7. NODARBĪBA

Datu aizsardzība, ētika un atbildīga AI izmantošana HR procesos

- GDPR un sensitīvie dati
- Algoritmiskā neobjektivitāte
- AI riski un caurspīdīgums
- Profesionālā atbildība

ERASMUS+ projekts Nr. 2024-2-LV01-KA210-VET-000280127

Finansē Eiropas Savienība. Tomēr paustie uzskati un viedokļi ir tikai autora(-u) uzskati un viedokļi un ne vienmēr atspoguļo Eiropas Savienības vai Valsts izglītības attīstības aģentūras (VIAA) uzskatus un viedokļus. Ne Eiropas Savienību, ne piešķīrēju iestādi (VIAA) nevar saukt pie atbildības par tiem.
Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or The State Education Development Agency (hereinafter – VIAA). Neither the European Union nor the granting authority (VIAA) can be held responsible for them.

Prof. Mg. sc. soc. Kristīna Buluševa

ĪSUMĀ: KO ESAM APGUVUŠI IEPRIEKŠĒJĀ NODARBĪBĀ?

01

HR KPI un rādītāji

Headcount, mainība, time/cost to hire, iesaiste, ROI.

02

Atskaites un dashboardi

Operatīvais, taktiskais, stratēģiskais līmenis. Power BI, Tableau, Looker.

03

AI HR analītikā

Prognozēšana, risku noteikšana, sentimentu analīze un AI atskaites.

Šodien: no datu izmantošanas pie datu aizsardzības, ētikas un atbildības

ŠODIEN

7. nodarbības saturs

GDPR HR procesos

Tiesiskie pamati, darbinieku tiesības, sensitīvu datu apstrāde

AI riski un ētika

Algoritmiskā neobjektivitāte, caurspīdīgums un cilvēka kontrole

Profesionālā atbildība

Reputācijas riski, dokumentēšana un atbildīga lēmumu pieņemšana

Noslēguma pārbaudījums

Kompleksa praktiskā darba prasības un vērtēšanas kritēriji









ATBILDĪGA DATU PĀRVALDĪBA HR VIDĒ

Sensitīvu datu aizsardzība un atbildīga AI izmantošana

20 M €

GDPR sods var sasniegt līdz 20 miljoniem EUR vai 4% no uzņēmuma gada apgrozījuma

POLITIKAS

Daudzos uzņēmumos AI pārvaldības un lietošanas politika vēl nav izstrādāta

INFORMĀCIJA

Darbiniekiem trūkst skaidras informācijas par savu datu izmantošanu

NEOBJEKTIVITĀTE

AI atlases sistēmās var parādīties algoritmiskā neobjektivitāte

Avoti: GDPR Regula (ES) 2016/679 Art. 83; IBM Global AI Adoption Index; Harvard Business Review; Stanford AI Index; Fairness and Bias in Algorithmic Hiring Research

GDPR PAMATPRINCIPI HR DARBĀ

Seši pamatprincipi drošai datu apstrādei HR procesos

1 Tiesiskums un caurspīdīgums

Apstrādei nepieciešams skaidrs juridiskais pamats

2 Mērķa ierobežojums

Datus drīkst izmantot tikai tiem mērķiem, kas iepriekš norādīti

3 Datu minimizācija

Vākt tikai tik datu, cik patiešām nepieciešams konkrētam mērķim

4 Precizitāte

Dati jāuztur aktuāli un, ja nepieciešams, jālabo vai jādzēš

5 Glabāšanas ierobežojums

Datus glabā tikai tik ilgi, cik tas patiešām nepieciešams

6 Integritāte un drošība

Datu aizsardzība pret nesankcionētu piekļuvi, noplūdi vai zaudēšanu

SENSITĪVIE DATI HR VIDĒ

Īpašas personas datu kategorijas ar paaugstinātu aizsardzības līmeni

Sensitīvie dati

- Veselības dati un slimības lapas
- Reliģiskā vai filozofiskā pārliecība
- Politiskie uzskati
- Rasu vai etniskā izcelsme
- Seksuālā orientācija un dzimumidentitāte
- Biometriskie dati
- Dalība arodbiedrībā

Apstrādes prasības

- Skaidra un nepārprotama piekrišana
- Šifrēta datu glabāšana un pārsūtīšana
- Stingri ierobežota piekļuve
- Datu apstrādes uzskaite un audits
- Minimāls datu glabāšanas termiņš
- Automātiska datu dzēšana pēc termiņa beigām
- Datu aizsardzības ietekmes novērtējums (DPIA)

Sensitīvu datu noplūde HR vidē var radīt nopietnus GDPR pārkāpumus, finansiālus sodus un reputācijas riskus.

