# Turvalisuse valge raamat

Enterprise Security Overview - AI Interview Analyzer

| | |
|---|---|
| **Pakkuja:** | AI Interview Analyzer Sp. z o.o. |
| **Aadress:** | ul. Jedrusik 6/53, 01-748 Warszawa, Poland |
| **NIP:** | 5253079974 |
| **REGON:** | 54402118500000 |
| **Klassifikatsioon:** | PUBLIC |
| **Kuupäev:** | 24.06.2026 |

# Contents

# Turvalisuse valge raamat

**Teenusepakkuja:** AI Interview Analyzer Sp. z o.o., Warszawa, Poland

**Sihtgrupp:** Ettevõtte turvalisuse, IT ja hanke meeskonnad

**Klassifikatsioon:** Avalik

## 1. Juhtkokkuvõte

AI Interview Analyzer on ettevõtetele mõeldud värbamisplatvorm, mis salvestab intervjuusid kandidaadi selgesõnalise nõusoleku alusel, transkribeerib ja struktureerib need ning loob tõenduspõhist hindamistuge värbajatele. Kuna platvorm töötleb kandidaatide isikuandmeid ja toetab värbamisprotsesse, käsitleme turvalisust ja privaatsust esmaste arhitektuuriliste piirangutena, mitte hiljem lisatud funktsioonidena.

See valge raamat kirjeldab konkreetsete ja kontrollitavate terminitega, kuidas me kaitseme kliendi- ja kandidaadiandmeid. See on kirjutatud inimestele, kes hindavad teenusepakkujaid: turvainseneridele, IT-administraatoritele, andmekaitseametnikele ja hankespetsialistidele. Iga selles dokumendis esitatud näitaja pärineb otse meie enda insenerisüsteemidest, mitte turundusmaterjalidest.

Keskne sõnum on lihtne: **me ei väida üksnes, et platvorm on turvaline, vaid testime seda pidevalt.** Meie koodibaas sisaldab **3,171 automatiseeritud testi**, sealhulgas spetsiaalset turbetestide komplekti, mis katab autentimist, autoriseerimist, organisatsioonidevahelist isolatsiooni, süstekaitseid ja andmete kustutamist. Sellele lisaks käitame korduvat penetratsioonitestimise raamistikku reaalsete juurutuste vastu ja koostame kirjalikke auditiraporteid. Seitsme sisemise turvaauditiga märtsis ja aprillis 2026 registreerisime **zero critical findings**, kusjuures meie viimase auditi lõppotsus oli **PASS**. (Nende kontrollimeetmete ametlik kolmanda osapoole sertifitseerimine on meie tegevuskavas; vt jaotis 18.)

| Turbeomadus | Kokkuvõte |
|---|---|
| Majutus | Microsoft Azure, ainult EL piirkonnad |
| Võrgumudel | Private endpoints, vaikimisi-keelatud võrgusegmentatsioon, puudub avalik andmebaas |
| Krüpteerimine | AES-256 puhkeolekus, TLS 1.2 või kõrgem edastusel |
| Identiteet | Lühiealised allkirjastatud tokenid, bcrypt parooliräsi, SSO tugi |
| Juurdepääsukontroll | Rollipõhine juurdepääsukontroll range organisatsioonipõhise isolatsiooniga |
| Saladused | Tsentraliseeritud saladuste hoidla managed-identity juurdepääsuga |
| Privaatsus | Selgesõnaline nõusolek, seadistatav säilitamine, ühe üksuse kustutamine |
| Vastutustundlik AI | Ainult otsustustugi, inimene on alati protsessis |
| Kindlus | 3,171 automatiseeritud testi ning korduvad penetratsioonitestid ja auditid |

### 1.1 Kuidas seda dokumenti lugeda

Jaotised 3 kuni 11 kirjeldavad andmeid kaitsvaid kontrolle: arhitektuuri, võrku, identiteeti, rakendust, andmekaitset, privaatsust ja turvalist arendustsüklit. Jaotised 12 ja 13 käsitlevad meie eristuvat pideva testimise programmi ja auditiajalugu. Jaotised 14 kuni 17 katavad toimingud, ohumudeldamise, haavatavuste halduse ja vastavuskaardistuse. Lisad pakuvad kontrollikataloogi, hindaja KKK-d ja sõnastikku, mida turvameeskond saab hinnangu andmisel otse kasutada.

# 2. Dokumendi ulatus ja lähenemine

## 2.1 Mida see dokument katab

See valge raamat katab AI Interview Analyzer teenuse turbearhitektuuri ja tavad: majutuskeskkonna, võrgu disaini, identiteedi- ja juurdepääsuhalduse, rakendustaseme kontrollid, andmekaitse, privaatsuse ja regulatiivse vastavuse, turvalise arendustsükli ning meie pideva turbetestimise programmi.

## 2.2 Mis teeb selle kontrollitavaks

Teenusepakkuja turvaväiteid on lihtne kirjutada ja raske usaldada. Seetõttu oleme sidunud iga peamise väite selles dokumendis millegi konkreetse ja loendatavaga meie insenerisüsteemides: koodis rakendatud kontroll, test, mis tõendab kontrolli toimimist, infrastruktuurimääratlus, mis seda jõustab, või auditiraport, mis dokumenteerib kontrolli. Kui mõni kontroll on alles meie tulevikuplaanis, mitte täna kasutuses, ütleme seda selgesõnaliselt. Eelistame väita vähem ja olla usaldatud, kui väita liiga palju ja jääda vahele.

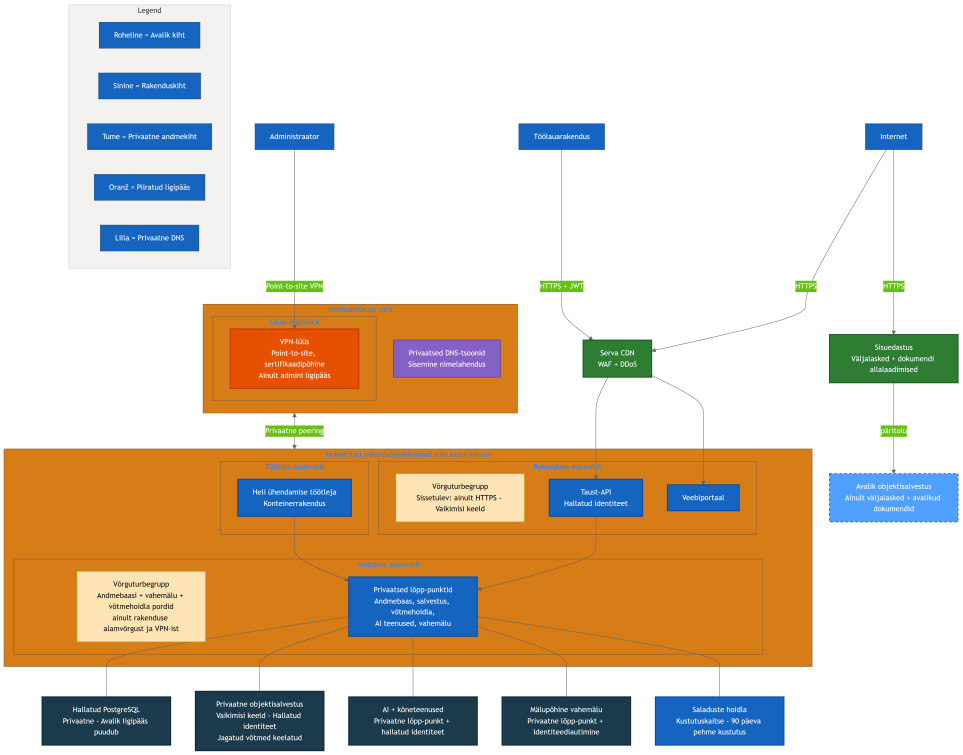
## 2.3 Jagatud vastutus

Platvormi pakutakse tarkvarateenusena. Me haldame infrastruktuuri, rakendust, AI torujuhet ja andmetöötlust. Klient vastutab oma kasutajakontode ja rollide haldamise, andmete säilitamise perioodide seadistamise eest vastavalt sisepoliitikale ning selle eest, et kandidaadi nõusolek saadakse platvormi pakutava nõusoleku töövoo kaudu. Jaotis 14 kirjeldab seda jaotust täpsemalt.

---

# 3. Turbearhitektuuri ülevaade

Platvorm on ehitatud väikese arvu koostööd tegevate teenustena, mitte ühe monoliidina. Kliendina toimivad töölauarakendus ja veebiportaal. Keskne backend API haldab kogu püsisalvestust, autentimist, arveldust, AI torujuhet, nõusolekut, e-posti, failikäsitlust ja juhtpaneele. Heli ühendamise töötluskomponent töötleb salvestisi asünkroonselt. Kogu tundlik olek asub backend API taga; kliendid ei suhtle kunagi otse andmebaasi, salvestuse ega AI teenustega.




