

ĒTISKIE ASPEKTI UN DATU

aizsardzība MI izmantojumā

Kiberdrošība, privātums un atbildīga rīcība 2026. gada digitālajā vidē

11.Lekcija | Prasmju pilnveide pieaugušajiem

Kitija Spēka-Štobe



Ko šodien apskatīsim

1 Personas dati un riski MI laikmetā

2 Kiberdrošība un reālie draudi

3 Likumi: GDPR un ES AI Act

4 Praktiskais darbs: AI + Kiberdrošības čekliste

5 Diskusija un noslēgums

Kas ir datu aizsardzība?

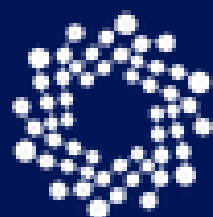
Datu aizsardzība

Procesu, noteikumu un tehnoloģiju kopums, kas nodrošina, ka personas dati tiek apstrādāti droši, likumīgi un ar cieņu pret privātumu. Mī laikmetā tas nozīmē - katrs Tavs prompts, augšupielādēts fails vai čats var kļūt par daļu no modeļa apmācības datiem.

Kiberdrošība

Prakses un tehnoloģijas, kas aizsargā datus pret ārējiem uzbrukumiem - hakeriem, vīrusiem un Mī radītiem draudiem. Tā nav tikai IT nodaļas problēma. Tā ir katra lietotāja ikdienas atbildība.

Datu aizsardzība + Kiberdrošība = Tavs digitālais vairogs



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Kas ir personas dati?

Personas dati ir jebkura informācija, kas ļauj tieši vai netieši identificēt konkrētu cilvēku. Mūlaikmetā tas ir daudz vairāk nekā vārds un uzvārds.

1

Vārds, uzvārds,
personas kods

2

Kontakt-
informācija

3

Foto un video

4

IP adrese,
sīkdatnes

5

Paradumi
un uzvedība

6

Atrašanās
vieta

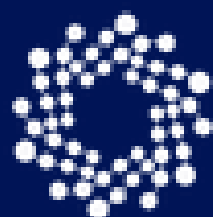
7

Politiskie uzskati,
religija

8

Biometriskie dati,
veselības stāvoklis

Katrs prompts, ko ieraksti ChatGPT, ir arī personas dati - ja tajā ir kaut kas, kas atklāj Tevi.



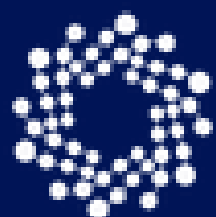
KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



1 Personas dati un riski

MI laikmetā



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Finansē
Eiropas Savienība
NextGenerationEU



Īpaši sensitīvie dati - ko nekad nedrīkst dot MI rīkiem



Veselības stāvoklis un
diagnozes



Biometriskie dati (seja, pirkstu
nospiedumi)



Ģenētiskā informācija



Reliģiskā pārliecība



Politiskie uzskati



Seksuālā orientācija



Rase un tautība



Sodāmība

MI var izmantot šos datus manipulācijai vai diskriminācijai. Kibernoiedznieki - identitātes zādzībai vai šantāžai.

Vizuālais saturs arī ir personas dati

Sejas, tetovējumi vai citas ķermeņa īpatnības ir personas dati. Augšupielādējot attēlus MI rīkos (piemēram, Midjourney), nedrīkst būt redzami citi cilvēki bez viņu skaidras piekrišanas.

Deepfake risks

Hakeri var izmantot Tavus attēlus, lai radītu pārliecinošus deepfake video Tavā vārdā. Šādi uzbrukumi pieaug eksponenciāli.

Biometriskā atpazīšana

MI sejas atpazīšanas sistēmas var identificēt cilvēkus no publiskiem attēliem bez viņu ziņas vai piekrišanas.

Piekrišanas princips

Pirms jebkura attēla ar citu personu augšupielādes MI rīkā jāsaņem skaidra, rakstiska piekrišana. Bez izņēmumiem.

Digitālā pēda

"Digitālā pēda ir kā tetovējums - to gandrīz nav iespējams pilnībā izdzēst."

Ko Tu atstāj

Katrs klikšķis, patīk, komentārs, meklēšana, atrašanās vieta un MI rīkā ievadīts teksts veido Tavu digitālo profilu, ko uzņēmumi glabā gadiem.

Ko ar to dara

Uzņēmumi izmanto šos datus reklāmām un personalizācijai. Kibernoziedznieki - identitātes zādzībai, šantāžai un mērķētiem uzbrukumiem.

Ko Tu vari darīt

Regulāri pārbaudi privātuma iestatījumus. Dzēs čatu vēsturi MI rīkos. Neievadi vairāk informācijas, nekā konkrētam uzdevumam nepieciešams.

Kāpēc tas skar Tevi personīgi?

Identitātes zādzība

Ja nozog personas kodu, bankas datus vai paroles - var atvērt kredītu, iztukšot kontu, iegādāties preces Tavā vārdā.

Manipulācija

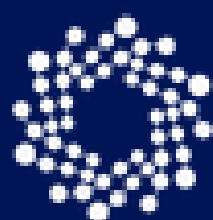
Cambridge Analytica izmantoja Facebook datus, lai ietekmētu vēlēšanas. Tas notika. Ar MI tas kļūst vēl efektīvāk.

Diskriminācija

Algoritmi var izslēgt cilvēkus no darba, kredīta vai pakalpojumiem, pamatojoties uz datiem, ko viņi nav apzināti atklājuši.

MI uzbrukumi

2025. gadā Latvijā kiberincidenti pieauga par 62%. Lielākā daļa bija MI pastiprināti - personalizēti un grūti atpazīstami.



Ko MI rīki dara ar Taviem datiem?

ChatGPT (OpenAI)

ASV uzņēmums. Bezmaksas versijā čati var tikt izmantoti modeļa apmācībai. Plus versijā iespējams atslēgt sadaļā 'Data Controls'.

Grok (xAI)

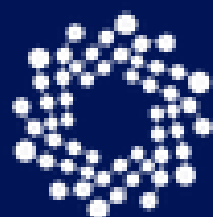
Elon Musk uzņēmums. Integrēts ar X platformu. Dati var tikt izmantoti personalizācijai visā platformā. Privātuma iestatījumi ir ierobežoti.

Claude (Anthropic)

Drošībā orientēts MI. Bezmaksas versijā čati netiek izmantoti apmācībai pēc noklusējuma. Viens no pārredzamākajiem rīkiem tirgū.

Midjourney

Visi ģenerētie attēli ir publiski pieejami bezmaksas versijā. Augšupielādēti attēli var palikt platformas sistēmā uz nenoteiktu laiku.



KOMPETENČU
CENTRS

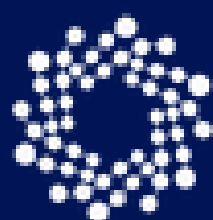
ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



DISKUSIJA

**Cik % no saviem datiem Tu esi
gatavs atdot
MI rīkiem, zinot kibernetikas
draudus?**

Un vai Tev ir atšķirīga robeža darbam un personīgajai dzīvei?



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001

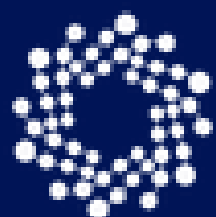


Finansē
Eiropas Savienība
NextGenerationEU



Kiberdrošība un reālie draudi

MI laikmetā



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Finansē
Eiropas Savienība
NextGenerationEU

2027
Nacionālais
attīstības plāns

Kas ir kiberdrošība MI laikmetā?