DATU DROŠĪBAS INCIDENTA 72 STUNDU PROTOKOLS

Seši soļi, kas obligāti jāveic 72 stundu laikā pēc datu drošības incidenta atklāšanas

1 0–4h: Atklāšana un fiksācija

Reģistrē incidentu: laiku, avotu, apjomu un atbildīgo personu

2 4–12h: Izolācija un kontrole

Ierobežo incidentu un novērs turpmāku datu noplūdi

3 12–24h: Riska novērtējums

Cik datu subjektu skarti? Kāds ir risks? Vai nepieciešams ziņot DVI un skartajām personām?

4 24–48h: Iekšējā komunikācija

Informē datu aizsardzības speciālistu (DPO), vadību, IT komandu un juristus

5 48–72h: Paziņojums DVI

Oficiāls paziņojums Datu valsts inspekcijai un nepieciešamības gadījumā arī skartajām personām

6 Pēc 72h: Mācība un audits

Galvenā cēloņa analīze, korektīvie pasākumi un dokumentācijas pārbaude

REĀLI DATU AIZSARDZĪBAS UN AI PĀRKĀPUMI HR JOMĀ

Lielāko sodu apkopojums — kā kļūdas datu apstrādē izmaksā miljonus

1 H&M Vācija — €35.3M

Nelikumīga sensitīvu darbinieku datu apkopošana un uzraudzība (2020)

https://www.edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en

2 Amazon Francija — €32M

Pārmērīga noliktavas darbinieku uzraudzība un produktivitātes izsekošana (2024)

https://www.edpb.europa.eu/news/national-news/2024/employee-monitoring-french-sa-fined-amazon-france-logistique-eu32-million_en

3 iTutorGroup ASV — $365K

AI atlases sistēma diskriminēja kandidātus pēc vecuma (EEOC, 2023)

https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit

4 Clearview AI — €20M

Biometrisko datu nelikumīga apkopošana bez cilvēku piekrišanas (2022)

https://www.edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

5 Marriott — £18.4M

339 miljonu viesu datu noplūde un nepietiekama datu aizsardzība (ICO, UK, 2020)

https://www.edpb.europa.eu/sites/default/files/article-60-final-decisions/uk_2020-10_personal_data_breach_decisionpublic_final.pdf

6 Meta Platforms — €91M

Nepietiekama paroļu un lietotāju datu aizsardzība (2024)

https://www.reuters.com/technology/eu-privacy-regulator-fines-meta-91-million-euros-over-password-storage-2024-09-27/

DATU VALSTS INSPEKCIJA (DVI) LATVIJĀ

Uzraugošā iestāde personas datu aizsardzības jomā

1 Kas ir DVI

Datu valsts inspekcija — uzraugošā iestāde personas datu aizsardzības jomā Latvijā

2 Galvenās funkcijas

Pārbaudes, konsultācijas, sūdzību izskatīšana un sodu piemērošana

3 Sūdzības iesniegšana

Sūdzību var iesniegt DVI mājaslapā. Atbilde parasti tiek sniegta 1 mēneša laikā, sarežģītos gadījumos — ilgāk

4 Sodi Latvijā

Sodi var sasniegt līdz €20M vai 4 % no uzņēmuma gada apgrozījuma. Latvijā praksē sodi parasti ir ievērojami zemāki

5 Kontakti

Elijas iela 17, Rīga • +371 67223131 • pasts@dvi.gov.lv

6 DPO reģistrācija

Noteiktos gadījumos organizācijām jāieceļ datu aizsardzības speciālists (DPO)

