

# DATI IR VĒRTĪBA – SARGĀ TOS!



ŠEIT TU UZZINĀSI:

Kas ir personas dati?

Kā rīkoties, ja radušās problēmas?

Kur meklēt uzticamu informāciju?



Datu valsts inspekcija



Projekts tiek finansēts no  
Eiropas Savienības tiesību,  
vienlīdzības un pilsonības  
programmas (2014-2020. gads)



## Kas ir personas dati?

Personas dati ir jebkura informācija, kas attiecas uz tevi kā indivīdu. Piemēram, tavs vārds, adrese, e-pasta adrese, dzimšanas datums, fotogrāfijas, balss ieraksts un video, informācija par tavām interesēm un uzskatiem, informācija, ko par sevi esi norādījis sociālajos tīklos. Arī tava IP adrese\* un digitālās pēdas, ko esi atstājis, lietojot internetu, ir tavi personas dati.

\*IP adrese ir unikāls identifikators, kas tiek piešķirts datoram. Tu vari nelietot savu vārdu internetā, tomēr interneta lietotāju ir iespējams noteikt pēc viņa IP adreses.

Tādi personas dati, kas saistīti ar informāciju par cilvēka veselību, rases vai etnisko piederību, politiskajiem un filozofiskajiem uzskatiem vai seksuālo dzīvi, ir īpaši aizsargājami. Tos sauc par īpašu kategoriju personas datiem.

**!** Ir jābūt īpaši uzmanīgam, atklājot kādam šo informāciju.

Personas dati var sniegt plašu priekšstatu par cilvēku, un tie var tikt izmantoti gan labiem mērķiem (lai nodrošinātu tev piemērotāko iespēju mācīties, sniegtu palīdzību, kad tā ir vajadzīga), gan arī negodīgiem mērķiem krāpnieciskos vai manipulatīvos nolūkos.



Lai sevi pasargātu no nepatīkamām emocijām, mēģinājumiem manipulēt vai pat smagiem noziegumiem, ir svarīgi domāt par savu personas datu drošību gan reālajā dzīvē, gan virtuālajā vidē.

## Atceries!

Vienmēr, kad tu lieto internetu, tu atstāj savas digitālās pēdas, kas nekur nepazūd un var saglabāties uz visiem laikiem.



Ikreiz, kad tu meklē informāciju, izmantojot Google meklētāju, šī informācija tiek saglabāta – sākot no meklēšanas vaicājuma (vārda vai frāzes, ko ierakstīji) līdz informācijai par jebkuru lapu, ko tu atver. Tevis Facebook veiktā atzīme

**"Patīk"** vai **"Nepatīk"**, atzīmējot to pie kādas bildes vai ieraksta, var būt redzama cilvēkiem, kuri nav tavu draugu lokā.



Arī ikreiz, kad aizpildi bezmaksas testu, lai noskaidrotu, kura slavenība bērībā ir bijusi līdzīga tev, ikreiz, kad dalies sociālajos tīklos ar ziņu, spied

**"Sekot"**, **"Patīk"** vai **"Nepatīk"**,

vai vienkārši klikšķini uz kādām ziņām lapā, šī informācija saglabājas.

Šie dati var tikt izmantoti mārketinga nolūkos, kā rezultātā tavā datorā "nejauši" sāk parādīties reklāmas, kas saistītas ar tavām interesēm (ja priedējies par kaķu bildēm – informācija par jauno kaķu barību; kosmētika, ko izmanto slavenība, kurai seko), vai arī interesēm, kādas parasti ir citiem cilvēkiem ar līdzīgu lietotāja profilu kā tev.



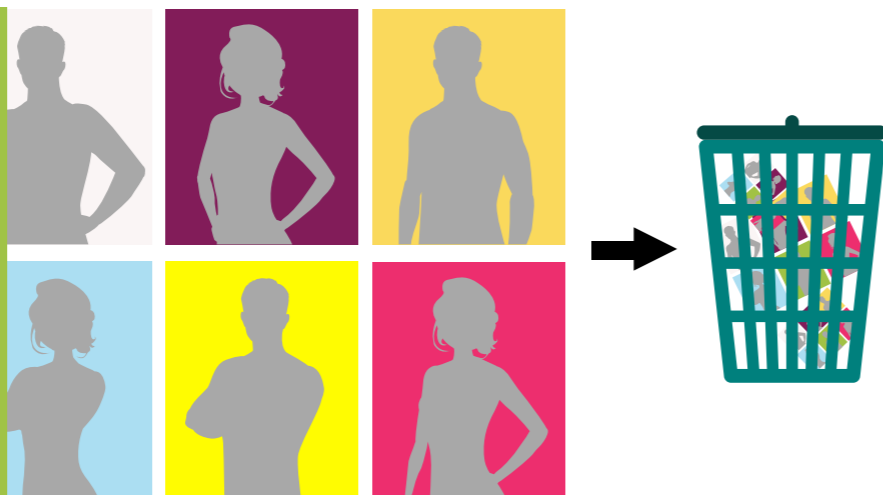
Dažas vietnes piedāvā iespēju redzēt un mainīt reklāmas iestatījumus savā kontā. Eiropas Savienības noteikumi paredz, ka noteiktās situācijās ikvienam ir tiesības prasīt savu datu dzēšanu (tiesības tikt aizmirstam).