Kiberdrošība ir prakses, tehnoloģijas un procesi, kas aizsargā datorus, tīklus un datus pret uzbrukumiem. MI laikmetā tas nozīmē aizsardzību pret jauniem, automatizētiem un personalizētiem draudiem.

Vecā kiberdrošība

- Vīrusi un ļaunatūra
- Vājās paroles
- Neaizsargāti tīkli
- Phishing e-pasti

MI pastiprināti draudi

- Personalizēti deepfake uzbrukumi
- Prompt injection MI rīkos
- MI radīts phishing (grūti atpazīt)
- Model poisoning - saindēti dati

Galvenie kiberapdraudējumi MI rīkos

Phishing ar MI

MI ģenerē personalizētus viltotus e-pastus. 2025. gadā tie kļuvuši tik pārliecinoši, ka pat eksperti tos nevar atpazīt pēc stila vien.

Ransomware

Uzbrucēji bloķē Tavus datus un prasa izpirkumu. MI palīdz viņiem izvēlēties labāko uzbrukuma laiku un personalizēt ziņojumu.

Deepfake uzbrukumi

MI rada pārliecinošus video un audio Tavā vārdā. Izmanto, lai malinātu kolēģus, radītu viltus pārstāvjus vai izspiestu naudu.

Datu noplūdes

MI platformu serveru uzlaušana var atklāt visu Tavu čatu vēsturi - ieskaitot dokumentus, stratēģijas un personīgo informāciju.

Latvija 2025. - reālie skaitļi (avots: CERT.LV)

923

manuāli apstrādāti
kiberincidenti tikai 4.
ceturksnī (+62%)

731 783

kompromitētas ierīces (8x
vairāk nekā 2022. gadā)

+35%

krāpšanas gadījumu
pieaugums, lielākoties ar
MI palīdzību

1. vieta

AI pastiprināta krāpšana
kā dominējošais drauds
Latvijā

Konkrēti gadījumi:

- Ransomware uzbrukumi Kultūras informācijas sistēmu centram un privātiem uzņēmumiem (2025. g. 3. ceturksnis)
- Datu noplūde pašvaldībā caur Vidar infostealer - lietotāju paroles un dokumenti (decembris 2025)
- ClickFix uzbrukumi - MI ģenerētas viltus Google reklāmas ar ļaunatūru Latvijas lietotājiem

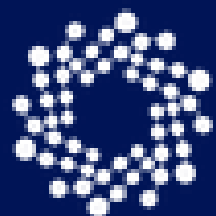
Kā atpazīt phishing un deepfake 2026. gadā?

Phishing pazīmes

- Steidzamība un bailes - 'Jūsu konts tiks slēgts 24 stundu laikā'
- URL adrese izskatās gandrīz pareiza (google.com ar kirilicas 'o')
- Lūgums ievadīt paroli vai bankas datus pa e-pastu vai ziņojumā
- Teksts bez gramatikas kļūdām, bet ar nereālu steigu vai solījumu

Deepfake pazīmes

- Nenaturāla acu mirdzēšana vai neparasta mirgošana video
- Balss skan nedaudz mehāniski, bez dabisku emociju niansēm
- Fona objekti video izskatās neskaidri vai pēkšņi mainās
- Persona prasa naudu vai datus, ko nekad prasītu klātienē



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Kā aizsargāties - praktiski soļi

2FA visur

Ieslēdz divfaktoru autentifikāciju e-pastā, bankā, MI rīkos. Pat ja parole noplūst, konts paliek aizsargāts.

Spēcīgas paroles

Izmanto parolu pārvaldnieku (Bitwarden, 1Password). Katram kontam atšķirīga parole - nekad neatkārtot.

VPN publiskajos tīklos

Kafejnīcas, lidostas Wi-Fi ir bīstami. VPN šifrē Tavu savienojumu un aizsargā datus ceļā.

Šifrēta saziņa

Sensitīvai saziņai izmanto Signal - end-to-end šifrēšana, nav reklāmu, nav datu pārdošanas.

Lokālie MI modeļi

Ollama ar Llama 3 darbojas Tavā datorā. Dati nekur nepārsūtās - ideāli sensitīvam darbam.

Regulāri atjauninājumi

Atjauninājumi aizlabo drošības caurumus. Ieslēdz automātiskos atjauninājumus operētājsistēmā.

Key Takeaways - Kiberdrošība

1. MI rīki rada jaunus draudus - phishing, deepfake un datu noplūdes ir realitāte, ne teorija
2. Latvijā 2025. gadā kiberincidenti pieauga par 62% - un lielākā daļa bija MI pastiprināti
3. 2FA + spēcīgas paroles + VPN = pamata aizsardzība, ko vari iestatīt šodien, pēc lekcijas
4. Sensitīvam darbam izmanto lokālos MI modeļus (Ollama) - dati paliek pie Tevis

Reālie MI risku pētījumi Latvijā 2024.-2025.

Latvijā veikti vairāki nozīmīgi pētījumi par MI riskiem:

- Saeimas pētījums (2025): detalizēti analizēti kiberdrošības, datu aizsardzības, ētikas un diskriminācijas riski valsts pārvaldē.
- Tiesībsarga pētījums (2024): algoritmiskā diskriminācija un cilvēktiesības.
- Valsts kontroles revīzija (2025): 53 % iestāžu nav veikts ētikas/neobjektivitātes risku novērtējums.
- KPMG pētījums (2025): 76 % Latvijas iedzīvotāju bažas par riskiem un dezinformāciju.

Secinājums

Latvija aktīvi pēta riskus, bet praktiskā risku vadība (īpaši publiskajā sektorā) vēl ir nepilnīga.

Avoti:

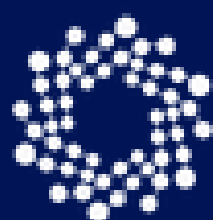
Saeimas pētījums: saeima.lv/petijumi

Tiesībsargs: tiesibsargs.lv

Valsts kontrole: lrvk.gov.lv

KPMG globālais pētījums 2025

Pauze 10 min



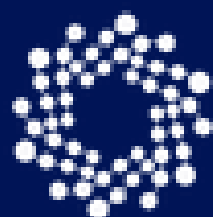
KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Likumi: GDPR un ES AI Act

MI laikmetā



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Kas ir GDPR?

GDPR jeb Vispārīgā datu aizsardzības regula ir ES likums, kas stājās spēkā 2018. gadā. Tā nosaka, kā uzņēmumi drīkst vākt, glabāt un izmantot ES iedzīvotāju personas datus.

Vienoti noteikumi visā ES

Pirms GDPR katrā valstī bija atšķirīgi datu aizsardzības likumi. Tagad - viena sistēma visiem uzņēmumiem.

Cilvēku tiesību aizsardzība

Ikvienam ir tiesības zināt, kādi dati par viņu tiek vākti, un pieprasīt to dzēšanu vai labošanu.

Atbildība uzņēmumiem

Datu vākšana nedrīkst būt patvaļīga - tai jābūt caurskatāmai, pamatotai un drošai. Sods līdz 20M EUR.

Attiecas uz visiem

Facebook, Google, TikTok, Amazon - visi ir spiesti ievērot GDPR, ja strādā ar ES lietotājiem.