DARBINIEKU TIESĪBAS GDPR IETVAROS

Tiesības, kuras HR jānodrošina katram darbiniekam

Piekļuves tiesības

Darbinieks var pieprasīt informāciju par to, kādi dati par viņu tiek glabāti un apstrādāti

Labojumu tiesības

Tiesības pieprasīt neprecīzu vai nepilnīgu datu labošanu

Dzēšanas tiesības

Tiesības tikt aizmirstam" — pieprasīt datu dzēšanu, ja tie vairs nav nepieciešami

Iebilduma tiesības

Iebilst pret datu apstrādi, ja tā balstīta uz leģitīmajām interesēm

Pārnesamības tiesības

Saņemt savus datus strukturētā un mašīnlasāmā formātā

Tiesības uz cilvēka iesaisti

Darbiniekam ir tiesības nepieļaut, ka būtiski lēmumi tiek pieņemti tikai automatizēti

Svarīgi lēmumi par darbinieku nedrīkst balstīties tikai uz automatizētu apstrādi

ANONIMIZĀCIJA UN PSEIDONIMIZĀCIJA HR DATOS

Divas dažādas tehnikas — atšķirīgas juridiskās sekas

1 Anonimizācija

Dati tiek pārveidoti tā, lai personu vairs nevarētu identificēt. Uz pilnībā anonimizētiem datiem GDPR parasti vairs neattiecas

2 Pseidonimizācija

Personas identifikatori tiek aizstāti ar kodiem, bet sākotnējie dati tiek glabāti atsevišķi. GDPR joprojām piemērojas.

3 HR piemērs: atalgojums

Anonimizēti dati: Vidējā alga komandā — €2500
Pseidonimizēti dati: Darbinieks ID-4521 — €2500

4 HR piemērs: aptauja

Anonīma aptauja — bez iespējas identificēt konkrētu personu.
Pseidonimizēta aptauja — ar kodu, kuru noteiktos gadījumos iespējams sasaistīt ar personu.

5 Kad ko izvēlēties

Anonimizāciju izmanto publiskām atskaitēm un ārējai statistikai.
Pseidonimizāciju biežāk izmanto iekšējai HR analītikai un datu analīzei.

6 Biežākās kļūdas

Pat neliels datu elementu kopums, piemēram, vecums, amats, dzimums un reģions, var radīt personas atkārtotas identificēšanas risku.

DARBINIEKU MONITORINGA ROBEŽAS

Kur beidzas leģitīmā interese un sākas GDPR pārkāpums

1 E-pasts un saziņa

DRĪKST: uzraudzīt tehniskos un drošības aspektus uzņēmuma tīklā.
NEDRĪKST: bez pamatota iemesla lasīt darbinieku privāto saziņu vai e-pastu saturu.

2 Kameras darbavietā

DRĪKST: izmantot drošības zonās un īpašuma aizsardzībai.
NEDRĪKST: filmēt tualetes, atpūtas telpas vai veikt pastāvīgu nesamērīgu uzraudzību.

3 Ekrānuzņēmumi

Pieļaujami tikai ar skaidru biznesa pamatojumu, iepriekšēju informēšanu un minimālā apjomā.

4 Lokācijas izsekošana

DRĪKST: darba transportlīdzekļiem darba laikā.
NEDRĪKST: izsekot darbinieku ārpus darba laika vai bez skaidra pamatojuma.

5 Tastatūras aktivitātes uzraudzība

Keylogging un detalizēta tastatūras uzraudzība parasti tiek uzskatīta par nesamērīgu un rada augstu GDPR pārkāpuma risku.

6 Tests pirms ieviešanas

Leģitīmā Pirms jebkura monitoringa jāizvērtē leģitīmā interese, nepieciešamība, samērīgums, informēšanas pienākums un nepieciešamības gadījumā jāveic DPIA.