Vairāk informācijas vari atrast šeit:

<https://www.dvi.gov.lv/lv/zinas/par-visparejo-kriteriju-sarakstu-sudzibu-partiesibam-tikt-aizmirstam-interneta-vide-izskatsanai-2/>

## Piemērs:

Ja esi ievietojis sociālajos tīklos savu fotogrāfiju, tev ir tiesības to dzēst jebkurā brīdī.



Arī daudzos citos sociālajos tīklos tu vari mainīt reklāmas iestatījumus. Ieejot savā profilā, meklē sadaļu, kas varētu saukties "Personalizēt" vai "Privātums" un tad meklē sadaļu "Reklāma".

Uzzini, kā mainīt reklāmas iestatījumus Snapchat šeit:




Informāciju par to, kā mainīt reklāmas iestatījumus Twitter tu vari atrast šeit:



Padomus, kā mainīt reklāmas iestatījumus TikTok tu atradīsi šeit:



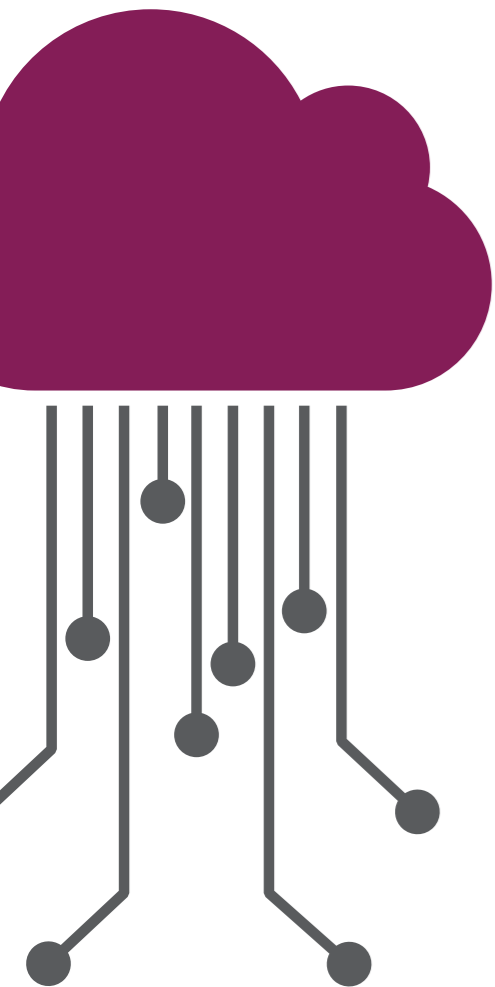


Ņem vērā, ka, pat ja esi "iztīrījis"  
savu interneta pārlūka vēsturi, izdzēsis vecās ziņas  
sociālajos tīklos vai fotogrāfijas savā profilā,  
pastāv liela iespēja, ka sociālo tīklu vai  
e-pasta uzturētāji tomēr saglabā šos datus,  
radot tev maldīgu pārliecību par datu dzēšanu.

Lai palīdzētu cilvēkiem kontrolēt savu datu izmantošanu, sociālo tīklu, e-pasta platformu un mājaslapu uzturētājiem ir pienākums sniegt informāciju par to, kā tiks izmantoti viņu personas dati. Parasti šī informācija tiek sniegta

Privātuma politikā.





Privātuma politikā vajadzētu atrasties informācijai par to, kādus tavus personas datus attiecīgā vietne apstrādā, kādiem mērķiem tas tiek darīts un kam vēl vietne "nodod" tavus datus.

Tāpat Privātuma politikā vajadzētu būt informācijai, par to, kas notiek ar tavām "dzēstajām" ziņām vai "izdzēsto" profilu (piemēram, lietotāja profils netiek vienkārši deaktivizēts – joprojām ir pieejams vietnes uzturētājiem, bet nav redzams ne tev, ne citiem lietotājiem). Tomēr ne vienmēr vietnes sniedz pilnīgu un precīzu informāciju par datu izmantošanu.