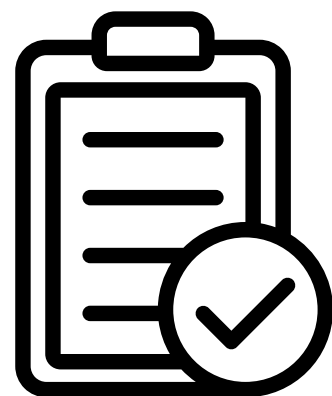
Tavas tiesības un uzņēmumu pienākumi

Tev kā lietotājam ir tiesības:

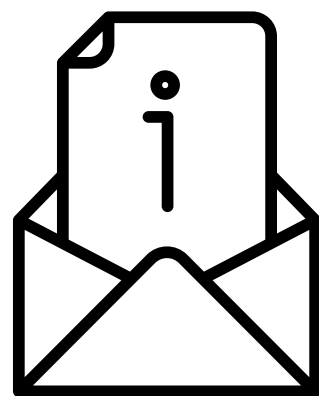
- ✓ Piekļūt saviem datiem - uzzināt, kas par Tevi tiek vākts
- ✓ Labot datus - ja kāda informācija ir nepareiza
- ✓ Dzēst datus ('tiesības tikt aizmirstam')
- ✓ Ierobežot datu izmantošanu - piemēram, atteikties no mārketinga
- ✓ Datu pārnesamība - saņemt savus datus lasāmā formātā
- ✓ Iebilst pret datu apstrādi noteiktās situācijās

Sods par GDPR pārkāpumiem:

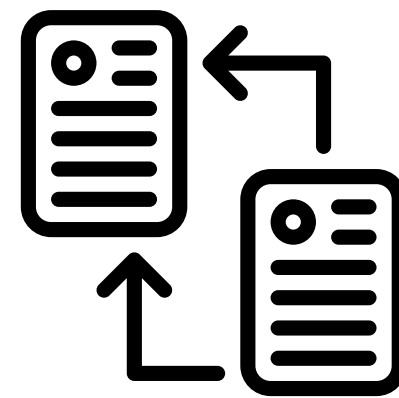
Līdz 20 miljoniem EUR vai 4% no gada apgrozījuma - atkarībā no tā, kas ir lielāks.



Zināt



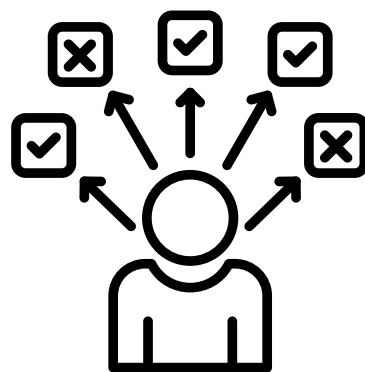
Saņemt



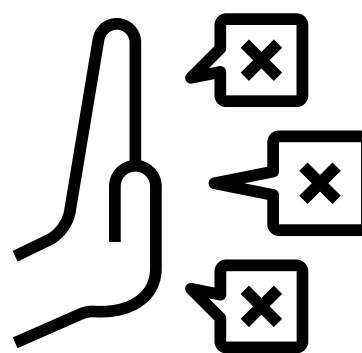
Pārnest



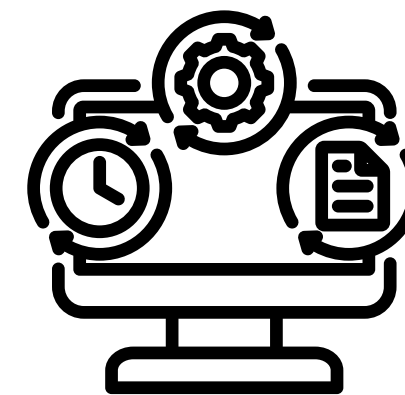
Dzēst



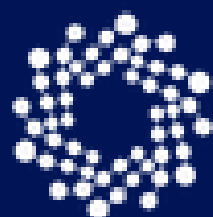
Ierobežot



Iebilst



Atteikties no
automatizētiem lēmumiem



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



sods par GDPR pārkāpumiem

Līdz 20 miljoniem EUR vai 4% no gada apgrozījuma - atkarībā no tā, kas ir lielāks.

Google (2019)

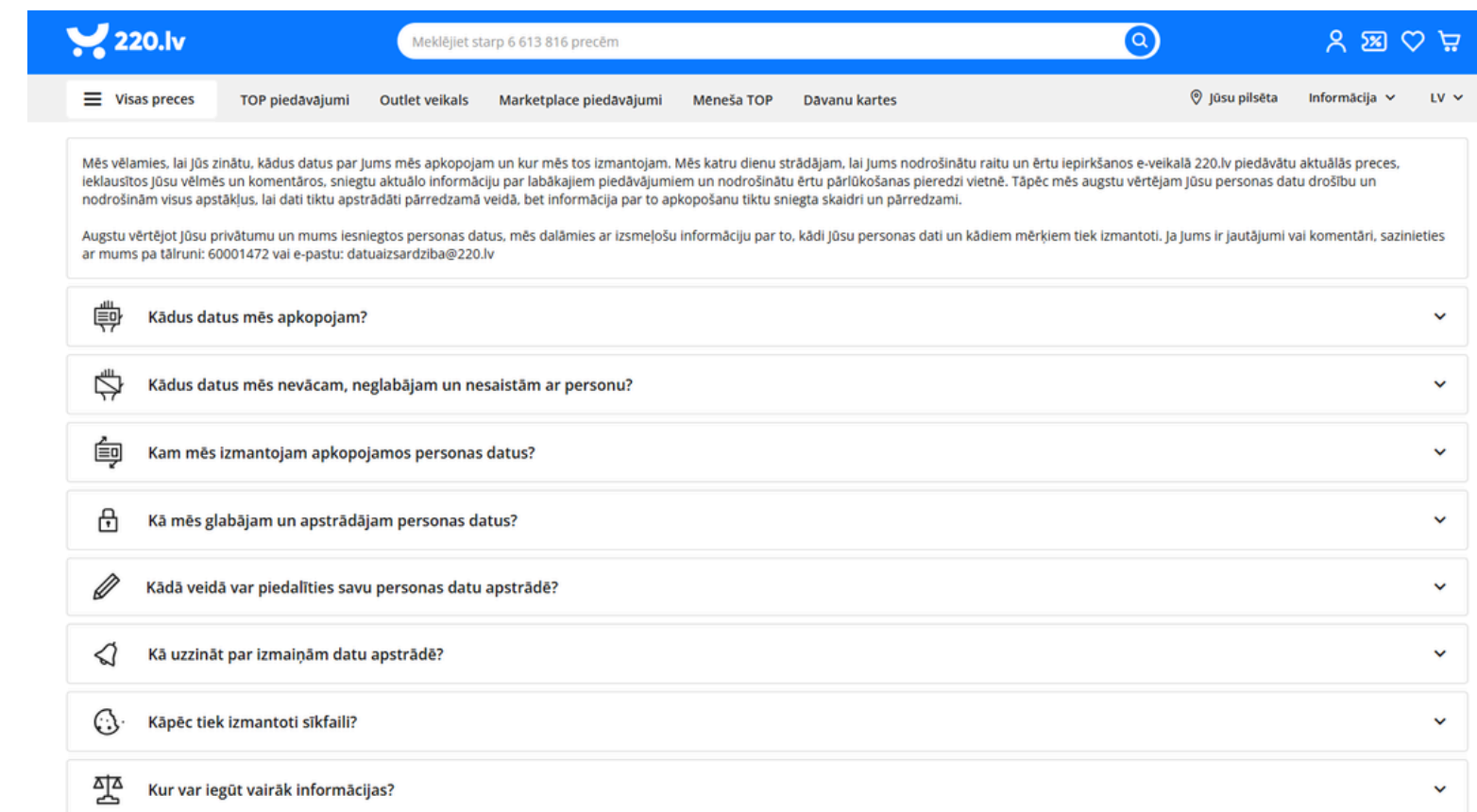
- Francija uzlika 50 miljonu € sodu Google.
- Iemesls: Google nesniedza lietotājiem skaidru un saprotamu informāciju par to, kā tiek vākti un izmantoti viņu dati.
- Lietotāji nevarēja viegli atrast un saprast privātuma politiku.