HR KOMANDAS GDPR APMĀCĪBU PLĀNS

Sešu moduļu programma — pamatapmācība pie pieņemšanas darbā un ikgadējs zināšanu atjauninājums

1 Pamati un terminoloģija

GDPR pamatjēdzieni, lomas (pārzinis, apstrādātājs, DPO) un galvenie juridiskie pamati datu apstrādei.

2 Datu apstrāde praksē

Tiesiskie pamati, datu minimizācija, mērķa ierobežojums un droša datu apstrāde HR ikdienā.

3 Darbinieku tiesības

Piekļuves, labošanas, dzēšanas, iebilduma un datu pārnesamības tiesības HR procesos.

4 Drošība un incidenti

Šifrēšana, piekļuves līmeņi, 72 stundu ziņošanas pienākums un DPIA praktiskā pielietošana.

5 AI un automatizācija

GDPR 22. pants, automatizēti lēmumi, AI pārredzamība, audits un cilvēka iesaiste lēmumu pieņemšanā.

6 Praktiskie scenāriji

Praktiski piemēri par sensitīviem datiem, exit procesiem, datu pārkāpumiem un AI izmantošanu HR darbā.

VENDOR DUE DILIGENCE — HR SaaS PĀRBAUDE

Jautājumi, kas HR komandai jāizvērtē pirms jauna HR rīka ieviešanas

1 DPA — Datu apstrādes līgums

Datu apstrādes līgumam jābūt noslēgtam ar katru pakalpojuma sniedzēju. GDPR 28. pants nosaka pušu lomas, atbildību, drošības prasības un apakšapstrādātāju izmantošanu.

2 Datu lokācija

Svarīgi noskaidrot, kur fiziski tiek glabāti dati — ES, ASV vai citur. Jāpārbauda, vai tiek izmantots adequacy decision vai SCC mehānisms datu pārsūtīšanai ārpus ES.

3 Apakšapstrādātāji (sub-processors)

Pakalpojuma sniedzējam jānodrošina pilns apakšapstrādātāju saraksts un savlaicīgi paziņojumi par izmaiņām. Jāpārbauda arī viņu drošības līmenis.

4 Drošības sertifikāti

Svarīgi pārbaudīt ISO 27001, SOC 2 Type II vai citus drošības sertifikātus, kā arī pieprasīt auditu vai atbilstības pierādījumus.

5 Incidentu protokols

Jānoskaidro, cik ātri piegādātājs ziņo par drošības incidentiem. Ideālā gadījumā — ne vēlāk kā 24 stundu laikā, lai organizācija spētu ievērot GDPR 72 stundu ziņošanas termiņu.

6 Exit stratēģija

Pirms sadarbības uzsākšanas jāzina, kā organizācija saņems savus datus atpakaļ, cik ātri tie tiks dzēsti un vai būs pieejams strukturēts datu eksports.

AI RISKI HR VIDĒ

Četri galvenie riski, ko HR komandai jāzina

Algoritmiskā neobjektivitāte

AI modeļi mācās no vēsturiskiem datiem, kuros var būt aizspriedumi vai nevienlīdzība. Piemēram, Amazon AI atlases rīks 2018. gadā diskriminēja sievietes tehniskajās vakancēs.

Caurspīdīguma trūkums

Daudzi AI modeļi darbojas kā “melnā kaste” — ir grūti izskaidrot, kāpēc pieņemts konkrēts lēmums vai rekomendācija.

Pārmērīga uzticēšanās

Pastāv risks, ka HR speciālisti sāk pieņemt AI ieteikumus bez kritiskas izvērtēšanas. Tas var radīt automatizētus aizspriedumus lielākā mērogā.

Datu noplūde caur AI

Sensitīvi dati var nonākt trešo pušu sistēmās vai tikt izmantoti AI modeļu apmācībai bez pietiekamas kontroles un pārraudzības.

AI ACT IEVIEŠANAS GRAFIKS 2024–2027

Kad AI Act prasības stājas spēkā HR procesos

1 **Augusts 2024**

AI Act stājas spēkā un sākas pārejas periods. ES dalībvalstis sāk veidot uzraudzības mehānismus un institūcijas.

2 **Februāris 2025**

Sāk piemērot aizliegumus noteiktām AI praksēm: emociju atpazīšanai darbavietā, sociālajai vērtēšanai un manipulējošām sistēmām.