Ülaltoodud diagramm näitab tootmiskeskkonna topoloogiat, kus ressursside nimed on teadlikult üldistatud. Selles on nähtavad kolm põhimõtet:

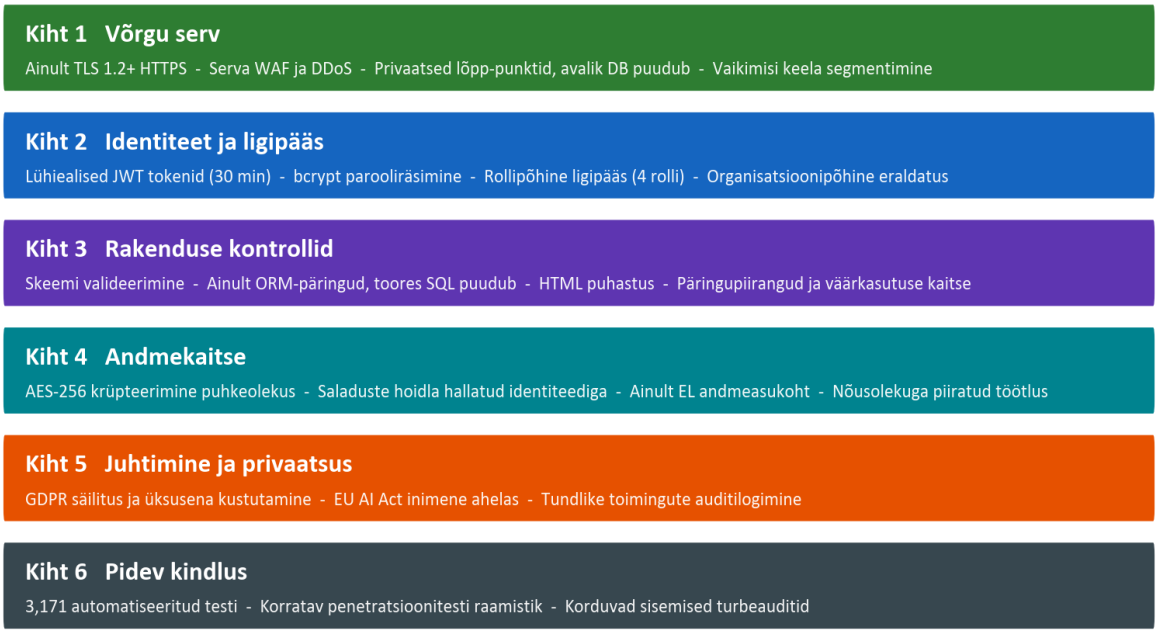
- **Andmeteenuseid ei eksponeerita otse.** Andmebaasil, privaatsel objektisalvestusel, AI teenustel ja vahemälul on avalik võrgupääs keelatud ning need on kättesaadavad ainult private endpoints kaudu isoleeritud virtuaalvõrgus. Saladuste hoidlat kasutab rakendus private endpoint kaudu ning seda kaitsevad täiendavalt platvormi identiteediautentimine ja vähimate õiguste juurdepääsupoliitikad, seega nõuab iga juurdepääs kehtivat, autoriseeritud identiteeti sõltumata võrguteest.
- **Eraldatud avalik pind.** Ainus avalik objektisalvestus sisaldab väljalasete allalaadimisi ja avalikke dokumente. See ei sisalda kunagi kandidaadiandmeid. Kliendile suunatud rakendusliiklus läbib servakihti, mis pakub web application firewall kaitset, distributed-denial-of-service kaitset ja sisu edastust.
- **Administratiivne juurdepääs on piiratud.** Operaatorid jõuavad sisemiste ressurssideni ainult sertifikaadipõhise point-to-site VPN kaudu haldussõlme võrgus, mitte avaliku interneti kaudu.

Iga juurutusaste (arendus ja tootmine) on täielikult isoleeritud keskkond, millel on oma võrk, salvestuskontod, andmebaas ja saladused. Kliendi tootmisandmeid ei esine kunagi madalamates keskkondades. Jagatud haldussõlm sisaldab ainult VPN gateway'd ja private DNS-i, mis on iga keskkonnaga privaatselt seotud.

# 4. Mitmekihiline kaitse

Ühtegi üksikut kontrolli ei usaldata peatama kõiki ründeid. Platvorm kihistab sõltumatuid kontrolle nii, et ühe kihi rike ei avaldaks andmeid. Allpool toodud kihid on kõik rakendatud ja, nagu kirjeldatud jaotises 12, individuaalselt testitud.

**Kihiline turbemudel: sõltumatud kontrollid igal tasemel**




| Kiht | Tüüpilised kontrollid |
|---|---|
| Võrgu serv | Ainult TLS transport, serva WAF ja DDoS kaitse, private endpoints, vaikimisi-keelatud segmentatsioon |
| Identiteet ja juurdepääs | Lühiealised allkirjastatud tokenid, bcrypt räsi, rollipõhine juurdepääsukontroll, organisatsioonipõhine isolatsioon |
| Rakendus | Skeemipõhine valideerimine kogu sisendile, ainult ORM-põhine andmepääs, väljundkodeerimine, kiiruse piiramine |
| Andmekaitse | Krüpteerimine puhkeolekus, saladuste hoidla managed identity'ga, EL andmeresidentsus, nõusolekuga piiratud töötlemine |
| Haldus ja privaatsus | Seadistatav säilitamine, ühe üksuse kustutamine, inimese järelevalvega AI, auditilogimine |
| Pidev kindlus | Automatiseeritud testide komplekt, korduvad penetratsioonitestid, regulaarsed sisemised turvaauditid |

Ülejäänud dokument käib need kihid ükshaaval läbi ning kirjeldab seejärel, kuidas me pidevalt tõendame, et need kihid peavad vastu.

# 5. Võrguturvalisus

## 5.1 Vaikimisi privaatne

Andmekiht on konstruktsioonilt privaatne. Hallatud PostgreSQL andmebaasil on avalik võrgupääs keelatud ja see on kättesaadav ainult private endpoint kaudu. Privaatne objektisalvestus on seadistatud vaikimisi võrgupääsu keelama, keelab täielikult shared access keys kasutamise ning on rakenduse alamvõrgust kättesaadav ainult managed identity kaudu. Vahemälu, AI teenused ja saladuste hoidla on samuti kättesaadavad private endpoints kaudu koos private DNS lahendusega.

Praktikas tähendab see, et puudub internetti suunatud andmebaasi connection string ja puudub kandidaadiheli avalik salvestus-URL: andmebaasil ja privaatsel salvestusel on avalik võrgupääs otseselt keelatud. Saladuste hoidlat kasutab rakendus private endpoint kaudu ning seda kaitsevad platvormi identiteediautentimine ja vähimate õiguste juurdepääsupoliitikad; rakenduse identiteetidele on antud ainult lugemisõigus ainult nendele saladustele, mida nad vajavad, seega ei saa saladusi kätte ilma kehtiva, autoriseeritud identiteedita. Ründepind, mida väline vastane üldse puudutada saab, piirdub rakenduse HTTPS lõpp-punktidega servakihi taga.

## 5.2 Võrgusegmentatsioon

Iga keskkond on jagatud eraldi alamvõrkudeks rakenduskihi, andmekihi ja asünkroonse töötluskomponendi jaoks. Iga alamvõrku juhib network security group, mille viimane reegel keelab kogu sissetuleva liikluse. Rakenduse alamvõrk aktsepteerib ainult sissetulevat HTTPS liiklust. Andmealamvõrk aktsepteerib ainult konkreetseid andmebaasi, vahemälu ja hoidla porte ning ainult rakenduse alamvõrgust või administratiivsest VPN-ist. See tähendab, et isegi kui ründaja jõuaks kuidagi rakenduskihini, ei saa ta vabalt liikuda andmekihini; lubatud on ainult need teed, mida rakendus õiguspäraselt kasutab.

## 5.3 Servakiht

Avalik rakendusliiklus on suunatud servakihile, mis pakub web application firewall kaitset, DDoS kaitset ja content delivery network teenust. Väljalasete ja dokumentide allalaadimised teenindatakse spetsiaalsest avalikust salvestuskontost läbi sisuedastuse esikihi, mis on täiesti eraldi privaatsest salvestusest, kus hoitakse kandidaadiandmeid. Need kaks salvestustasandit ei segune kunagi: vale konfiguratsioon avalikul tasandil ei saa paljastada privaatseid kandidaadiandmeid, sest need asuvad eri kontodel erinevate võrgureeglitega.