https://www.edpb.europa.eu/news/national-news/2019/cnils-restricted-committee-imposes-financial-penalty-50-million-euros_en?utm_source=chatgpt.com

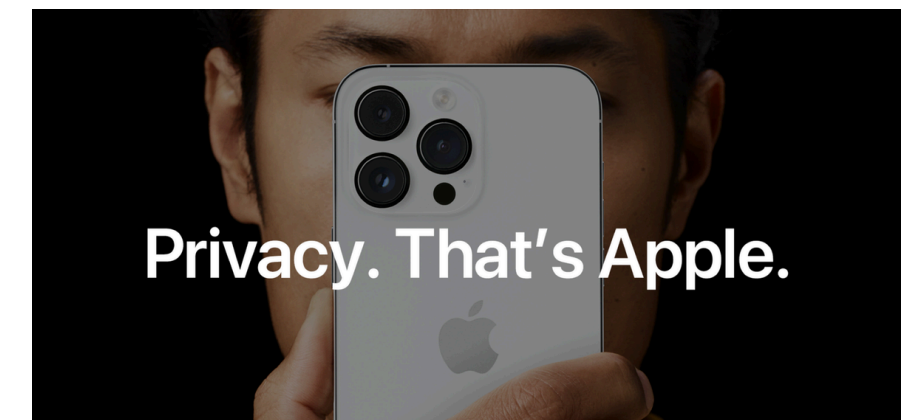
GDPR pamatprincipi

Interneta veikals 220.lv ir izstrādājis detalizētu privātuma politiku, kas atbilst Vispārīgās datu aizsardzības regulas (GDPR) prasībām. Viņi skaidri norāda, kādus personas datus vāca, kāpēc tos izmanto un kā lietotāji var īstenot savas tiesības attiecībā uz datu apstrādi.



Privātuma politika reālos piemēros

Privātuma politika ir dokuments, kurā uzņēmums paskaidro, kādus datus vāc un kā izmanto. Lasi to pirms reģistrēties jebkurā MI rīkā.



220.lv

Detalizēta privātuma politika atbilstoši GDPR. Skaidri norāda kādus datus vāc, kāpēc, un kā lietotāji var realizēt savas tiesības. Labs paraugs.

Apple



'Privacy by Design' - lietotāju dati netiek pārdoti trešajām pusēm. Šifrēšana nodrošina privātumu pēc noklusējuma.

Signal

Neuzglabā sarunu saturu. Nav reklāmu, nav datu pārdošanas. Atvērtā koda risinājums ar augstāko drošības līmeni.

ChatGPT (bezmaksas)

Ļauj izmantot čatus modeļa uzlabošanai. Iespēja atslēgt: Settings → Data Controls → pārslēgt uz 'off'.

		
Open Source	No	Yes
Privacy Level	Moderate	Very High
Data Collection	Extensive*	Minimal**
Backup Default	Cloud	Local
Backup Type Encrypted	No	Yes
Calls Over Tor Network	No	Yes
Owned By	Meta	Signal

* Extensive data collection: Meta collects the following info from your WhatsApp: phone number, contacts, location, usage, behavioural data, etc. where as **Signal collects the following: phone number only.

Kas ir ES AI Act?

ES AI Act ir pirmais likums pasaulē, kas speciāli regulē mākslīgā intelekta sistēmas. Stājās spēkā 2024. gadā, pilnībā piemērojams no 2026. gada.

Nepieļaujams risks	PILNĪGS AIZLIEGUMS	Sociālais reitings, sejas atpazīšana publiskās vietās reāllaikā, manipulatīvas MI sistēmas.
Augsts risks	STINGRA REGULĀCIJA	MI medicīnā, tieslietu sektorā, lēmumi par darbu vai kredītu - jāreģistrē ES datubāzē.
Ierobežots risks	PĀRREDZAMĪBAS PIENĀKUMS	Čatbotiem jāpaziņo, ka lietotājs runā ar MI, nevis cilvēku.
Minimāls risks	BRĪVA IZMANTOŠANA	Videospēļu MI, surogātpasta filtri, lielākā daļa ikdienas MI rīku (ChatGPT, Claude u.c.).

Kas ir datu šifrēšana?

Šifrēšana pārvērš Tavus datus neizlasāmā kodā. Tikai ar speciālu atslēgu dati tiek 'atšifrēti'. Pat ja hakeris iegūst datus, bez atslēgas tie ir bezjēdzīgi.

WhatsApp un Signal

End-to-end šifrēšana - pat uzņēmums nevar izlasīt Tavas ziņas. Ideāli sensitīvai saziņai darbā.

Google Drive

Faili tiek šifrēti glabāšanā, lai tie nebūtu pieejami hakeriem servera uzlaušanas gadījumā.

Swedbank lietotne

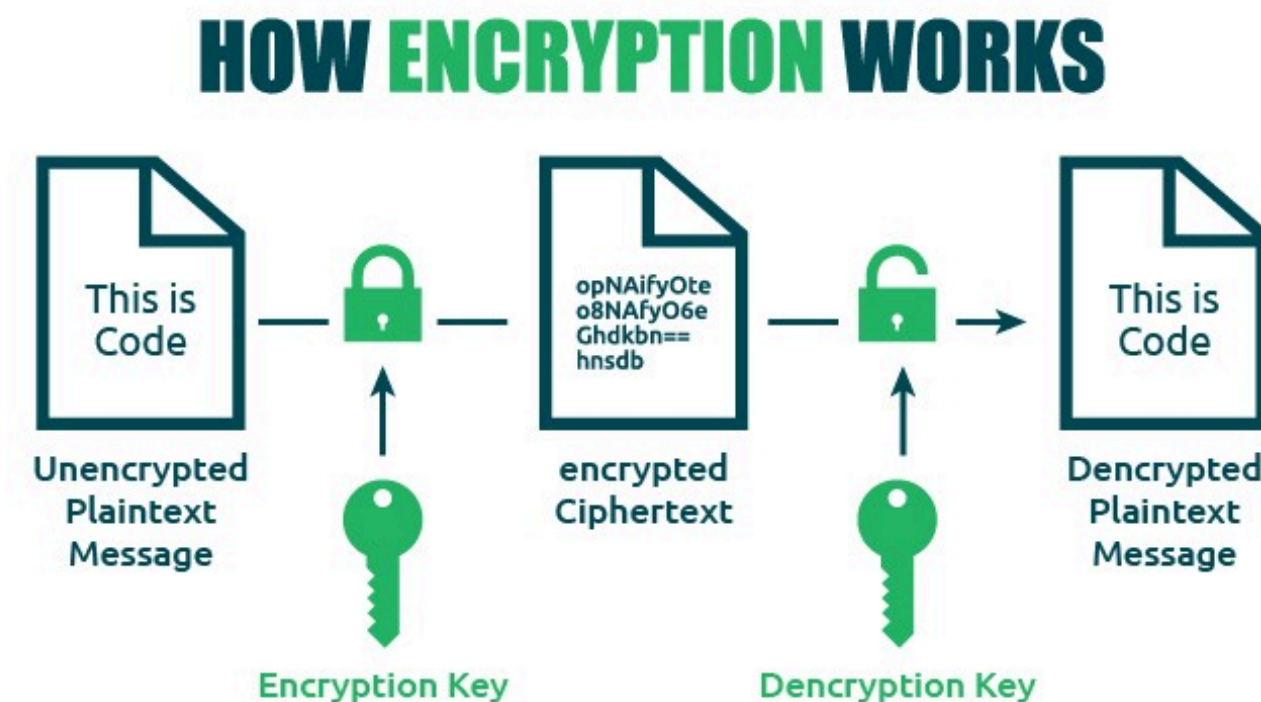
Visi maksājumu dati tiek šifrēti ceļā starp Tavu telefonu un bankas serveriem.