3 **Augusts 2025**

GPAI modeļiem stājas spēkā prasības par dokumentāciju, caurspīdīgumu un autortiesību ievērošanu.

4 **Augusts 2026**

Sāk piemērot augsta riska AI sistēmu prasības, tostarp CV atlasei, snieguma vērtēšanai un darbinieku monitoringam.

5 **Augusts 2027**

Pilnīga vairuma AI Act prasību piemērošana. Par pārkāpumiem iespējami sodi līdz €35M vai 7 % no globālā apgrozījuma.

6 **Ko darīt tagad**

Inventarizēt HR AI rīkus, klasificēt tos pēc riska līmeņa, sagatavot dokumentāciju un nepieciešamības gadījumā veikt DPIA.

AUGSTA RISKA AI SISTĒMAS HR PĒC AI ACT

Annex III sistēmas — kurām piemērojas stingrākās prasības

1 CV atlase un atlases lēmumi

AI sistēmas, kas automātiski šķiro kandidātus, veido rankingus vai novērtē kandidātu atbilstību amatam, tiek klasificētas kā augsta riska sistēmas saskaņā ar Annex III.

2 Snieguma vērtēšana

AI rīki, kas analizē produktivitāti, vērtē sniegumu vai ietekmē paaugstināšanas lēmumus, ietilpst augsta riska kategorijā.

3 Atalgojuma lēmumi

AI sistēmas, kas sniedz rekomendācijas par algu pārskatīšanu, prēmijām vai paaugstinājumiem, var būtiski ietekmēt darbinieku tiesības un karjeru.

4 Darbinieku monitorings

Sistēmas, kas uzrauga darbinieku uzvedību, produktivitāti vai ekrāna aktivitātes darba laikā, tiek uzskatītas par paaugstināta riska risinājumiem.

5 Atlaišanas lēmumi

AI rīki, kas iesaka vai automatizē lēmumus par darba attiecību izbeigšanu, ir pakļauti īpaši stingrām prasībām un cilvēka kontrolei.

6 AIZLIEGTS: emociju AI

Emociju atpazīšanas sistēmu izmantošana darbavietā un izglītībā AI Act ietvaros lielākoties ir aizliegta (Art. 5).

ATBILDĪGAS AI IEVIEŠANAS PRINCIPI

Pieci principi, kas palīdz samazināt AI riskus HR procesos

1

Cilvēka iesaiste

Galvenie lēmumi (atlase, atalgojums, atbrīvošana) — vienmēr cilvēks

2

Caurspīdīgums

Skaidri informēt darbiniekus par AI izmantošanu

3

Audits

Regulāri pārbaudīt AI rezultātus uz aizspriedumiem

4

Datu kontrole

Skaidri zināt, kādi dati tiek nodoti AI rīkiem

5

Iespēja iebilst

Darbiniekam — tiesības iebilst pret pilnībā automatizētu apstrādi

Princips: AI ir asistents, kas paātrina darbu — bet atbildība un galvenais lēmums vienmēr paliek pie cilvēka.

PROFESIONĀLĀ ATBILDĪBA UN REPUTĀCIJAS RISKI

Datu noplūde

Vidējās izmaksas — aptuveni 4,4 miljoni USD par incidentu (IBM, 2025). HR dati ir vieni no sensitīvākajiem un dārgākajiem datu veidiem.*

Diskriminācijas prasības

AI atlases rīku aizspriedumi var radīt juridisku atbildību un diskriminācijas prasības. iTutorGroup gadījums — 365 000 USD.**

Darbinieku uzticības zudums

Ja darbinieki nezina, kā tiek izmantots AI vai kā tiek pieņemti lēmumi, samazinās uzticība un iesaiste.

Mediju un sociālo tīklu krīzes

Jārēķinās, ka datu vai AI incidenti var ātri nonākt publiskajā telpā un radīt reputācijas krīzi dažu stundu laikā.

