovanju; bcrypt zgoščevanje gesel; skrivnosti v upravljanem trezorju
Injection	Parametrizirane poizvedbe samo prek ORM; stroga validacija shem; HTML sanitization ob zapisu
Insecure design	Večplastna obramba; modeliranje groženj in pregled arhitekture v vsaki reviziji
Security misconfiguration	Infrastruktura kot koda; omrežne skupine s privzeto prepovedjo; varnostne glave; onemogočeni ključi skupne shrambe; API schema ni izpostavljena v produkciji
Vulnerable components	Tedensko avtomatizirano spremljanje odvisnosti; revizije CVE odvisnosti v periodičnem pregledu
Identification and authentication failures	Kratkoživi žetoni; prijava z omejitvijo hitrosti; verifikacija e-pošte; podpora za SSO; brez gesel v navadnem besedilu
Software and data integrity failures	Pripeti, nespremenljivi koraki cevovoda; podpisani namestitveni programi za namizno aplikacijo; preverjanje podpisov webhookov; produkcijske namestitve, nadzorovane z oznakami
Security logging and monitoring failures	Centralizirana telemetrija; namenske revizijske tabele za občutljiva dejanja
Server-side request forgery	Odhodni klici omejeni na zaupanja vredne končne točke; SSRF preizkusi v okviru penetracijskega testiranja

Ta preslikava je hrbtenica našega argumenta o zagotovilih: za vsak dobro znan razred napadov obstaja poimenovana kontrola in za vsako poimenovano kontrolo obstaja test.

16. Upravljanje ranljivosti in odgovorno razkritje

Varnost ni nikoli dokončana, zato izvajamo neprekinjeno zanko odkrivanja in odpravljanja.

- **Odkrivanje.** Ranljivosti se odkrijejo iz štirih virov: avtomatiziranega testnega sklopa, ponavljajočih se revizij penetracijskega testiranja, avtomatiziranega spremljanja odvisnosti ter poročil strank ali raziskovalcev.
- **Triaža.** Vsaki ugotovitvi se dodeli resnost (critical, high, medium, low ali informational), dokazi in lastnik odprave, natančno tako, kot je zapisano v naših revizijskih poročilih.
- **Cilji odprave.** Ugotovitve critical in high imajo prednost za takojšnjo odpravo; v naši zgodovini revizij so bile ugotovitve višje resnosti običajno odpravljene in ponovno preverjene še isti dan. Ugotovitve medium in nižje se načrtujejo v rednem ciklu vzdrževanja.
- **Preverjanje.** Popravki se ponovno testirajo, kjer je ustrezno pa se izvede tudi preverjanje v živo proti nameščenemu okolju, da se potrdi, da je težava dejansko zaprta in ne le zaprta v kodi.
- **Razkritje.** Varnostne pomisleke nam je mogoče prijaviti neposredno. Poročila potrdimo, jih raziščemo in prijavitelja obveščamo do rešitve.

17. Preslikava skladnosti

17.1 GDPR

Področje GDPR	Implementacija na platformi
Pravna podlaga (Art. 6)	Izrecno soglasje kandidata, zajeto pred obdelavo
Načelo najmanjšega obsega podatkov in omejitve hrambe (Art. 5)	Obdelujejo se le podatki, relevantni za intervju; nastavljiva hramba z avtomatskim izbrisom
Pravica do izbrisa (Art. 17)	Brisanje vseh podatkov kandidata kot enotne celote z zabeleženim dokazom o izbrisu
Pravice posameznika (Art. 15 to 20)	Podprti so dostop, izbris, prenosljivost in ugovor
Obveznosti obdelovalca (Art. 28)	DPA je sprejet ob registraciji in verzioniran po organizaciji
Varnost obdelave (Art. 32)	Šifriranje, nadzor dostopa, izolacija in neprekinjeno testiranje, kot je opisano v tem dokumentu
Transparentnost podobdelovalcev	Razkriti v DPA s predhodnim obvestilom o spremembi

17.2 EU AI Act

Platforma se obravnava kot AI sistem visokega tveganja, ki podpira odločitve o zaposlovanju, in vzdržujemo dokumentacijo, usklajeno z uredbo, vključno s kartico transparentnosti, uporabniško dokumentacijo in izjavo o skladnosti. Ključni zaščitni ukrepi, človeški nadzor, transparentnost, ocenjevanje na podlagi dokazov in stroge omejitve obsega tega, kar AI ocenjuje, so opisani v Oddelku 10. Formalno dokumentacijo o skladnosti še naprej nadgrajujemo skladno z napredovanjem časovnice implementacije uredbe.