## 5.4 Administratiivne juurdepääs

Privaatsesse võrku ei ole avalikku administratiivset lõpp-punkti. Operaatorid ühenduvad point-to-site VPN gateway kaudu, mis kasutab sertifikaadipõhist autentimist. Administratiivne juurdepääs andmebaasile ja vahemälule on võimalik ainult selle tunneli seest, kuna neil teenustel on avalik võrgupääs keelatud. See hoiab igapäevased toimingud täielikult avalikust internetist eemal.

# 6. Identiteedi- ja juurdepääsuhaldus

## 6.1 Autentimine

Kasutajaseansid luuakse allkirjastatud access tokeniga, mis kehtib kolmkümmend minutit, koos eraldi läbipaistmatu serveripoolse refresh tokeniga. Access tokenid verifitseeritakse igal päringul ning kasutaja valideeritakse uuesti andmebaasi vastu (sealhulgas aktiivse konto kontroll), selle asemel et usaldada ainult tokeni sisu. Väljalogimine tühistab serveripoolse refresh seansi kohe, seega ei saa varastatud refresh token jääda kehtima pärast väljalogimist.

Paroole ei salvestata kunagi loetaval kujul. Need räsitakse bcrypt abil, kasutades iga parooli jaoks unikaalset soola. Organisatsioonidele, kes eelistavad single sign-on'i, toetab platvorm OAuth sisselogimist Microsofti ja Google'iga; sel juhul paroole üldse ei hoita.

E-posti aadressi omandiõigus verifitseeritakse ühekordse, ajaliselt piiratud verifitseerimislingi kaudu enne, kui iseregistreeritud kontot käsitletakse verifitseerituna, ning verifitseerimiskirjade uuestisaatmised on väärkasutuse vältimiseks kiirusepiiranguga.

## 6.2 Rollipõhine juurdepääsukontroll

Autoriseerimine jõustatakse rollimudeliga, millel on neli kasvava õigustasemega rolli: intervjueerija, värbamisjuht, värbaja ja administraator. Juurdepääs privilegeeritud toimingutele jõustatakse serveripoolsete sõltuvuste kaudu, mis kontrollivad nii kutsuja rolli kui ka verifitseerimisstaatust. Need rollikontrollid kaitsevad oluliselt rohkem kui sadat eraldiseisvat API toimingut.

| Roll | Tüüpilised õigused |
|---|---|
| Intervjueerija | Viib läbi talle määratud intervjuusid; näeb ainult talle määratud intervjuusid |
| Värbamisjuht | Haldab värbamisi, mille omanik või liige ta on |
| Värbaja | Täielik värbamise ja kandidaatide haldus organisatsiooni sees |
| Administraator | Organisatsiooni seaded, arveldus, kasutajate ja API võtmete haldus |

Lisaks jämedama taseme rollikontrollidele rakendab platvorm andmetaseme nähtavusreegleid. Värbamisjuhid näevad ainult neid värbamisi, mille nad on loonud või mille liikmed nad on; intervjueerijad näevad ainult neile määratud intervjuusid. Seega jõustatakse õigused nii tasandil „milline tegevus" kui ka tasandil „millised kirjed".

## 6.3 Organisatsioonipõhine isolatsioon

Platvorm on mitmerendiline ning rentnike isolatsiooni käsitletakse esmataseme turbekontrollina. Iga autentitud identiteet kannab organisatsiooni identifikaatorit ja andmepäringud piiritletakse selle organisatsiooniga. Kui kasutaja taotleb kirjet, mis kuulub teisele organisatsioonile, tagastab platvorm vastuse „not found", selle asemel et paljastada kirje olemasolu. Sisemisi andmebaasi identifikaatoreid ei eksponeerita kunagi liideses; API esitab kuvatavaid identifikaatoreid ja kaardistab need iga päringu kohta ümber, mis eemaldab levinud organisatsioonidevahelise loendusründe klassi.

See ei ole ainult arhitektuuriline kavatsus. Nagu kirjeldatud jaotises 12, käitab meie automatiseeritud komplekt ulatuslikku organisatsioonidevahelist maatriksit, mis üritab jõuda ühe organisatsiooni andmeteni teise organisatsiooni mandaatidega ning kontrollib, et kõik sellised katsed ebaõnnestuvad.

## 6.4 Programmiliselt kasutatav juurdepääs

Integratsioonide jaoks saavad sobivatel plaanidel olevad organisatsioonid väljastada API võtmeid. Võtmetel on äratuntav prefiks, 128 bitti entroopiat ning neid salvestatakse ainult räsina; toorvõti kuvatakse loomisel üks kord ja mitte kunagi enam. Igal võtmel on selgesõnaline õigusskoop (lugemine, kirjutamine või ATS integratsioon), seda saab piirata konkreetsete lähtevõrkudega, seda saab koheselt tühistada ning sellele rakenduvad võtmepõhised kiirusepiirangud, mis tulenevad organisatsiooni plaanitasemest. Võtme verifitseerimine kasutab ajastussõltumatut võrdlust, et vältida teabe lekkimist vastuse ajastuse kaudu.

# 7. Rakendusturvalisus

Rakendus on kirjutatud nii, et eemaldada terveid haavatavuse kategooriaid, mitte parandada neid üksikjuhtumite kaupa.

- **Injection.** Kogu andmebaasipääs käib läbi object-relational mapper'i parameetriseeritud päringutega. Koodibaasis puudub toore stringivormindusega SQL. See kõrvaldab struktuurselt SQL injection'i.
- **Sisendi valideerimine.** Iga päringu keha valideeritakse range skeemi vastu enne äriloogikani jõudmist. Liiga suured koormused lükatakse tagasi ja loendi lõpp-punktid on lehekülgendatud, et piirata ressursikasutust.
- **Väljundkodeerimine ja cross-site scripting.** Kasutaja sisestatud ja AI loodud teksti käsitletakse ebausaldusväärsena. Kui sisu tuleb renderdada HTML-ina, läbib see kirjutamise ajal lubatud loendi põhise puhastuse ning spetsiaalne testikomplekt kinnitab, et script-tagid, event handler'id ja javascript URL-id eemaldatakse.
- **Mass assignment.** Uuendustoimingud kasutavad selgesõnalisi skeeme, mis välistavad privilegeeritud väljad nagu roll, organisatsioon ja krediidijääk, seega ei saa klient lisavälju postitades õigusi eskaleerida.
- **Kiiruse piiramine.** Autentimise ja kuritarvitamisele kalduvad lõpp-punktid on piiratud püsiva, andmebaasipõhise limiter'iga, mis elab taaskäivitused üle ja töötab korrektselt mitme rakendusinstantsi vahel. Sisselogimisel, registreerimisel, parooli lähtestamisel ja verifitseerimise uuestisaatmisel on kõigil oma piirangud. Kliendi IP lahendamine on tugevdatud forwarding header'ite võltsimise vastu.
- **Webhookid.** Sissetulevad webhookid makse- ja e-posti teenusepakkujatelt verifitseeritakse teenusepakkuja allkirjade vastu toorpäringu kehal enne töötlemist.
- **Failiüleslaadimised.** Üleslaadimistele on kehtestatud mahu ülempiir, neid valideeritakse, need salvestatakse genereeritud identifikaatorite alla, mitte kasutaja antud nimedega, ning neid piiratakse nii päringu kui organisatsiooni lõikes.
- **Turbepealkirjad.** Tootmiskeskkonnas sisaldavad vastused strict transport security, content-type ja frame options, referrer policy ja piiravat permissions policy't ning peidavad serveri ja raamistiku bännerid.

# 8. Andmekaitse

## 8.1 Krüpteerimine

Kõik andmed on puhkeolekus krüpteeritud AES-256 abil Azure platvormi salvestus- ja andmebaasikrüpteerimise kihtides. Kogu võrguliiklus teenindatakse eranditult üle HTTPS kasutades TLS 1.2 või kõrgemat; lihttekstiline HTTP suunatakse igal tasandil HTTPS-ile ümber. Tootmiskeskkonnas väljastavad API ja veebiportaal strict transport security päiseid koos tugevdamispäiste kogumiga ning peidavad serveri ja raamistiku versioonibännerid.

## 8.2 Saladuste haldus

Rakenduse saladusi hoitakse tsentraliseeritud saladuste hoidlas, kus on purge protection lubatud ja üheksakümnepäevane soft-delete aken. Rakendused autentivad Azure ressurssidele süsteemi määratud managed identities kaudu, mitte pikaealiste võtmetega; näiteks privaatsel salvestusel on shared access keys täielikult keelatud, seega on juurdepääs võimalik ainult identiteedipõhiste rollimäärangute kaudu, mis on piiritletud üksikule ressursile. Hoidla juurdepääsupoliitikad annavad rakenduse põhiosalistele ainult lugemisõiguse konkreetsetele saladustele, mida nad vajavad, järgides vähimate õiguste põhimõtet.