Facebook privātuma  
politiku tu atradīsi šeit:



Instagram privātuma  
politiku vari apskatīt šeit:



## Padomā!

Vai sociālo tīklu, spēles vai tērzētavas (čata) uzturētājam tiešām vajadzētu sniegt visu prasīto informāciju? Piemēram, tavas atrašanās vietas datus, informāciju par skolu, kurā mācies, savu adresi, to, kā šobrīd jūties, visu par tavām interesēm.

**Internets** ir ātrākais veids, kā tu vari pavēstīt visiem par tev svarīgu vai kādu satraucošu notikumu tavā dzīvē. Tomēr, vai esi aizdomājies, ka, publicējot fotogrāfijas un video internetā, tu pavisam nejauši svešiniekiem vari parādīt, kādas vērtīgas mantas ir atrodamas tavās vai tavu draugu mājās?

Savukārt, daloties ar ikvienu par lietām, ko plāno darīt, tu vari publiskot arī laiku, kad neviena nebūs mājās. Ja internetā publicē biļetes no koncerta, kuru plāno apmeklēt kopā ar visu ģimeni, ir viegli saprast, kurā laikā mājā neviena nebūs.



- Lietojot sociālos tīklus, izmanto privātuma iestatījumus. Noskaidro, kādi privātuma iestatījumi sociālajā tīklā tiek izmantoti noklusējuma režīmā (t.i., kurus tavus ierakstus, bildes, video un citu informāciju varēs redzēt jebkurš).
- Privātuma iestatījumu uzstādīšana var būt sarežģīta, bieži mainīties un tie var nebūt pieejami latviešu valodā. Tādēļ nekautrējies prasīt palīdzību un neaizmirsti pārlicināties, vai iestatījumi strādā tā, kā esi iedomājies\*.
- Ja pārtrauc lietot kādu kontu, izdzēs to. Tas novērsīs risku, ka šis konts tev nezinot var tikt uzlauzts un izmantots noziedzīgām darbībām.

\* Dodies uz sadaļu "Kā rīkoties, ja radušās problēmas?" 24. lpp



Informāciju par YouTube  
privātuma iestatījumiem  
vari atrast šeit:



Informāciju par Facebook  
privātuma iestatījumiem  
atradīsi šeit:



Informāciju par Snapchat  
privātuma iestatījumiem  
vari atrast šeit:



Informāciju par Instagram  
privātuma iestatījumiem  
vari atrast šeit:



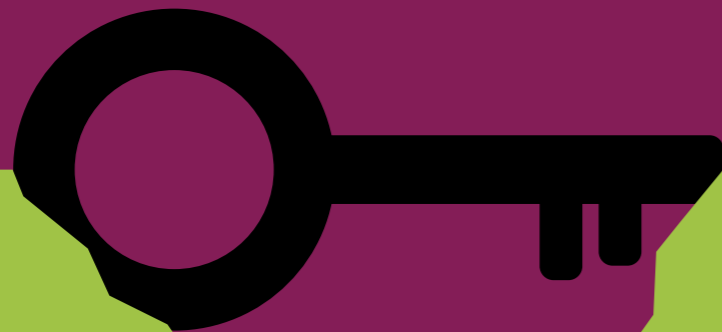
Informāciju par TikTok  
privātuma iestatījumiem vari  
atrast šeit:



# Atceries!

Kamēr bilde ir publiska, tā ir pieejama visiem.  
Kāds var to paspēt lejuplādēt vai pārpublicēt.

Viss, kas nonāk internetā, nokļūst ārpus tavas kontroles.  
Tādēļ domā, kur un ar kādu informāciju tu dalies.  
Tā tu vari pasargāt sevi, savu ģimeni, draugus.



- Vienmēr kārtīgi padomā pirms kaut ko publicē savā sociālo tīklu kontā. Kamēr bilde ir publiska, tā ir pieejama visiem. Arī negatīvi komentāri vēlāk var "atspēlēties".
- Runājot tērzētavās (čatos), vai spēlējot spēles internetā, atceries, ka nevienam nav nepieciešama personīga informācija par tevi.
- Domā, ko publisko arī par citiem (savu ģimeni, draugiem, skolasbiedriem, skolotājiem). Ja vēlies dalīties ar informāciju, kas skar citus cilvēkus, vienmēr noskaidro viņu domas par to.
- Nekad nepakļaujies steidzināšanai vai draudiem, ja kāds prasa publiskot vai nosūtīt kaut ko, ko īsti nevēlies.





**AHĀ, TAD TĀ VIŅA PAR MANI UZZINĀJA!**

Sameklē informāciju par sevi internetā.

Ieraksti interneta meklētājprogrammā:

"Vārds Uzvārds"; "Vārds Uzvārds  
dzīvesvieta"; "Vārds Uzvārds skola"

un uzzini, ko par tevi viegli var  
atrast ikviens.