17.3 Certifikati gostovanja

Platforma v celoti deluje na Microsoft Azure, katerega podatkovni centri imajo neodvisne certifikate, vključno z ISO 27001 in SOC 2. Ti certifikati pokrivajo fizične in platformne plasti pod našo aplikacijo; kontrole na ravni aplikacije so tiste, opisane v tem dokumentu.

17.4 Register podobdelovalcev

Podobdelovalec	Namen	Regija
Microsoft Azure	Gostovanje, AI in obdelava govora, shramba, transakcijska e-pošta	EU (West Europe, Sweden Central)
Stripe	Obdelava naročnin in plačil	EU (Ireland)
Fakturownia	Izdajanje računov	EU (Poland)
ATS connector (optional)	Integracija s sistemom za sledenje kandidatom, omogočena le na zahtevo	EU

18. Varnostni razvojni načrt

Varnost obravnavamo kot program neprekinjenih izboljšav. Trenutne pobude na našem razvojnem načrtu vključujejo okrepitev možnosti večfaktorske avtentikacije za administratorske račune, razširitev centraliziranega revizijskega beleženja dostopa do podatkov, nadaljnje redno zaostrovanje aktualnosti odvisnosti in napredovanje formalnega certificiranja kontrol, opisanih v tem dokumentu, s strani tretjih oseb. Nobena od teh točk danes ne predstavlja vrzeli, ki bi izpostavljala podatke strank; vsaka je izboljšava že tako večplastne varnostne drže.

19. Povzetek

AI Interview Analyzer varuje podatke kandidatov in strank z večplastno arhitekturo: omrežjem, ki je privzeto zasebno in brez javnih podatkovnih storitev, močno identiteto in izolacijo po organizacijah, aplikacijsko kodo, ki iz zasnove odstranjuje celotne razrede ranljivosti, šifriranjem in hrambo podatkov v EU ter kontrolami zasebnosti, vgrajenimi v podatkovni model. Tisto, kar platformo ločuje, so dokazi za temi trditvami. Z 3,171 avtomatiziranimi testi, ponovljivo metodologijo penetracijskega testiranja v živo, namenskim programom varnosti AI in zgodovino sedmih internih varnostnih revizij z zero critical findings lahko pokažemo, ne le trdimo, da je platforma varna.

Priloga A: Katalog varnostnih kontrol

Strnjen pregled primarnih kontrol in dokazov, ki podpirajo vsako od njih.

Kontrola	Mehanizem	Dokaz
Šifriranje prenosa	Samo HTTPS, TLS 1.2+, preusmeritev HTTP	Infrastruktura kot koda; arhitekturna revizija
Šifriranje v mirovanju	Platformno šifriranje AES-256 na shrambi in bazi podatkov	Konfiguracija platforme; arhitekturna revizija
Zaščita gesel	bcrypt s soljo za vsako geslo	Nadzor izvorne kode; testi avtentikacije
Upravljanje sej	30-minutni podpisani žetoni, prekličljiv osvežitveni mehanizem na strani strežnika	Nadzor izvorne kode; testi avtentikacije
Avtorizacija	Nadzor dostopa s štirimi vlogami na privilegiranih končnih točkah	Testni sklop uveljavljanja vlog
Izolacija najemnikov	Omejevanje poizvedb po organizaciji; 404 pri medorganizacijskem dostopu	Medorganizacijska testna matrika
Varnost API ključev	Zgoščena hramba, omejena dovoljenja, omejitve hitrosti na ključ	Testni sklop API ključev
Zaščita pred injekcijami	Parametrizirane poizvedbe samo prek ORM	Statična analiza; testi injekcij
Zaščita pred cross-site scripting	HTML sanitization ob zapisu	Testni sklop HTML sanitization
Omejevanje hitrosti	Trajni omejevalnik na podlagi baze podatkov na avtentikacijskih končnih točkah	Testi omejevanja hitrosti; preverjanja sunkov v živo
Integriteta webhookov	Preverjanje podpisov ponudnika na surovem telesu	Testni sklop webhookov
Upravljanje skrivnosti	Upravljan trezor, zaščita pred trajnim izbrisom, upravljana identiteta	Infrastruktura kot koda; arhitekturna revizija
Izolacija omrežja	Zasebne končne točke; segmentacija s privzeto prepovedjo	Infrastruktura kot koda; arhitekturna revizija
Brisanje podatkov	Kaskadni izbris kot enotna celota z revizijskim dnevnikom	Testni sklop GDPR za brisanje
Dobavna veriga	Pripeti koraki cevovoda; tedensko spremljanje odvisnosti	Konfiguracija cevovoda; revizija odvisnosti

Priloga B: Pogosta vprašanja za varnostne presojevalce

Kje so shranjeni naši podatki? V celoti znotraj Evropske unije, na Microsoft Azure, v West Europe z obdelavo AI v regijah EU. Podatki kandidatov nikoli ne zapustijo EU.