## 8.3 Andmeresidentsus

Kõik kliendi- ja kandidaadiandmed salvestatakse ja töödeldakse Euroopa Liidus. Rakenduse majutus, andmebaas, salvestus, vahemälu ja saladused asuvad West Europe piirkonnas ning AI töötlus toimub EL piirkondades. AI teenusepakkuja ei kasuta kliendiandmeid oma mudelite treenimiseks.

## 8.4 Ühe intervjuu elutsükkel

Kõige selgem viis andmekaitsekontrollide mõistmiseks on jälgida ühte intervjuud algusest lõpuni. Nõusolek kogutakse ja registreeritakse enne mis tahes töötlemist. Üleslaadimine krüpteeritakse edastusel. Transkriptsioon ja analüüs toimuvad EL andmekeskustes. Tulemused kirjutatakse krüpteeritud salvestusse. Iga kirjet juhib seejärel üksainus säilitamistähtaeg, mis lõpeb logitud kaskaadkustutusega. Igal hetkel võivad kandidaadi õigused, nagu tagasivõtmine, kustutamine, juurdepääs või ülekantavus, selle voo katkestada.

# 9. Privaatsus disaini kaudu ja GDPR

Privaatsus on sisse ehitatud andmemudelisse ja töövoogu, mitte lisatud üksnes poliitikaga.

## 9.1 Nõusolek

Ühtegi intervjuud ei salvestata ega analüüsita ilma kandidaadi selgesõnalise nõusolekuta. Kui kandidaat lisatakse värbamisse, väljastab platvorm e-posti teel unikaalse ühekordse nõusolekulingi. Kandidaat vaatab üle, mis juhtuma hakkab, ja kas nõustub või keeldub. Nõusoleku olek, sealhulgas vastamise aeg, salvestatakse selle konkreetse värbamise juurde, seega on nõusolek alati seotud konkreetse värbamisprotsessiga, mitte ei ole antud üldiselt.

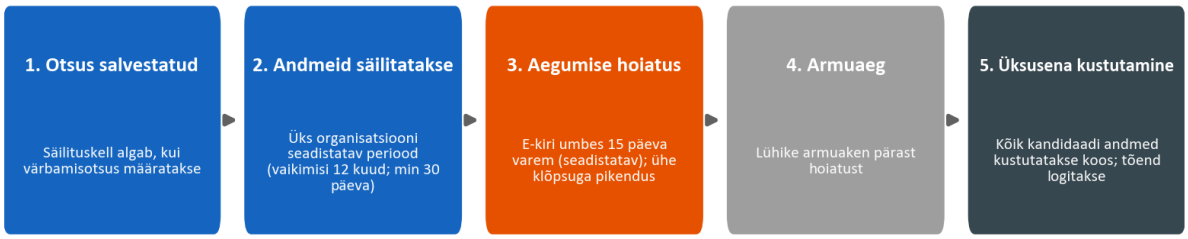
**Kandidaadi nõusolek: selge ja salvestatud enne igasugust töötlust**


## 9.2 Säilitamine ja kustutamine

Andmete säilitamine on organisatsioonipõhiselt seadistatav, vaikeväärtusega kaksteist kuud ja seadistatava miinimumiga kolmkümmend päeva, ning seda saab kandidaadipõhiselt üle kirjutada. Kandidaadi andmetel on üksainus säilitamistähtaeg, mitte eraldi taimer iga artefakti jaoks. Tähtaeg algab, kui värbamisotsus registreeritakse. Enne andmete aegumist saadab platvorm hoiatuse (vaikimisi umbes viisteist päeva ette) ja pakub ühe klõpsuga pikendust. Kui andmed kustutatakse, kustutatakse need ühe üksusena: kandidaadi kirje, intervjuud, transkriptid, helisalvestised, dokumendid ja võrdlused eemaldatakse kõik koos ning kustutamine registreeritakse auditilogis. Osalist või orvuks jäänud jääki ei jää.

Allolev elutsükkel näitab seda ühte taimerit ja seda, kuidas see koondub üheks kaskaadkustutuseks koos logitud kustutamistõendiga.

**Andmesäilitus: üks kell kandidaadi kohta, üksusena kustutamine**




## 9.3 Andmesubjekti õigused ja alamvolitatud töötlejad

Platvorm toetab GDPR alusel nõutavaid andmesubjekti õigusi, sealhulgas juurdepääsu, kustutamist, ülekantavust, vastuväidet ja selgitust. Töötlemine toimub andmetöötluslepingu alusel, mille kliendid aktsepteerivad registreerimisel ja mis on versioonitud organisatsiooni kohta. Meie alamvolitatud töötlejad ja nende rollid, kõik EL-is või asjakohaste kaitsemeetmete all, on selles

lepingus avalikustatud ning kliendid saavad iga muudatuse kohta ette teatise. Jaotis 17 sisaldab alamvolitatud töötlejate registrit ja artiklipõhist vastavuskaardistust.

# 10. Vastutustundlik AI ja EU AI Act

Platvorm kuulub EU AI Act alusel kõrge riskiga kategooriasse, kuna toetab töölevõtmise otsuseid, ja me käsitleme seda klassifikatsiooni tõsiselt.

Toote määrav reegel on, et **AI on otsustustugi, mitte otsustaja.** Süsteem ei võta kandidaati kunagi automaatselt vastu ega lükka tagasi. See transkribeerib kõnet, struktureerib küsimusi ja vastuseid, hindab vastuseid värbaja määratletud kriteeriumide järgi ning koostab tagasiside mustandeid, ja inimene vaatab iga väljundi üle enne selle kasutamist. See hoiab inimese kindlalt protsessis.

Sama oluline on see, mida AI ei tee. See ei hinda isiksust, „kultuurilist sobivust", emotsionaalset seisundit, hääletooni, aktsenti, sugu, vanust, etnilist päritolu, välimust ega kehakeelt. Hindamine on seotud transkripti tõendusmaterjali ja värbaja määratletud kriteeriumidega ning kandidaatide nimed jäetakse hindamise sisendist välja, et vähendada kallutatust. Avaldame läbipaistvuskaardi, kasutajadokumentatsiooni ja vastavusdeklaratsiooni, mis kirjeldavad süsteemi, selle piiranguid ja kaitsemeetmeid.

| Vastutustundliku AI kontroll | Kuidas see toimib |
|---|---|
| Inimene protsessis | Iga skoor ja iga tagasiside osa vaadatakse enne kasutamist värbaja poolt üle |
| Puuduvad automaatsed otsused | Süsteem ei võta kandidaati kunagi automaatselt vastu ega lükka tagasi |
| Tõenduspõhine hindamine | Skoorid viitavad transkripti toetavale tõendusmaterjalile |
| Kallutatusevastane disain | Nimed jäetakse hindamisest välja; sisu hinnatakse stiilist kõrgemalt |
| Ulatuspiirangud | Isiksust, emotsiooni, aktsenti ja kaitstud tunnuseid ei hinnata kunagi |
| Kandidaaditagasiside ohutus | Privaatne kandidaaditagasiside läbib loomise ja valideerimise turvapiirde |

Neid piiranguid ei ole ainult dokumentatsioonis kirjeldatud; need on kodeeritud AI prompt-kihis ja neid kontrollib spetsiaalne AI-ohutuse testiprogramm, mida kirjeldatakse jaotises 12.3.

# 11. Turvaline arendustsükkel

Turvalisus jõustatakse tarkvara ehitamise ja väljastamise viisis, mitte ainult töötavas süsteemis.

• **Keskkondade eraldatus.** Arendus ja tootmine on täielikult eraldi, kummalgi oma infrastruktuur, salvestuskontod, andmebaas, saladused ja alamdomeenid. Jagatud olekut ei ole.

• **Infrastructure as code.** Kogu pilvekeskkond on määratletud koodina ja läbi vaadatud koodina, mis muudab turbehoiaku auditeeritavaks ja reprodutseeritavaks. Hindaja saab täpselt lugeda, millised pordid on avatud, millised ressursid on privaatsed ja millistel identiteetidel millised õigused on.

• **Fikseeritud ja piiratud juurutused.** Iga samm continuous-integration torujuhtmes on seotud täpse muutumatu versiooniga. Tootmisjuurutused on sildipõhised, toimuvad ainult kaitstud tootmistorujuhtme kaudu ja on kohustusliku heakskiidu taga. Automatiseeritud testide komplekt toimib väljastusväravana: juurutust ei saa väljastada, kui testid ebaõnnestuvad.

• **Sõltuvuste hügieen.** Automatiseeritud sõltuvuste jälgimine pakub iganädalaselt uuendusi backendile, töölauarakendusele, veebile, infrastruktuurile ja torujuhtme määratlustele ning sõltuvuste auditid on osa meie perioodilisest turbeülevaatusest.