## Kā sevi pasargāt?

Lai sevi pasargātu, ir svarīgi atcerēties arī par drošību, lietojot internetu.  
Vienmēr izmanto paroles visur, kur vien tas nepieciešams (arī telefonā),  
un atceries par paroles drošību:

- Drošai parolei būtu jā sastāv no lielajiem un mazajiem burtiem, cipariem un simboliem;
- Paroli **nav ieteicams veidot** no viegli uzminamas personīgas informācijas (piemēram, savs vārds, iesauka, ģimenes locekļa vai drauga vārds; mājdzīvnieka vārds vai šķirne, lietas, kas tev ir īpaši mīļas); skaitļiem vai burtiem, kas uz klaviatūras izvietoti viens aiz otra ("123456" vai "qwerty") vai ir vienkārši un viegli uzminamas (piemēram, "saulīte", "saulīte123", "skola", "parole", "0000000");
- Izvairies no datora piedāvātās iespējas "atcerēties paroli"! **Nekad neizmanto iespēju "atcerēties paroli"**, ja izmanto publisku datoru (piemēram, skolā vai bibliotēkā);

- Lai veidotu grūti uzminamu paroli, **izmanto paroles frāzi – paroli, kas sastāv no vairākiem vārdiem** (piemēram, fragments no dziesmas). Parole būs viegli iegaumējama tev, bet grūti uzminama kibernetziedzniekiem.

- Izmantojot publiski pieejamu datoru, rēķinies, ka citi lietotāji pārlūkprogrammas vēsturē varēs redzēt vietnes, ko esi apmeklējis, kā arī datnes (failus), ko esi lejuplādējis. Lai izvairītos no nepatīkamām situācijām, **pēc datora lietošanas izdzēs pārlūkprogrammas vēsturi un savas lejuplādētās datnes (failus).**

- **Esi piesardzīgs attiecībā uz saitēm vai pielikumiem, ko saņem gan e-pastā, gan sociālajos tīklos:** draugs, kurš atsūta tev dīvainu ziņu vai kaut ko, kas nav viņam raksturīgs, visticamāk var izrādīties ļaundaris, kurš tikai izliekas par draugu. Ja tev rodas kaut mazākās šaubas, sazinies ar sūtītāju, piemēram, piezvani un pajautā, vai viņš tev tiešām ko sūtījis.



- Publiski pieejamos **“Wi - Fi”** tīklus neizmanto, lai pieslēgtos savam profilam. Pastāv varbūtība, ka krāpnieki, pieslēdzoties tīklam, var pārtvert privāto informāciju. Nekad neiepērcies, izmantojot publiskos **“Wi-Fi”** tīklus.

- Lejupielādējot telefonā dažādas aplikācijas, **centies izvēlēties tās, kuras ir visiem labi zināmas** un ir iespējams pārliicināties par to drošību.



# Kā rīkoties, ja radušās problēmas?

Lietojot sociālos tīklus, vienmēr savlaicīgi noskaidro, vai varēsi izmantot bloķēšanas un dzēšanas iespējas. Tāpat noskaidro, kā par pārkāpumiem informēt attiecīgo sociālo mediju. Tomēr, ja tiešsaistē ir noticis kas tāds, kas tevi satrauc, **vienmēr vari meklēt palīdzību** arī citur:

- Par notikušo informē vecākus vai kādu labi pazīstamu pieaugušo.
- Pastāsti par notikušo vai prasi padomu mājaslapā - **drossinternets.lv**, izmantojot ziņojuma formu – ZIŅOT - vai rakstot uz e-pastu: **zinojumi@drossinternets.lv**. **<https://drossinternets.lv/lv/zinot>**. Lai arī ziņojuma formā ir lauks, kurā vari norādīt savu vārdu un uzvārdu, **rakstīt vari arī anonīmi**.
- Ziņo par situāciju Valsts policijas mobilajā lietotnē - **"Mana drošība"** (lejupielādē bez maksas *Google Play* un *App Store*)
- Vai zvani uz Valsts bērnu tiesību aizsardzības inspekcijas **Uzticības tālruni: 116111**



# Kur meklēt uzticamu informāciju?

**Datu valsts inspekcija**  
dvi.gov.lv

**Latvijas Drošāka interneta centrs**  
drossinternets.lv

**Informācijas tehnoloģiju  
drošības incidentu novēršanas institūcija**  
esidross.lv

**UK Safer Internet Centre**  
saferinternet.org.uk

**Better Internet for Kids**  
betterinternetforkids.eu

# DPSME

Šīs publikācijas finansējumam ir saņemts Eiropas Komisijas atbalsts.  
Šajā publikācijā ir atspoguļots vienīgi Datu valsts inspekcijas viedoklis, un Eiropas Komisija  
neuzņemas atbildību par publikācijā ietvertās informācijas tālāko izmantošanu.