Ali se naši podatki uporabljajo za učenje AI modelov? Ne. Ponudnik AI podatkov strank ne uporablja za učenje.

Ali je baza podatkov dosegljiva z interneta? Ne. Javni omrežni dostop je onemogočen, baza podatkov pa je dosegljiva samo prek zasebne končne točke znotraj virtualnega omrežja.

Ali lahko ena stranka vidi podatke druge stranke? Ne. Vsaka poizvedba je omejena na organizacijo klicatelja, medorganizacijski dostop vrne »ni najdeno«, avtomatizirana matrika pa to izolacijo neprekinjeno testira.

Kako so shranjena gesla? Zgoščena z bcrypt in enkratno soljo za vsako geslo. Podprta je enotna prijava z Microsoft in Google, v tem primeru pa geslo ni shranjeno.

Ali podpirate enotno prijavo? Da, prek Microsoft in Google OAuth.

Kako dolgo veljajo dostopni žetoni? Trideset minut, v paru s prekličljivo osvežitveno sejo na strani strežnika, ki se ob odjavi razveljavi.

Kako se obravnava soglasje kandidata? Vsak kandidat prejme unikatno, enkratno povezavo za soglasje in jo mora sprejeti pred kakršnim koli snemanjem ali analizo. Soglasje se zabeleži pri konkretnem zaposlitvenem postopku.

Kako se podatki izbrišejo? Kot enotna celota, ki zajema zapis kandidata, intervjuje, prepise, zvok, dokumente in primerjave, po nastavljivem razporedu hrambe, z zabeleženim dokazom o izbrisu. Kandidati lahko izbris zahtevajo tudi neposredno.

Ali imate DPA? Da, sprejet je ob registraciji in verzioniran po organizaciji, vključno z registrom podobdelovalcev.

Ali AI sprejema odločitve o zaposlovanju? Ne. Zagotavlja le podporo pri odločanju; človek pregleda vsak izhod in sprejme vse odločitve.

Kako dokazujete svoje varnostne trditve? Z 3,171 avtomatiziranimi testi, vključno z namenskim varnostnim sklopom, ponovljivo šestfazno metodologijo penetracijskega testiranja, ki se izvaja proti živim okoljem, programom testiranja varnosti AI in ponavljajočimi se pisnimi revizijskimi poročili.

Kaj se zgodi, ko odkrijete ranljivost? Dodeljeni so ji resnost, dokazi in lastnik, odpravljena je po prioritetnem razporedu, ponovno preverjena, vključno s preverjanji v živo, kjer je to ustrezno, ter zabeležena v revizijskem poročilu.

Ali lahko izvedemo lastni penetracijski test? Varnostne presoje je mogoče urediti prek vašega skrbnika računa ob ustrezno določenem obsegu in razporedu.

Priloga C: Slovar

Izraz	Pomen
AES-256	Močan simetrični šifrirni standard za zaščito podatkov v mirovanju
bcrypt	Namensko zasnovana funkcija za zgoščevanje gesel s soljenjem za vsako geslo
Upravljana identiteta	Identiteta, ki jo izda platforma in storitvi omogoča avtentikacijo brez shranjenih ključev
Zasebna končna točka	Zasebni omrežni naslov, ki storitev v oblaku ohranja zunaj javnega interneta
Network security group	Nabor pravil dovoli/zavrni, ki filtrira omrežni promet do podomrežja
RBAC	Nadzor dostopa na podlagi vlog, ki dodeljuje dovoljenja glede na vlogo uporabnika
IDOR	Insecure direct object reference, napaka v nadzoru dostopa, pred katero se platforma brani
SSRF	Server-side request forgery, razred napadov, ki ga preverjamo v naših penetracijskih testih
Web application firewall	Robna kontrola, ki filtrira zlonameren spletni promet
Data processing agreement	Pogodba, ki ureja, kako obdelovalec ravna z osebnimi podatki v imenu upravljavca

Priloga D: Kontakt in upravljanje dokumenta

AI Interview Analyzer Sp. z o.o.

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

NIP: 5253079974

Za varnostni pregled, kopijo našega DPA ali naše dokumentacije o skladnosti z EU AI Act se obrnite na svojega skrbnika računa.

Ta dokument opisuje varnostno držo storitve AI Interview Analyzer na datum izdelave, naveden v nogi dokumenta. Zagotovljen je za namene presoje in ne predstavlja dela nobene pogodbe. Posebne pogodbene varnostne zaveze so določene v veljavnem sporazumu in DPA.