• **Allkirjastatud artefaktid.** Töölauarakenduse paigaldajad on koodiallkirjastatud, nii et kliendid saavad kontrollida, et paigaldatav tarkvara pärineb tõepoolest meilt.

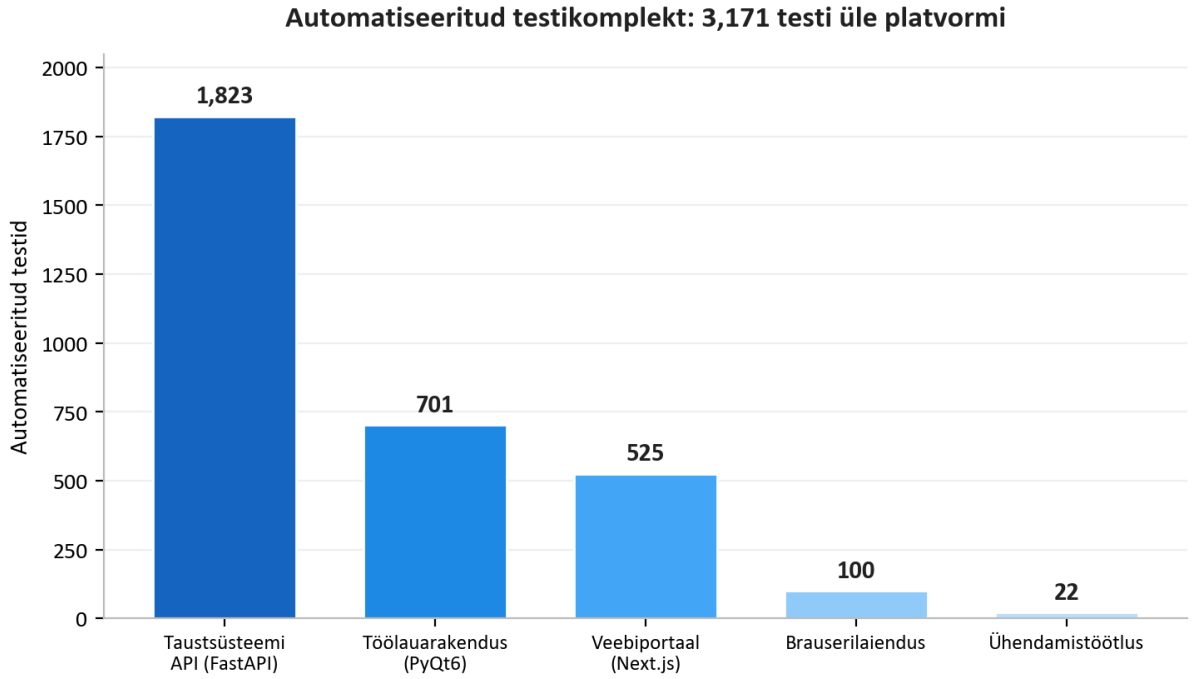
• **Saladuste distsipliin.** Saladused asuvad hoidlas ja kaitstud torujuhtme saladustes, mitte kunagi lähtekoodis.

# 12. Pidev turbetestimine

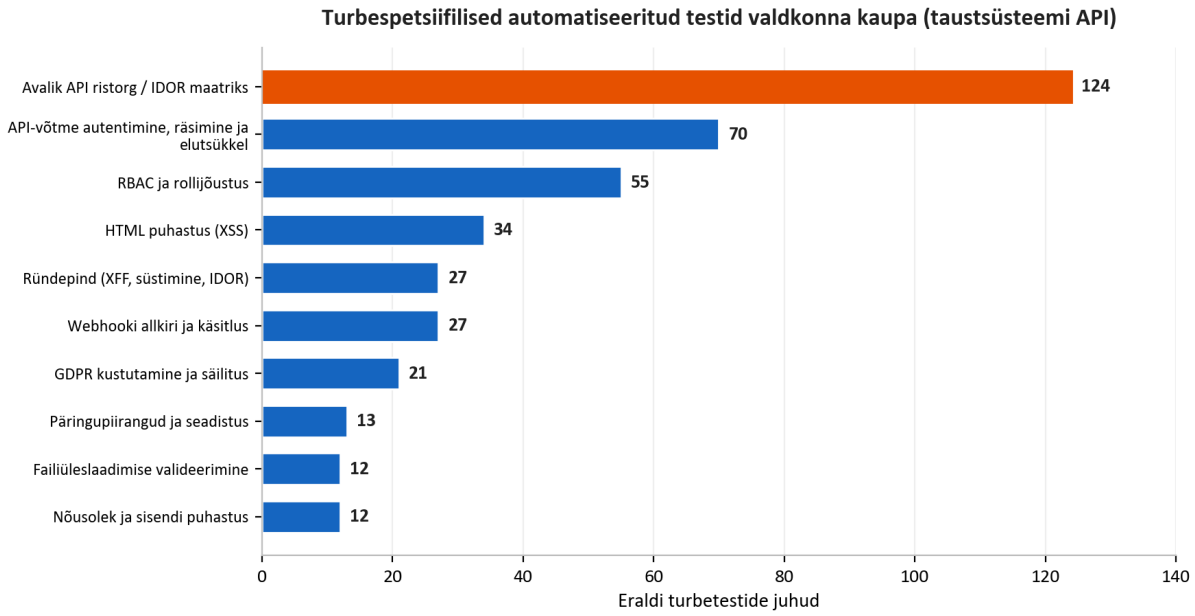
See on meie kindlusloo tuum ja osa, mida enamik teenusepakkujaid ei suuda näidata. Käsitleme turvalisust kui midagi, mida tuleb pidevalt mõõta täidetavate kontrollidega, mitte mida kord väita.

## 12.1 Automatiseeritud testide komplekt

Platvormi katab **3,171 automatiseeritud testi**, mis hõlmavad backend API-t, töölauarakendust, veebiportaali, brauserilaiendit ja heli ühendamise töötluskomponenti.




Need ei ole ainult funktsionaalsed testid. Märkimisväärne eraldi turbetestide komplekt katab selles dokumendis varem kirjeldatud kontrollid. Allolev diagramm jaotab backend API turbespetsiifilised testid valdkondade kaupa.



Paljude teiste hulgas sisaldab see komplekt ulatuslikku avaliku API maatriksit, mis käivitab iga lõpp-punkti õiguspärase kasutajana, organisatsiooni enda API võtmena ja konkureeriva organisatsiooni API võtmena, kontrollides, et kõik organisatsioonidevahelised katsed blokeeritakse. See sisaldab kümneid vastase stiilis ründepinna teste forwarding header'ite võltsimise, päiste süstimise ja identifikaatorite lekke jaoks, sihitud HTML puhastamise komplekti cross-site scripting jaoks, rollijõustuse teste kogu rollimudelile ning teste, mis tõestavad, et kandidaadiandmed kustutatakse päriselt ühe üksusena. Kuna need testid toimivad väljastusväravana, peataks regressioon, mis nõrgestaks mõnd neist kontrollidest, väljastuse enne klientideni jõudmist.

## 12.2 Reaalne penetratsioonitestimine

Automatiseeritud ühiktestid tõestavad, et kontrollid käituvad eraldi korrektselt. Tõestamaks, et need toimivad koos reaalses juurutuses, hoiame korduvkasutatavat penetratsioonitestimise metoodikat, mis käivitab tõelised ründeskriptid töötava keskkonna vastu. See on korraldatud kuude etappi:

| Etapp | Fookus | Näited sellest, mida kontrollitakse |
|---|---|---|
| 1. Staatiline analüüs | Lähtekood | Saladused, süstemustrid, ohtlikud funktsioonid, puuduv autentimine, ebaturvaline HTML |
| 2. Arhitektuuri ülevaatus | Infrastruktuur | Private endpoints, segmentatsioon, TLS, saladuste konfiguratsioon |
| 3. Ründevektorite analüüs | Lähtekoodihoidla ja pilv | Harukaitse, identiteedi ulatus, avalik eksponeeritus |
| 4. Reaalne penetratsioonitestimine | Töötav keskkond | Autentimata sondeerimine, organisatsioonidevaheline juurdepääs, süsted, tokenite muutmine, SSRF, kiirusepiirangu pursked |
| 5. Ettevõtte skoorimine | Küpsus | Kuusteist turbekategooriat hinnatud ettevõtte baasjoone vastu |
| 6. Sõltuvused ja tarneahel | Kolmanda osapoole risk | Sõltuvuste CVE audit, fikseeritud torujuhtme tegevused, lock-file terviklus |