Ollama (lokāls MI)

Dati paliek Tavā datorā, nekad nepārsūtās uz ārējiem serveriem. Augstākais privātuma līmenis.

Kā uzņēmumi var aizsargāt datus?

- **Šifrēšana:** Aizsargā datus, padarot tos nelasāmus nepiederošām personām.
- **Piekļuves kontrole:** Tikai autorizēti darbinieki var redzēt datus.
- **Datu anonimizēšana:** Personas dati tiek pārveidoti tā, lai nevar identificēt lietotāju.
- **Regulāras drošības pārbaudes:** Testē sistēmu, lai atrastu ievainojamības.
- **Izglītošana:** Darbinieki tiek mācīti atpazīt riskus un pareizi rīkoties ar datiem.



Lielākā daļa uzņēmumu, kas regulāri veic datu šifrēšanu un darbinieku drošības apmācības, samazina datu noplūdes risku līdz pat 70%.

Kā identificēt un novērst drošības riskus?

Risku identificēšana:

- Auditi un drošības pārbaudes
- Monitorings, lai pamanītu neparastas darbības

Risku novēršana:

- Atjaunot programmatūru un aizsardzības sistēmas
- Ieviest iekšējās politikas un procedūras datu aizsardzībai
- Ātra reakcija uz incidentiem (datu noplūdes gadījumā)

2019. gadā Capital One banka ASV piedzīvoja noplūdi, kur personīgi dati vairāk nekā 100 miljoniem klientu (vārdi, adreses, sociālās apdrošināšanas numuri un bankas kontu informācija) tika pieklūti hakeru dēļ.

- Noplūde notika, izmantojot nepareizu serveru konfigurāciju.
- Bija milzīgas juridiskas un finanšu sekas bankai, kā arī klientu uzticības zudums.

Kā paskaidrot, kā dati tiks izmantoti?

- Lietotājam jāsaprot, kādi dati tiek vākti un kādam mērķim.
- Piemērs: “Mēs izmantojam jūsu e-pastu tikai, lai nosūtītu jaunumu vēstules, nevis pārdotu trešajām pusēm.”
- Izvairīties no sarežģīta juridiska teksta.

The screenshot shows a website interface for 'NESTE' with a privacy policy page titled 'Kāpēc mēs apkopojam Jūsu personas datus un kā tos izmantojam?'. The page content is partially obscured by a red dashed border. A red box highlights the right side of the page, which contains the following text:

Kāpēc mēs apkopojam Jūsu personas datus un kā tos izmantojam?

Mēs vācam personas datus, lai pārvaldītu mūsu klientu attiecības ar jums, mērķa mārketingu un izstrādātu produktus un pakalpojumus atbilstoši mūsu klientu vēlmēm. Mēs apstrādājam jūsu personas datus tikai iepriekš noteiktiem un likumīgiem mērķiem.

- Klientu attiecību pārvaldība
- Jūsu kredīspēju novērtēšana
- Mērķorientētais mārketingu
- Sadarbības uzsākšanas process

At the bottom of the page, there is a cookie consent banner with the text: "cookies", you agree to the storing of cookies on your device to enhance site navigation, analyze site usage, and assist in our marketing efforts. Below this text are three buttons: "Cookie Settings", "Necessary cookies only", and "Accept All Cookies".

Daudzās vietnēs piekrišanas paziņojumi tiek rādīti tā, ka lietotājs gandrīz spiests nospiest 'Piekrītu'. Piemēram, lapa tiek aizmiglota vai bloķēta, līdz lietotājs apstiprina sīkdatnes. Tādējādi piekrišana nav patiesa izvēle, bet drīzāk piespiedu solis.

Ko nozīmē "piekrišana" un datu izmantošanas atļauja?

Kas ir "piekrišana"?

- Piekrišana nozīmē, ka lietotājs brīvprātīgi dod atļauju vākt un izmantot viņa personas datus.
- Tā ir skaidra izvēle, nevis automātiska vai pasīva piekrišana.
- Piemērs: uzklikšķini "Piekrītu" privātuma politikā vai lietotnes noteikumos.

Kas ir datu izmantošanas atļauja?

- Tā nosaka, kā uzņēmums drīkst izmantot lietotāja datus.
 - Personalizētas reklāmas
 - Pakalpojumu uzlabošana
 - Datu nodošana trešajām pusēm (ja lietotājs piekrīt)



*Lietotājam jābūt iespējai atteikties vai atsaukt piekrišanu jebkurā brīdī.
Uzņēmumiem jāinformē lietotāji skaidri un saprotami, kā dati tiks izmantoti.*

Situācijas, kad MI var radīt ieguvumu, bet arī risku

Ieguvums:

- Veselības diagnostika – MI ātri analizē medicīniskos attēlus un palīdz ārstiem atklāt slimības.
- Satiksmes plānošana – optimizē maršrutus, samazina sastrēgumus un ietaupa degvielu.
- Personalizēta mācīšana – MI pielāgo mācību materiālus skolēniem atbilstoši viņu spējām, uzlabo mācīšanās rezultātus.

Risks:

- Veselības dati var noplūst vai tikt izmantoti neētiski, piemēram, apdrošinātāji varētu atteikt polises.
- Satiksmes optimizācija dažās pilsētas daļās var radīt nevienlīdzību – piemēram, satiksme tiek optimizēta tikai bagātākajās vai centrālajās zonās, bet mazāk attīstītās zonas paliek atslēgtas.
- Personalizēta mācīšana var pastiprināt nevienlīdzību, ja dati vai algoritms izceļ noteiktus skolēnus.

Kā lasīt un interpretēt datu paziņojumus (privacy policy - privātuma politika)?

Vai tu lasi privātuma politiku, vai vienkārši piekrīti, jo tā ir gara un sarežģīta?