**https://www.ibm.com/reports/data-breach*

***https://www.eeoc.gov/newsroom/itutorgroup-pay-365000-settle-eeoc-discriminatory-hiring-suit*

ATBILDĪGAS AI IZMANTOŠANAS ČEKLISTS

Sešu punktu ikdienas pārbaudes HR komandai pirms AI lēmumu pieņemšanas

- ✓ **Skaidri dokumentēts mērķis**
  Katrai AI sistēmai zināms tās uzdevums un pamatojums
- ✓ **Darbinieki ir informēti**
  Caurspīdīga komunikācija par to, kur tiek lietots AI
- ✓ **Regulārs audits**
  Vismaz reizi gadā tiek pārbaudīta neobjektivitāte un kvalitāte
- ✓ **Piekļuves līmeņi**
  AI sistēmām piekļūst tikai pilnvaroti HR darbinieki
- ✓ **Cilvēka uzraudzība**
  Lēmumus pieņem cilvēks, AI sniedz tikai ieteikumu
- ✓ **Incidentu plāns**
  Skaidri soļi, ja AI sniedz neobjektīvu rezultātu vai kļūdu

ATBILDĪGA PIEEJA: PIRMS UN TAGAD

PIRMS: Reaktīva pieeja	TAGAD: Proaktīva pieeja
Sods → reaģējam	Risku novērtēšana iepriekš (DPIA)
GDPR ir tikai juristu ziņā	Datu aizsardzība ir visas HR komandas atbildība
AI rezultāti netiek pārbaudīti	Regulārs AI rezultātu audits uz aizspriedumiem
Politikas pastāv tikai uz papīra	Politikas tiek ieviestas un ievērotas
Darbinieks uzzina, kad jau ir par vēlu	Caurspīdīga komunikācija jau no paša sākuma

ĒTISKĀS DILEMMAS HR DARBĀ

Reālas situācijas, kurās jāmeklē līdzsvars starp efektivitāti, privātumu un ētiku

AI prognozē, ka darbinieks aizies

Vai vadītājam būtu jāzina šāda prognoze? Vai tas palīdz noturēt darbinieku vai tieši pretēji — pasliktina uzticību un attiecības komandā?

Atlasē izmanto sociālos profilus

Cik lielā mērā HR drīkst izmantot kandidāta publiski pieejamo informāciju? Kur beidzas profesionāla izvērtēšana un sākas privātuma pārkāpums?

AI atlasa CV, bet nespēj izskaidrot lēmumu

Vai drīkst izmantot AI sistēmu, ja kandidātam nav iespējams skaidri izskaidrot atteikuma vai atlases iemeslu?

Slimības lapu monitorings

Vai HR drīkst analizēt slimības lapu tendences un biežumu? Kur ir robeža starp darbinieku atbalstu un pārmērīgu kontroli?

PRAKTISKAIS SCENĀRIJS



Situācija: Uzņēmums plāno ieviest AI atlases rīku, kas analizē un sarindo kandidātus pēc CV. HR vadītājs jautā: kā nodrošināt, lai šis rīks tiktu izmantots atbildīgi un neradītu juridiskus vai reputācijas riskus?

1. solis

DPIA novērtējums

Pirms ieviešanas jāveic datu aizsardzības ietekmes novērtējums (DPIA), lai identificētu iespējamos riskus un to ietekmi uz kandidātiem.

2. solis

Audits un testēšana

AI rīks jāpārbauda ar dažādām kandidātu grupām, lai identificētu iespējamos aizspriedumus vai diskriminācijas riskus.

3. solis

Caurspīdīga politika

Kandidāti skaidri jāinformē par AI izmantošanu atlases procesā. Galīgais lēmums vienmēr jāpieņem cilvēkam.

Rezultāts: pareizi ieviests AI rīks var paātrināt atlases procesu un vienlaikus samazināt aizspriedumu un juridisko risku iespējamību.