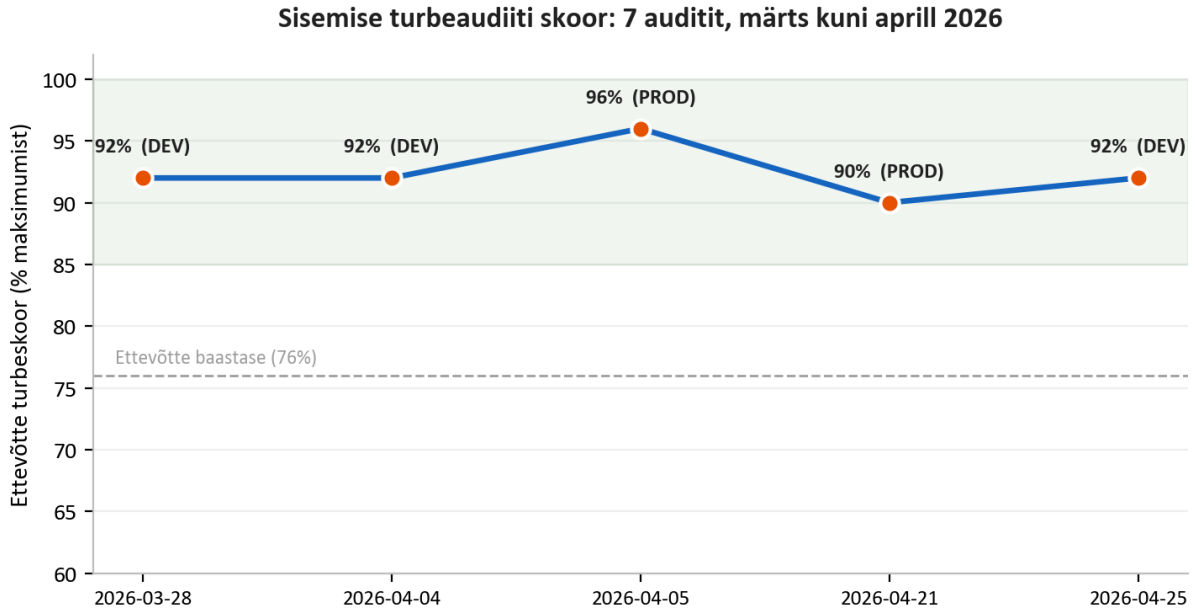
Etapp 4 on tegelik vastase stiilis testimine juurutatud süsteemi vastu, mitte kontrollnimekiri. See proovib kaitstud lõpp-punkte ilma mandaatideta ja kinnitab, et need keelduvad juurdepääsust; registreerib kaks organisatsiooni ja püüab jõuda ühe organisatsiooni kirjeteni teise organisatsiooni kontoga; süstib cross-site-scripting ja server-side-template koormusi ning kinnitab, et need neutraliseeritakse; muudab autentimistokeneid ja kinnitab, et need lükatakse tagasi; proovib server-side request forgery ründeid pilve metadata lõpp-punktide vastu; ning koormab autentimise lõpp-punkte, et kinnitada kiirusepiirangu tegelikku rakendumist töötavas keskkonnas, mitte ainult teoorias.

## 12.3 Kandidaaditagasiside ohutuse testimine

Kuna platvorm võib genereerida kandidaatidele privaatset arengutagasisidet, käitame selle funktsiooni vastu eraldi vastase stiilis ohutusprogrammi. See sisestab süsteemi tahtlikult karmi ja vaenuliku värbajapoolse märkmeid ning kinnitab, et kandidaadile suunatud väljund ei sisalda kunagi vulgaarsust, ei paljasta ega omista kunagi värbaja identiteeti ega eraarvamust ning ei kasuta kunagi hinnangulisi isiksusemärgendeid. See kaitseb nii kandidaati, kes peaks saama konstruktiivset ja lugupidavat tagasisidet, kui klienti, kelle sisemine arvamus ei tohiks kunagi väljapoole lekkida.

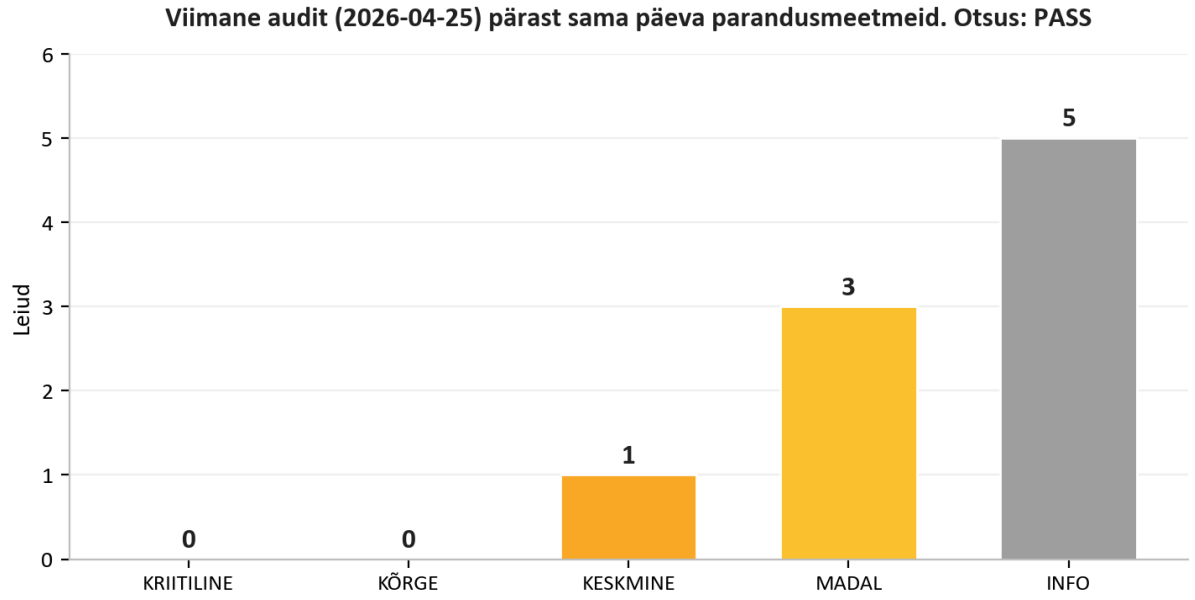
# 13. Turvaauditite tulemused

Viime läbi korduvaid turvaauditeid struktureeritud ja korratava penetratsioonitestimise metoodika abil ning vormistame igaühe kuupäevastatud raportina, kus on raskusastme järgi hinnatud leiud, tõendusmaterjal ja parandusmeetmed. Need on sisemised auditid, mida viib läbi meie enda turbeprotsess; samade kontrollide ametlik kolmanda osapoole sertifitseerimine on meie tegevuskavas. Märtsi lõpu ja aprilli lõpu 2026 vahel lõpetasime **seven such audits** arendus- ja tootmiskeskkondades.




Tulemus, mis potentsiaalsele kliendile kõige rohkem loeb, on järjepidevus: **across all seven audits there were zero critical findings.** Harvadel juhtudel, kui ilmnes kõrgema raskusastmega probleem, parandati see kiiresti, sageli samal päeval, ja verifitseeriti uuesti. Hindamisrubriiki muudeti selle perioodi jooksul teadlikult rangemaks (maksimaalset võimalikku skoori tõsteti, kui lisasime rohkem hinnatavaid kategooriaid), mistõttu normaliseeritud skoori joon püsib kõrge isegi siis, kui latt tõusis.

Meie viimane audit, 25 April 2026, näitab, kuidas protsess praktikas toimib. Tuvastati kaks kõrgema raskusastmega probleemi, mõlemad parandati ja verifitseeriti uuesti samal päeval ning audit lõpetati otsusega **PASS**, ilma et praeguses ohumudelis oleks jäänud ekspluateerimisvalmis probleeme.



| Audit | Keskkond | Critical | Otsus |
|---|---|---|---|
| 2026-03-28 | Arendus | 0 | Tootmiseks valmis |
| 2026-04-04 | Arendus | 0 | Ettevõtteks valmis |
| 2026-04-05 | Tootmine | 0 | Ettevõtteks valmis |
| 2026-04-20 | Arendus | 0 | Tootmiseks valmis, märkused |
| 2026-04-20 | Arendus | 0 | Läbitud märkustega |
| 2026-04-21 | Tootmine | 0 | Ohutu, ekspluateeritavaid leide pole |
| 2026-04-25 | Arendus | 0 | Läbitud |

Muster nende auditite lõikes on kõige ausam tõendus, mida saame pakkuda: probleeme leitakse, sest me otsime neid põhjalikult, ja need suletakse kiiresti, sest protsess on ehitatud nende sulgemiseks. Teenusepakkuja, kes ei raporteeri kunagi ühtegi leidu, on tavaliselt teenusepakkuja, kes ei otsi.