+371 22474467

info@kompetencu-centrs.lv

KOMPETENČU
CENTRS

SĀKUMS

JAUNUMI

PAR MUMS

KURSU KATALOGS

PRIVĀTUMA POLITIKA

Šī ir sabiedrības ar ierobežotu atbildību "DKC", reģistrācijas numurs 40203379714, juridiskā adrese: Āraišu iela 34, Rīga, LV-1039 (turpmāk – Mēs/Mūsu/Mums) Privātuma politika (turpmāk – Politika).

Politikas mērķis ir izskaidrot mūsu klientiem – datu subjektiem (turpmāk – Jūs/Jūsu/Jums), kā Mēs īstenojam personas datu apstrādi un to aizsardzību, kā arī aprakstīt citus ar fizisko personu datu apstrādi saistītos jautājumus. Mēs veicam atbilstošus pasākumus, lai nodrošinātu, ka Jūsu personas dati pie mums ir drošībā, kā arī, lai Jūsu personas datu apstrāde notiktu atbilstoši spēkā esošajiem normatīvajiem aktiem, mūsu iekšējām politikām un vadlīnijām.

Ņemot vērā, ka Mēs veicam Jūsu personas datu apstrādi, Mēs esam uzskatāmi par Jūsu personas datu pārziņi. Mūsu kontaktinformācija ar personas datu apstrādi saistītajos jautājumos ir:

1. e-pasts: info@kompetencu-centrs.lv, vai
2. Mūsu juridiskā adrese: Āraišu iela 34, Latvija, Rīga, LV-1039.

Šī privātuma politika ir izstrādāta saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679 (2016.gada 27.aprīlis) "Par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK" (Vispārīgā datu aizsardzības regula) (turpmāk – Regula), kā arī Fizisko personu datu apstrādes likumu un citiem normatīvajiem aktiem, kas regulē fizisko personu datu apstrādes jautājumus. Tāpēc arī šajā politikā lietotie termini un to jēga ir tāda pati, kā Regulas 4.pantā sniegtajās definīcijās.

Mēs aicinām laiku pa laiku visus datu subjektus rūpīgi iepazīties ar šo Politiku, lai iegūtu aktuālo informāciju par Mūsu kā datu pārziņa veiktajiem personas datu apstrādes procesiem, jo tie laika gaitā var mainīties.

Informāciju par datu apstrādi, kas veikta saistībā ar sīkdatnēm aicinām skatīt Mūsu Sīkdatņu politikā.

1. Uz ko attiecas šī politika un kādas personas datu kategorijas mēs apstrādājam?

Politiku piemēro attiecībā uz sekojošām datu subjektu grupām:

1. fiziskajām personām – Mūsu klientiem (tajā skaitā, potenciālajiem, bijušajiem un esošajiem);

Digitālā ētika

Tehnoloģijas pašas par sevi nav “labas” vai “sliktas” tie ir instrumenti.

Ētikas jautājums rodas tur, kā mēs tās izmantojam.

GPS var palīdzēt atrast ceļu → bet to var izmantot arī cilvēku izsekošanai.

Digitālā ētika

Privātums ir cilvēktiesības, bet digitālajā laikmetā to bieži uztver kā “ērtību, ko var apmainīt pret pakalpojumiem.

Piemērs: cilvēki piekrīt dalīties ar datiem, lai izmantotu bezmaksas lietotnes vai atlaides kartes.

Digitālā ētika

Lietotājiem ir tiesības saprast, kādi dati tiek vākti un kā tie tiks izmantoti.



Mēs novērtējam jūsu privātumu

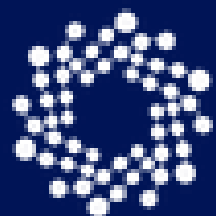
Mēs un mūsu [partneri](#) saglabājam un/vai piekļūstam informācijai ierīcē, piemēram, sīkfailiem, un apstrādājam personiskos datus, piemēram, unikālus identifikatorus un standarta informāciju, ko ierīce nosūta personalizētai reklāmai un saturam, reklāmu un saturu mērīšanai, auditorijas pētījumiem un pakalpojumu attīstībai. Ar jūsu atļauju mēs un mūsu partneri varam izmantot precīzus ģeogrāfiskās atrašanās vietas datus un identifikāciju, veicot ierīces skenēšanu. Jūs varat noklikšķināt, lai sniegtu piekrišanu mūsu un mūsu 1520 partneru veiktajai apstrādei, kā aprakstīts iepriekš. Jūs varat arī noklikšķināt, lai liegtu piekrišanu vai piekļūtu detalizētākai informācijai un pirms piekrišanas sniegšanas mainītu savas preferences. Lūdzu, ņemiet vērā, ka noteiktai jūsu personas datu apstrādei var nebūt nepieciešama jūsu piekrišana, bet jums ir tiesības iebilst pret šādu apstrādi. Jūsu iestatījumi attieksies uz vietņu grupu un tiks glabāti 13 mēnešus pakalpojumā IABGPP_HDR_GppString cookie. Jūs jebkurā laikā varat mainīt savas preferences vai atsaukt savu piekrišanu, atgriežoties uz šo vietni un noklikšķinot uz pogas "Noteikumi" lapas apakšā.

[Skatīt Privātuma politiku](#)

[PAPILDU OPCIJAS](#)

[PIEKRITU](#)

Vai ir ētiski sekot līdz lietotāju uzvedībai,
lai pārdotu vairāk?



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



No vienas puses

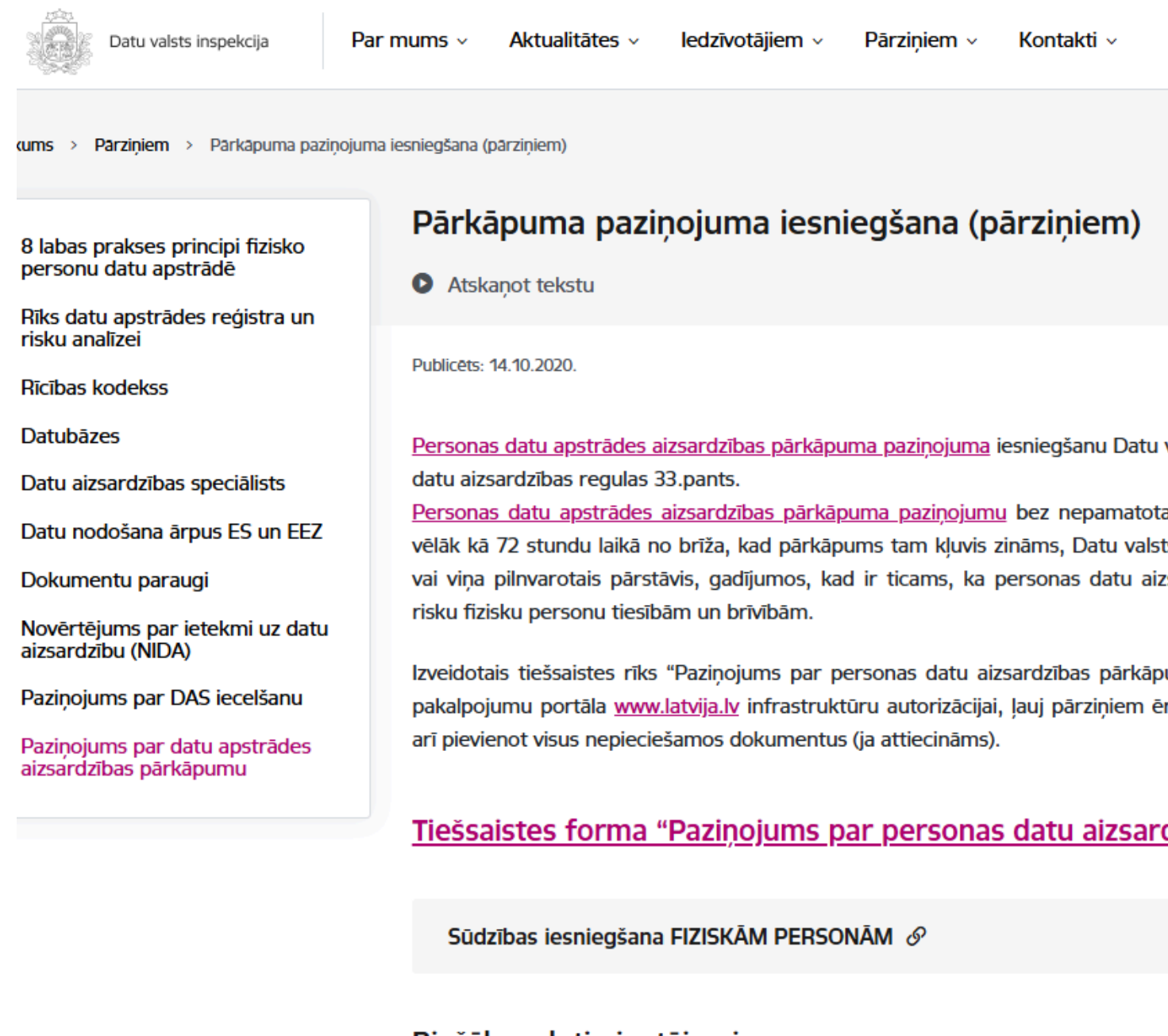
- Uzņēmumiem tas palīdz pielāgot reklāmas un sniegt piemērotākus piedāvājumus.
- Klients saņem saturu, kas atbilst viņa interesēm.