BIEŽĀKĀS KĻŪDAS DATU AIZSARDZĪBĀ UN AI ĒTIKĀ

✗ Sensitīvu datu glabāšana Excel failos uz darbvirsmas	✓ Sensitīvu datu glabāšana drošā HRIS sistēmā ar šifrēšanu
✗ AI rīka ieviešana bez DPIA novērtējuma	✓ Risku novērtējums pirms jebkura jauna AI rīka ieviešanas
✗ Viena piekrišana visiem datu apstrādes mērķiem	✓ Atsevišķa piekrišana katram konkrētam datu apstrādes mērķim
✗ AI rezultātu nepārbaudīšana	✓ Regulāra AI rezultātu pārbaude attiecībā uz aizspriedumiem un kļūdām
✗ Formāla un neskaidra darbinieku informēšana	✓ Skaidra, saprotama un pieejama komunikācija par datu un AI izmantošanu

DISKUSIJA

1. Vai uzņēmumam būtu jāinformē darbinieki, ka viņu dati tiek izmantoti AI analītikā? Kā to darīt ētiski?

2. Kur beidzas datu analītika un sākas darbinieku privātuma pārkāpums?

3. Kas ir svarīgāk HR procesos — efektivitāte vai caurspīdīgums?

4. Kāda ir HR profesionāļa atbildība laikmetā, kad daudzi lēmumi ir automatizēti?

KOPSAVILKUMS

- ✓ GDPR pamatprincipi: tiesiskums, mērķa ierobežojums, datu minimizācija, precizitāte, glabāšanas ierobežojums un drošība.
- ✓ Darbinieku tiesības: piekļuve datiem, datu labošana, dzēšana, iebildums, datu pārnesamība un tiesības uz cilvēka pieņemtu lēmumu
- ✓ Sensitīvie dati: veselības dati, pārliecība, biometriskie dati — nepieciešama papildu aizsardzība un audits
- ✓ AI riski HR vidē: aizspriedumi, caurspīdīguma trūkums, pārmērīga uzticēšanās un datu noplūde.
- ✓ Atbildīgas AI izmantošanas principi: cilvēks cilpā, caurspīdīgums, audits, datu kontrole un iespēja iebilst.
- ✓ Reputācijas riski un sodu izmaksas pārsniedz pareizas ieviešanas izmaksas.

KURSA NOSLĒGUMS — KO ESAM APGUVUŠI

Septiņu nodarbību ceļš caur HR digitalizāciju un AI

1. **Digitālie un AI rīki**
2. **Dokumenti un dati**
3. **ATS un kandidātu atlase**
4. **Intervijas un komunikācija**
5. **Procesu plānošana**
6. **Datu analīze**
7. **Aizsardzība un ētika**

No iepazīšanas ar tehnoloģijām līdz atbildīgai un ētiskai to izmantošanai HR procesos.

Pēc kursa: gatavošanās gala pārbaudījumam — kompleksa praktiskā darba izstrādei grupās un tā aizstāvēšanai.

GALA PĀRBAUDĪJUMS

Komplekss praktiskais darbs — aizstāvēšana prezentācijas formātā

Izanalizēt izvēlētu HR procesu reālā vai modelētā organizācijas situācijā un izstrādāt digitālu vai AI balstītu risinājumu tā uzlabošanai. Darbu var izstrādāt individuāli vai grupās līdz 4 cilvēkiem.
Darbs jāiesniedz līdz 10. jūnijam nosūtot uz e-pastu. Pirmajā slaidā jānorāda visu projekta dalībnieku vārdi un uzvārdi.

1

Procesa analīze

Identificēt esošo HR procesu un tā vājās vietas

2

Rīka izvēle

Piemērota digitālā vai AI rīka izvēle un praktiskā pielietojuma demonstrācija

3

Datu aizsardzība un ētika

GDPR un ētisko aspektu izvērtējums izvēlētajam risinājumam

4

Efektivitātes pamatojums

Risinājuma nepieciešamības un tā ieguvumu argumentēts pamatojums

Aizstāvēšana — prezentācijas formātā. Katram grupas dalībniekam jādemonstrē individuāls ieguldījums un izpratne.

Paldies!

Tagad jūsu rokās ir gan rīki, gan principi, lai padarītu HR procesus efektīvākus, taisnīgākus un cilvēcīgākus.

Veiksmi gala pārbaudījumā!