# 14. Töökindlus ja jagatud vastutus

## 14.1 Seire ja logimine

Rakenduse ja platvormi telemeetria suunatakse tsentraliseeritud log analytics tööruumi ja rakenduse seireteenusesse, andes meile nähtavuse saadavuse ja käitumise üle. Tundlikud toimingud, nagu andmete kustutamine, õiguslike kokkulepete aktsepteerimine ja AI kutsed, salvestatakse spetsiaalsetesse audititabelitesse, nii et on olemas püsiv jälg selle kohta, kes mida oluliste andmetega tegi.

## 14.2 Varundus ja taastamine

Hallatud andmebaas säilitab automatiseeritud varukoopiaid ning privaatne salvestus on kaitstud soft-delete säilitusega nii blobide kui konteinerite tasemel, seega saab juhuslikku või pahatahtlikku kustutamist säilitamisakna jooksul taastada. Kriitilisel infrastruktuuril on kustutuslukud, et vältida tootmisressursside juhuslikku mahavõtmist.

## 14.3 Jagatud vastutuse kokkuvõte

| Valdkond | AI Interview Analyzer | Klient |
|---|---|---|
| Infrastruktuur, võrk, paikamine | Jah | - |
| Rakendusturvalisus ja AI torujuhe | Jah | - |
| Krüpteerimine, saladused, andmeresidentsus | Jah | - |
| Kasutajate ja rollide haldus | Pakub kontrolle | Haldab kasutajaid ja rolle |
| Säilitamispoliitika seadistamine | Pakub kontrolle | Määrab säilitamisakna |
| Kandidaadi nõusolek | Pakub töövoogu | Tagab selle kasutamise |
| Tugevad lõppkasutaja mandaadid ja SSO | Toetab SSO-d ja poliitikaid | Jõustab sisepoliitikat |

# 15. Ohumudel ja OWASP kaardistus

Me kavandame kaitset konkreetse vastaste hulga vastu: väline ründaja ilma mandaatideta, ühe organisatsiooni uudishimulik või pahatahtlik autentitud kasutaja, kes proovib jõuda teise organisatsiooni andmeteni, kompromiteeritud sõltuvus ja sisemine eksimus. Allolev tabel kaardistab laialdaselt kasutatavad OWASP Top 10 riskikategooriad konkreetsete kontrollidega, mis neid selles platvormis maandavad, ja igaüht neist katab jaotises 12 kirjeldatud testimine.

| OWASP risk | Kuidas platvorm seda maandab |
|---|---|
| Katkine juurdepääsukontroll | Rollipõhine juurdepääsukontroll igal privilegeeritud lõpp-punktil; organisatsioonipõhine skoopimine; „not found" organisatsioonidevahelisel juurdepääsul; identifikaatorite ümberkaardistus; organisatsioonidevaheline testmaatriks |
| Krüptograafilised rikked | TLS 1.2+ edastusel; AES-256 puhkeolekus; bcrypt parooliräsi; saladused hallatud hoidlas |
| Injection | Ainult ORM-põhised parameetriseeritud päringud; range skeemivalideerimine; HTML puhastus kirjutamise ajal |
| Ebaturvaline disain | Kihiline mitmekihiline kaitse; ohumudeldamine ja arhitektuuri ülevaatus igas auditis |
| Turbekonfiguratsiooni vead | Infrastructure as code; vaikimisi-keelatud võrgurühmad; turbepealkirjad; keelatud jagatud salvestusvõtmed; API skeem ei ole tootmises avalikustatud |
| Haavatavad komponendid | Iganädalane automatiseeritud sõltuvuste jälgimine; sõltuvuste CVE auditid perioodilises ülevaatuses |
| Identifitseerimise ja autentimise rikked | Lühiealised tokenid; kiirusepiiranguga sisselogimine; e-posti verifitseerimine; SSO tugi; puuduvad lihttekstparoolid |
| Tarkvara ja andmete tervikluse rikked | Fikseeritud muutumatud torujuhtmesammud; allkirjastatud töölauapaigaldajad; webhooki allkirja verifitseerimine; sildiga piiratud tootmisjuurutused |
| Turbelogimise ja seire rikked | Tsentraliseeritud telemeetria; spetsiaalsed audititabelid tundlike toimingute jaoks |
| Server-side request forgery | Väljuvad kutsed piiratud usaldatud lõpp-punktidega; SSRF katsed penetratsioonitestimise raamistikus |

See kaardistus on meie kindlusargumendi selgroog: iga tuntud ründeklassi jaoks on olemas nimetatud kontroll ja iga nimetatud kontrolli jaoks on olemas test.

# 16. Haavatavuste haldus ja vastutustundlik avalikustamine

Turvalisus ei saa kunagi valmis, seega töötame pidevas avastamise ja parandamise tsüklis.

- **Avastamine.** Haavatavused tulevad esile neljast allikast: automatiseeritud testide komplekt, korduvad penetratsioonitestide auditid, automatiseeritud sõltuvuste jälgimine ning klientide või uurijate raportid.
- **Triaaž.** Igale leiule määratakse raskusaste (critical, high, medium, low või informational) koos tõendusmaterjali ja parandusvastutajaga, täpselt nii nagu meie auditiraportites kirjas.
- **Paranduse sihttähtajad.** Critical ja high leiud prioriseeritakse koheseks parandamiseks; meie auditiajaloos on kõrgema raskusastmega leiud tavaliselt lahendatud ja uuesti verifitseeritud samal päeval. Medium ja madalama taseme leiud planeeritakse regulaarse hooldustsükli sisse.
- **Verifitseerimine.** Parandusi testitakse uuesti ning vajaduse korral tehakse töötava keskkonna vastu reaalne kontroll, et kinnitada probleemi tegelik sulgemine, mitte ainult koodis sulgemine.
- **Avalikustamine.** Turbeprobleemidest saab meile otse teatada. Kinnitame raporti kättesaamist, uurime selle läbi ja hoiame teatlejat lahenduseni kursis.

# 17. Vastavuskaardistus

## 17.1 GDPR

| GDPR valdkond | Platvormi rakendus |
|---|---|
| Õiguslik alus (Art. 6) | Kandidaadi selgesõnaline nõusolek kogutakse enne töötlemist |
| Andmete minimeerimine ja säilitamise piirang (Art. 5) | Töödeldakse ainult intervjuuga seotud andmeid; seadistatav säilitamine automaatse kustutamisega |
| Õigus kustutamisele (Art. 17) | Kõigi kandidaadiandmete ühe üksuse kustutamine koos logitud kustutamistõendiga |
| Andmesubjekti õigused (Art. 15 kuni 20) | Toetatud on juurdepääs, kustutamine, ülekantavus ja vastuväide |
| Töötleja kohustused (Art. 28) | Andmetöötlusleping aktsepteeritakse registreerimisel ja versioonitakse organisatsiooni kohta |
| Töötlemise turvalisus (Art. 32) | Krüpteerimine, juurdepääsukontroll, isolatsioon ja pidev testimine, nagu selles dokumendis kirjeldatud |
| Alamvolitatud töötlejate läbipaistvus | Avalikustatud andmetöötluslepingus koos muudatuste etteteatamisega |

## 17.2 EU AI Act

Platvormi käsitletakse kõrge riskiga AI süsteemina, mis toetab töölevõtmise otsuseid, ning me hoiame regulatsiooniga kooskõlas dokumentatsiooni, sealhulgas läbipaistvuskaarti, kasutajadokumentatsiooni ja vastavusdeklaratsiooni. Põhilised kaitsemeetmed, inimjärelevalve, läbipaistvus, tõenduspõhine hindamine ja ranged piirangud sellele, mida AI hindab, on kirjeldatud jaotises 10. Jätkame ametliku vastavusdokumentatsiooni küpsuse tõstmist, kui regulatsiooni rakendamise ajajoon edeneb.

## 17.3 Majutuse sertifikaadid

Platvorm töötab täielikult Microsoft Azure peal, mille andmekeskustel on sõltumatud sertifikaadid, sealhulgas ISO 27001 ja SOC 2. Need sertifikaadid katavad füüsilise ja platvormikihi meie rakenduse all; rakendustaseme kontrollid on need, mida on kirjeldatud kogu selles dokumendis.

## 17.4 Alamvolitatud töötlejate register

| Alamvolitatud töötleja | Eesmärk | Piirkond |
|---|---|---|
| Microsoft Azure | Majutus, AI ja kõnetöötlus, salvestus, tehingulised e-kirjad | EL (West Europe, Sweden Central) |
| Stripe | Tellimuste ja maksete töötlemine | EL (Ireland) |
| Fakturownia | Arveldamine | EL (Poland) |
| ATS connector (optional) | Kandidaadihalduse integratsioon, lubatud ainult taotlusel | EL |

# 18. Turvalisuse tegevuskava

Käsitleme turvalisust kui pidevalt täiustatavat programmi. Meie tegevuskavas olevad praegused algatused hõlmavad mitmetegurilise autentimise valikute tugevdamist administratiivsete kontode jaoks, andmepääsu tsentraliseeritud auditilogimise laiendamist, sõltuvuste ajakohasuse regulaarset täiendavat karmistamist ning selles dokumendis kirjeldatud kontrollide ametliku kolmanda osapoole sertifitseerimise edendamist. Ükski neist ei ole lünk, mis täna kliendiandmeid paljastaks; igaüks neist on täiustus juba kihilisele turbehoiakule.