No otras puses

- Tas rada manipulācijas risku - cilvēkus ietekmē, nevis ļauj viņiem brīvi izvēlēties.
- Lietotāji bieži pat nezina, cik daudz par viņiem tiek vākti dati.

Kā ziņot par datu pārkāpumiem?

1. Pirmkārt, sazinies ar uzņēmuma atbalsta dienestu vai datu aizsardzības speciālistu.
2. Norādi konkrētus pārkāpumus
3. Precīzi pastāsti, kādi dati tika aizskarti un kā tu uzzināji par pārkāpumu.
4. Iesniedz oficiālu sūdzību
5. Daudzās valstīs ir datu aizsardzības iestādes (piemēram, Eiropā – [Datu valsts inspekcija](#)), kur var iesniegt sūdzību.
6. Saglabā pierādījumus
7. E-pastus, ekrānu uzņēmumus vai sarunas ar uzņēmumu – tas palīdzēs pierādīt pārkāpumu.
8. Sekojiet lietas gaitai
9. Datu aizsardzības iestāde var lūgt papildinformāciju vai veikt izmeklēšanu.



The screenshot shows the website of the Data Protection Inspectorate (Datu valsts inspekcija). The main navigation bar includes links for 'Par mums', 'Aktualitātes', 'Iedzīvotājiem', 'Pārziņiem', and 'Kontakti'. The breadcrumb trail indicates the path: 'Pārziņiem > Pārkāpuma paziņojuma iesniegšana (pārziņiem)'. The page title is 'Pārkāpuma paziņojuma iesniegšana (pārziņiem)'. A sidebar on the left lists various resources: '8 labas prakses principi fizisko personu datu apstrādē', 'Rīks datu apstrādes reģistra un risku analīzei', 'Rīcības kodekss', 'Datubāzes', 'Datu aizsardzības speciālists', 'Datu nodošana ārpus ES un EEZ', 'Dokumentu paraugi', 'Novērtējums par ietekmi uz datu aizsardzību (NIDA)', 'Paziņojums par DAS iecelšanu', and 'Paziņojums par datu apstrādes aizsardzības pārkāpumu'. The main content area includes a 'Publicēts: 14.10.2020.' date, a link to 'Atskaņot tekstu', and a paragraph explaining the process of reporting a data breach to the Inspectorate. It mentions that a breach must be reported if it is likely to result in physical or moral harm to individuals. A link to the 'Tiešsaistes forma "Paziņojums par personas datu aizsardzības pārkāpumu"' is provided. At the bottom, there is a button labeled 'Sūdzības iesniegšana FIZISKĀM PERSONĀM'.

Nākotnes izaicinājumi un atbildīga tehnoloģiju attīstība

Kā sagatavoties regulējuma izmaiņām:

- **Sekot jaunumiem** par datu aizsardzības likumiem (GDPR, CCPA u.c.).
- **Ieviešot elastīgas sistēmas**, kuras viegli pielāgot jauniem noteikumiem.
- **Apmācīt darbiniekus** par jauniem privātuma un drošības standartiem.

Galvenie nākotnes riski:

- **Datu noplūdes un uzlaušana** – lielāka datu koncentrācija var palielināt riskus.
- **Aizspriedumi algoritmos** – MI var neatbilstoši diskriminēt noteiktas grupas.
- **Nepareiza MI izmantošana** – piemēram, sejas atpazīšana vai profilēšana bez atļaujas.
- **Privātuma zaudējums** – vairāk datu nozīmē lielāku risku, ka lietotāju identitāte var tikt izmantota neētiski.

Ētika MI izmantošanā

Coca-Cola Ziemassvētku reklāmas piemērs

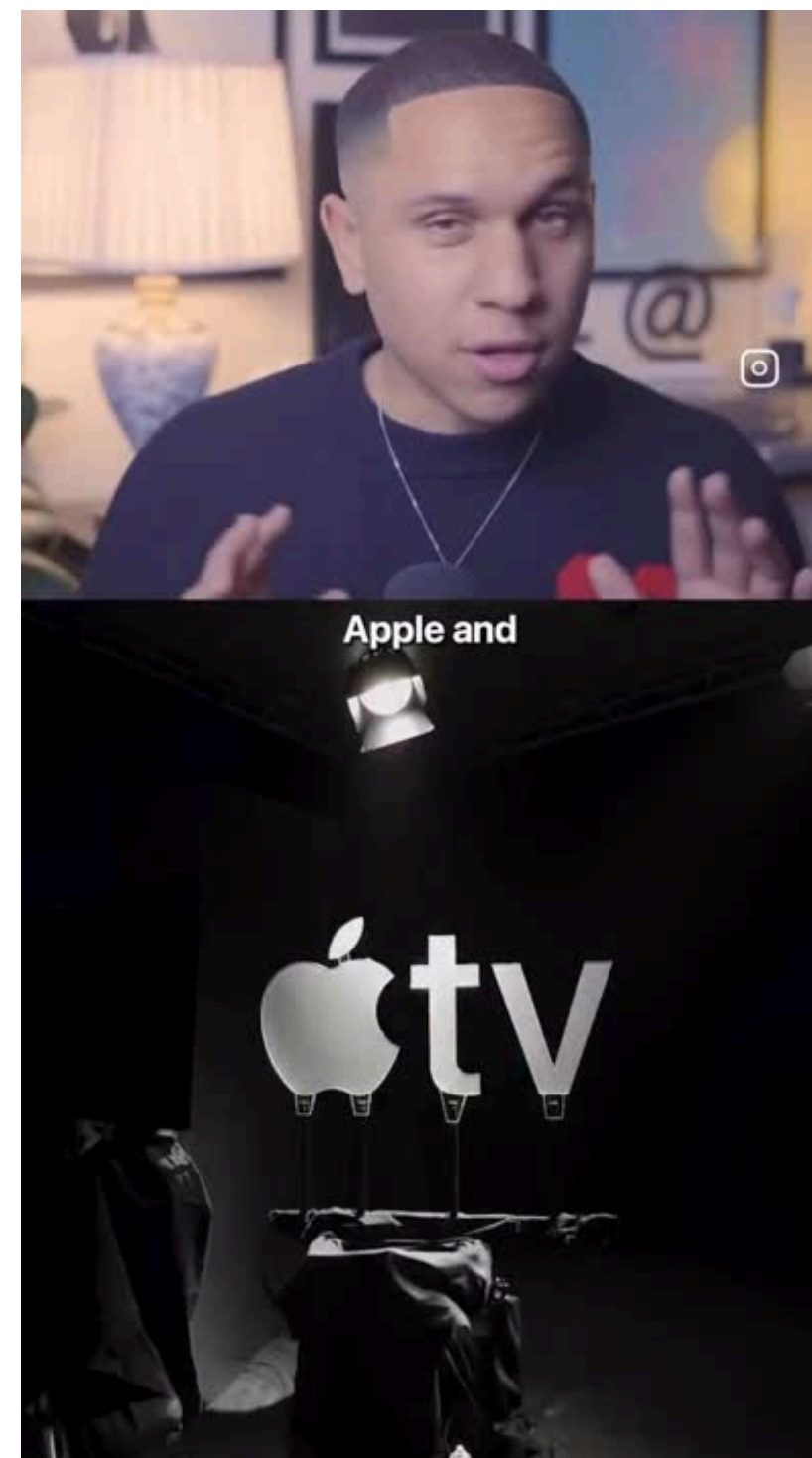
Coca-Cola radīja Ziemassvētku reklāmu, kas izmantoja mākslīgā intelekta ģenerētus vizuālos elementus un sižeta līnijas. Tas izraisīja plašas diskusijas par ētiku mārketingā.

Galvenās ētiskās problēmas:

- **Autentiskums:** vai "sirsnīgs svētku brīdis" vēl ir īsts, ja to ir radījis MI, nevis cilvēks?
- **Radošo profesiju vērtība:** vai MI aizvieto māksliniekus un stāstniekus?
- **Pārredzamība:** vai Coca-Cola skaidri norādīja, ka izmantots MI, vai radīja mākslīgu emocionālu ilūziju?

Ko tas māca:

Mārketingā MI var būt vērtīgs rīks, taču zīmoliem jābūt godīgiem par tā izmantošanu – īpaši, ja tas ietekmē emocionālu iesaisti un kultūras simbolus.

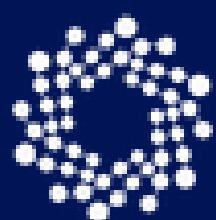


DISKUSIJA

Kur ir Tava personīgā robeža starp ērtībām un kibernetiskās drošības ML rīkos?

Ko Tu šodien mainīsi savā ikdienas ML lietošanā?

Pauze 10 min



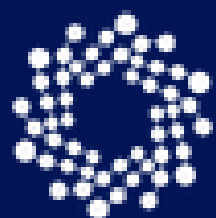
KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



4 Praktiskais darbs

AI + Kiberdrošības čekliste - 25 minūtes



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Praktiskais uzdevums

Uzdevums: Katras grupas ietvaros izvēlamies vienu MI rīku, ko izmantojat vai vēlētos izmantot darbā. Kopā izejam cauri čeklistei un novērtējam, cik drošs tas ir.

1. Vai MI rīks ir ES uzņēmums un atbilst GDPR?
2. Vai Tu vari pilnībā dzēst savus datus un čatu vēsturi?
3. Vai Tu nekad neievadi sensitīvus personas datus?
4. Vai ir iespējota 2FA un izmantots VPN publiskajos tīklos?
5. Vai Tu zini, kā atpazīt phishing un deepfake uzbrukumus?
6. Vai sensitīvam darbam izmanto lokālos MI modeļus (Ollama)?

☐☐☐☐☐☐

2 lietas, ko Tu vari izdarīt jau šodien

1

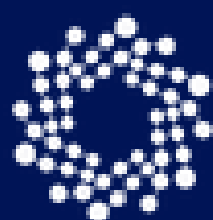
Atver ChatGPT iestatījumus

Ej uz Settings → Data Controls un izslēdz 'Improve the model for everyone'. Dzēs arī veco čatu vēsturi.

2

Iespējo 2FA visos MI kontos

ChatGPT, Grok, Claude, Midjourney - visur ieslēdz divfaktoru autentifikāciju. Izmanto autentifikatora lietotni, ne SMS.



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



Kopsavilkums

Datu valsts inspekcija

dvi.gov.lv

Latvijas uzraudzības iestāde datu aizsardzības jautājumos. Šeit vari iesniegt sūdzību, ja uzņēmums pārkāpj Tavas tiesības.

CERT.LV

cert.lv

Latvijas Informācijas tehnoloģiju drošības incidentu reaģēšanas institūcija. Aktuālie kiberdraudu brīdinājumi un ieteikumi.

Datu aizsardzība

Katrs prompts, foto un dokumenti, ko dod MI, ir Tava datu pēda. Apzināta rīcība aizsargā Tevi un citus.

Kiberdrošība

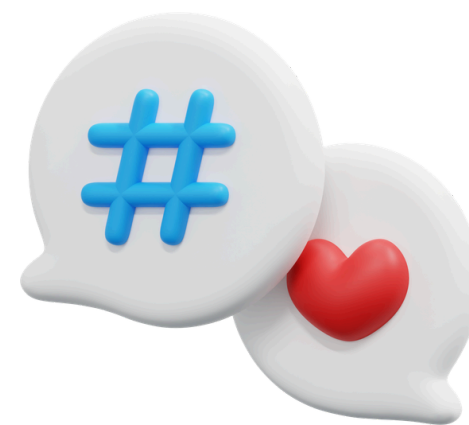
2FA, spēcīgas paroles, VPN un deepfake atpazīšana - tas nav sarežģīti, bet tas ir svarīgi.

Likumi

GDPR un AI Act aizsargā Tevi. Izmanto savas tiesības - pieprasīt, dzēst, kontrolēt savus datus.

Nobeigums

Jautājums: Kas ir tas, ko Jūs sev paņemat no šodienas lekcijas?

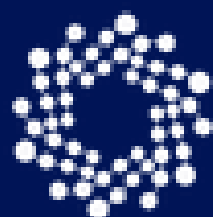


Nākamās lekcijas tēma - **Praktiskā MI kampaņas izstrāde**
Individuāls vai grupas projekts: kampaņas plānošana, MI rīku izvēle, izpilde

PALDIES!

Priecāšos par atsauksmēm, ieteikumiem vai
kādu komentāru.

Kitija Spēka-Štobe
@kitija.speka.stobe
kitija.speka.stobe@gmail.com



KOMPETENČU
CENTRS

ESF Plus projekta "Atbalsts pieaugušo izglītībai" 4.3.3.1/1/26/I/001



2027
Nacionālais
attīstības plāns