# 19. Kokkuvõte

AI Interview Analyzer kaitseb kandidaadi- ja kliendiandmeid kihilise arhitektuuri kaudu: vaikimisi privaatne võrk ilma avalike andmeteenusteta, tugev identiteedihaldus ja organisatsioonipõhine isolatsioon, rakenduskood, mis eemaldab terveid haavatavusklasse, krüpteerimine ja EL andmeresidentsus ning andmemudelisse sisse ehitatud privaatsuskontrollid. Platvormi eristab nende väidete taga olev tõendusmaterjal. 3,171 automatiseeritud testi, korratava reaalse penetratsioonitestimise metoodika, spetsiaalse AI-ohutusprogrammi ja seitsme sisemise turvaauditiga, milles oli zero critical findings, suudame näidata, mitte ainult öelda, et platvorm on turvaline.

# Lisa A: Turbekontrollide kataloog

Kokkusurutud viide peamistele kontrollidele ja neid toetavale tõendusmaterjalile.

| Kontroll | Mehhanism | Tõendus |
|---|---|---|
| Edastuskrüpteerimine | Ainult HTTPS, TLS 1.2+, HTTP ümber suunatud | Infrastructure as code; arhitektuuriaudit |
| Krüpteerimine puhkeolekus | AES-256 platvormikrüpteerimine salvestusel ja andmebaasis | Platvormi konfiguratsioon; arhitektuuriaudit |
| Paroolikaitse | bcrypt koos paroolipõhise soolaga | Lähtekoodihoidla; autentimistestid |
| Seansihaldus | 30-minutilised allkirjastatud tokenid, tühistatav serveripoolne värskendus | Lähtekoodihoidla; autentimistestid |
| Autoriseerimine | Nelja rolliga juurdepääsukontroll privilegeeritud lõpp-punktidel | Rollijõustuse testikomplekt |
| Rentnike isolatsioon | Organisatsioonipõhine päringute skoopimine; 404 organisatsioonidevahelisel juurdepääsul | Organisatsioonidevaheline testmaatriks |
| API võtmete turvalisus | Räsi kujul salvestus, skoopitud õigused, võtmepõhised kiirusepiirangud | API võtmete testikomplekt |
| Injection kaitse | Ainult ORM-põhised parameetriseeritud päringud | Staatiline analüüs; injection testid |
| Cross-site scripting kaitse | HTML puhastus kirjutamise ajal | HTML puhastamise testikomplekt |
| Kiiruse piiramine | Püsiv andmebaasipõhine limiter autentimise lõpp-punktidel | Kiirusepiirangu testid; reaalajas purskekontrollid |
| Webhooki terviklus | Teenusepakkuja allkirja verifitseerimine toorkehal | Webhooki testikomplekt |
| Saladuste haldus | Hallatud hoidla, purge protection, managed identity | Infrastructure as code; arhitektuuriaudit |
| Võrgu isolatsioon | Private endpoints; vaikimisi-keelatud segmentatsioon | Infrastructure as code; arhitektuuriaudit |
| Andmete kustutamine | Ühe üksuse kaskaadkustutamine auditilogiga | GDPR kustutamise testikomplekt |
| Tarneahel | Fikseeritud torujuhtmesammud; iganädalane sõltuvuste jälgimine | Torujuhtme konfiguratsioon; sõltuvuste audit |

# Lisa B: Korduma kippuvad küsimused turvahindajatele

**Kus meie andmeid hoitakse?** Täielikult Euroopa Liidus, Microsoft Azure peal, West Europe piirkonnas ning AI töötlusega EL piirkondades. Kandidaadiandmed ei lahku kunagi EL-ist.

**Kas meie andmeid kasutatakse AI mudelite treenimiseks?** Ei. AI teenusepakkuja ei kasuta kliendiandmeid treenimiseks.

**Kas andmebaas on internetist kättesaadav?** Ei. Avalik võrgupääs on keelatud ja andmebaas on kättesaadav ainult private endpoint kaudu virtuaalvõrgu sees.

**Kas üks klient saab näha teise kliendi andmeid?** Ei. Iga päring on piiratud kutsuja organisatsiooniga, organisatsioonidevaheline juurdepääs tagastab vastuse „not found" ning automatiseeritud maatriks testib seda isolatsiooni pidevalt.

**Kuidas paroole salvestatakse?** Räsi kujul bcrypt abil ja unikaalse paroolipõhise soolaga. Toetatud on single sign-on Microsofti ja Google'iga; sellisel juhul parooli ei salvestata.

**Kas toetate single sign-on'i?** Jah, Microsofti ja Google OAuth kaudu.

**Kui kaua access tokenid kehtivad?** Kolmkümmend minutit, koos tühistatava serveripoolse refresh seansiga, mis invalideeritakse väljalogimisel.

**Kuidas kandidaadi nõusolekut hallatakse?** Iga kandidaat saab unikaalse ühekordse nõusolekulingi ja peab nõustuma enne mis tahes salvestamist või analüüsi. Nõusolek salvestatakse konkreetse värbamisprotsessi juurde.

**Kuidas andmeid kustutatakse?** Ühe üksusena, hõlmates kandidaadi kirjet, intervjuusid, transkripte, heli, dokumente ja võrdlusi, seadistatava säilitamiskava alusel, koos logitud kustutamistõendiga. Kandidaadid võivad taotleda kustutamist ka otse.

**Kas teil on andmetöötlusleping?** Jah, see aktsepteeritakse registreerimisel ja versioonitakse organisatsiooni kohta, sealhulgas alamvolitatud töötlejate register.

**Kas AI teeb värbamisotsuseid?** Ei. See pakub ainult otsustustuge; inimene vaatab iga väljundi üle ja teeb kõik otsused.

**Kuidas te oma turvaväiteid tõendate?** 3,171 automatiseeritud testi kaudu, sealhulgas spetsiaalne turbetestide komplekt, korratav kuueetapiline penetratsioonitestimise metoodika töötavate keskkondade vastu, AI-ohutuse testiprogramm ja korduvad kirjalikud auditiraportid.

**Mis juhtub, kui leiate haavatavuse?** Sellele määratakse raskusaste koos tõendusmaterjali ja vastutajaga, see parandatakse prioriteedikava järgi, verifitseeritakse uuesti, sealhulgas vajaduse korral töötavas keskkonnas, ning registreeritakse auditiraportis.

**Kas me saame teha oma penetratsioonitesti?** Turvahinnanguid saab korraldada teie kontohalduri kaudu sobiva ulatuse ja ajastusega.

---

# Lisa C: Sõnastik

| Mõiste | Tähendus |
|---|---|
| AES-256 | Tugev sümmeetriline krüpteerimisstandard, mida kasutatakse puhkeolekus andmete kaitsmiseks |
| bcrypt | Eriotstarbeline parooliräsifunktsioon paroolipõhise soolamisega |
| Managed identity | Platvormi väljastatud identiteet, mis võimaldab teenusel autentida ilma salvestatud võtmeteta |
| Private endpoint | Privaatne võrguaadress, mis hoiab pilveteenuse avalikust internetist eemal |
| Network security group | Lubamis- ja keelureeglite kogum, mis filtreerib alamvõrgu võrguliiklust |
| RBAC | Roll-based access control ehk rollipõhine juurdepääsukontroll, mis annab õigused vastavalt kasutaja rollile |
| IDOR | Insecure direct object reference, juurdepääsukontrolli viga, mille vastu platvorm kaitseb |
| SSRF | Server-side request forgery, ründeklass, mida meie penetratsioonitestides sondeeritakse |
| Web application firewall | Servakontroll, mis filtreerib pahatahtlikku veebiliiklust |
| Data processing agreement | Leping, mis reguleerib, kuidas töötleja käsitleb isikuandmeid vastutava töötleja nimel |

# Lisa D: Kontakt ja dokumendihaldus

**AI Interview Analyzer Sp. z o.o.**

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

NIP: 5253079974

Turvahindamise, meie andmetöötluslepingu koopia või meie EU AI Act vastavusdokumentatsiooni saamiseks võtke palun ühendust oma kontohalduriga.

*See dokument kirjeldab AI Interview Analyzer teenuse turbehoiakut jaluses näidatud genereerimiskuupäeva seisuga. See on esitatud hindamise eesmärgil ega moodusta ühegi lepingu osa. Konkreetsed lepingulised turvakohustused on sätestatud kohaldatavas lepingus ja andmetöötluslepingus.*