სახელმწიფო ინსპექტორის სამსახური

TIK TOK - რამდენად უსაფრთხოა თქვენი საყვარელი აპლიკაცია

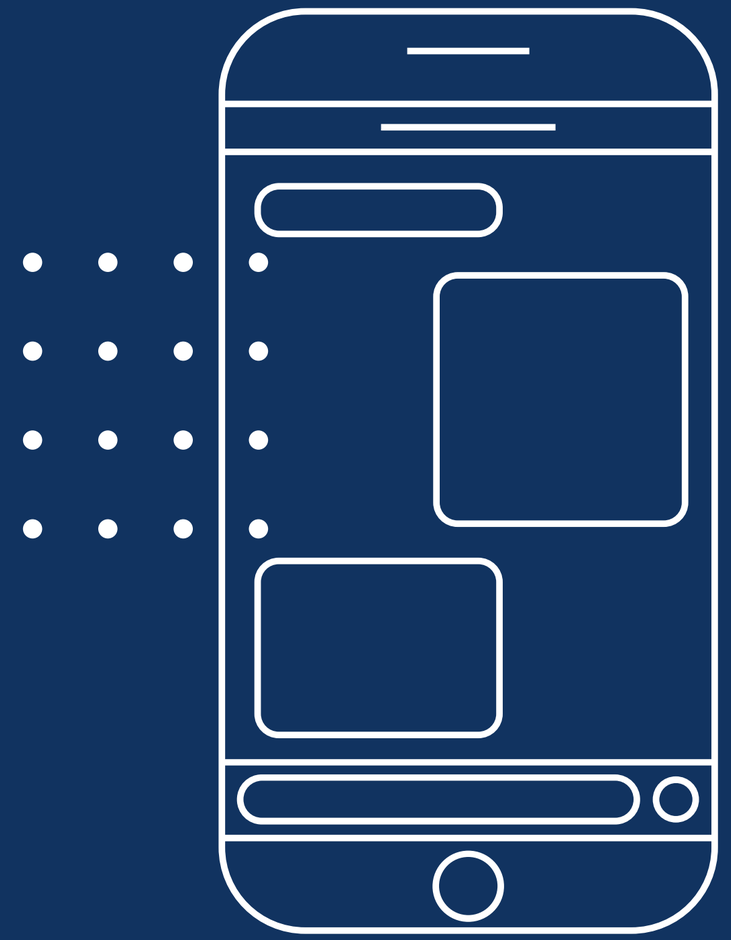
ჩინური კომპანიის **Bytedance**-ს აპლიკაცია **TikTok** მთელს მსოფლიოში დიდი პოპულარობით სარგებლობს. იგი იძლევა აპლიკაციაში ვიდეოების დამუშავების შესაძლებლობას. მისდამი განსაკუთრებული ინტერესი პანდემიის დროს გაჩნდა. ცნობილმა ადამიანებმა აქტიურად დაიწყეს სხვადასხვა სახის გასართობი ვიდეოების განთავსება, რამაც აპლიკაციის ცნობადობა კიდევ უფრო გაზარდა. აპლიკაცია საქართველოშიც დიდი პოპულარობით სარგებლობს.

ჩვენი მოქალაქეების უკეთ ინფორმირების, ინტერნეტის და ტექნოლოგიური სიახლეების ფონზე თითოეული ჩვენგანის პერსონალური მონაცემების დაცვის მიზნით, სახელმწიფო ინსპექტორის სამსახურმა შეისწავლა **TikTok**-ის ამჟამინდელი ფუნქციები, აპლიკაციის კონფიდენციალურობის პოლიტიკა და სხვადასხვა ქვეყნის მონაცემთა დაცვის წამყვანი ორგანიზაციების რეკომენდაციები.

რა მონაცემებს აგროვებს აპლიკაცია ჩვენ შესახებ?

აპლიკაციის კონფიდენციალურობის პოლიტიკა განსხვავებულია მომხმარებლის საცხოვრებელი ადგილის მიხედვით. კერძოდ, არსებობს სამი სახის კონფიდენციალურობის პოლიტიკა - ამერიკის შეერთებულ შტატებში მცხოვრები პირებისთვის, ევროპის ეკონომიკურ ზონაში შემავალ ქვეყნებში [1]/ შვეიცარიაში მცხოვრები პირებისთვის და სხვა ქვეყნებში მცხოვრები მომხმარებლებისთვის. შესაბამისად, აპლიკაციის იმ მომხმარებლებისთვის, რომელებიც ცხოვრობენ საქართველოს ტერიტორიაზე, მოქმედებს „სხვა ქვეყნებისთვის“ განსაზღვრული კონფიდენციალურობის პოლიტიკა.

აპლიკაციის სრული ფუნქციონალის გამოყენებისთვის აუცილებელია მომხმარებლის რეგისტრაცია. აპლიკაციაში რეგისტრაციისას მომხმარებელი გასცემს შემდეგი სახის პერსონალურ მონაცემებს: სახელი, დაბადების თარიღი (როცა ხდება ამ მონაცემის მითითება), ელექტრონული ფოსტის მისამართი ან/და ტელეფონის ნომერი.



[1]
ევროპის ეკონომიკურ ზონაში შედის ევროკავშირის წევრი ქვეყნები, ისლანდია, ლიხტენშტაინი და ნორვეგია.

რეგისტრაცია შესაძლებელია სხვადასხვა სოციალური ქსელის მეშვეობით. თუ მომხმარებელი აპლიკაციაში რეგისტრირება Facebook-ის, Twitter-ის, Instagram-ის ან მსგავსი პლატფორმის გამოყენებით, აპლიკაცია მომხმარებლის თანხმობით, დამატებით იღებს მითითებულ პლატფორმებზე მომხმარებლის პირად გვერდზე არსებული ინფორმაციის ნაწილს. ამასთან, აპლიკაცია აგროვებს ინფორმაციას მომხმარებლების ქცევის (მაგალითად, მომხმარებლის მიერ ბოლო პერიოდში განხორციელებული შესყიდვების) შესახებ.

Google Play-ში დაფიქსირებული მონაცემებიდან გამომდინარე აპლიკაცია თქვენს მოწყობილობაში ჩაწერისა და მისი გამოყენების დროს მოითხოვს ქვემოთ ჩამოთვლილ მონაცემებზე და მოწყობილობის ფუნქციებზე წვდომას:

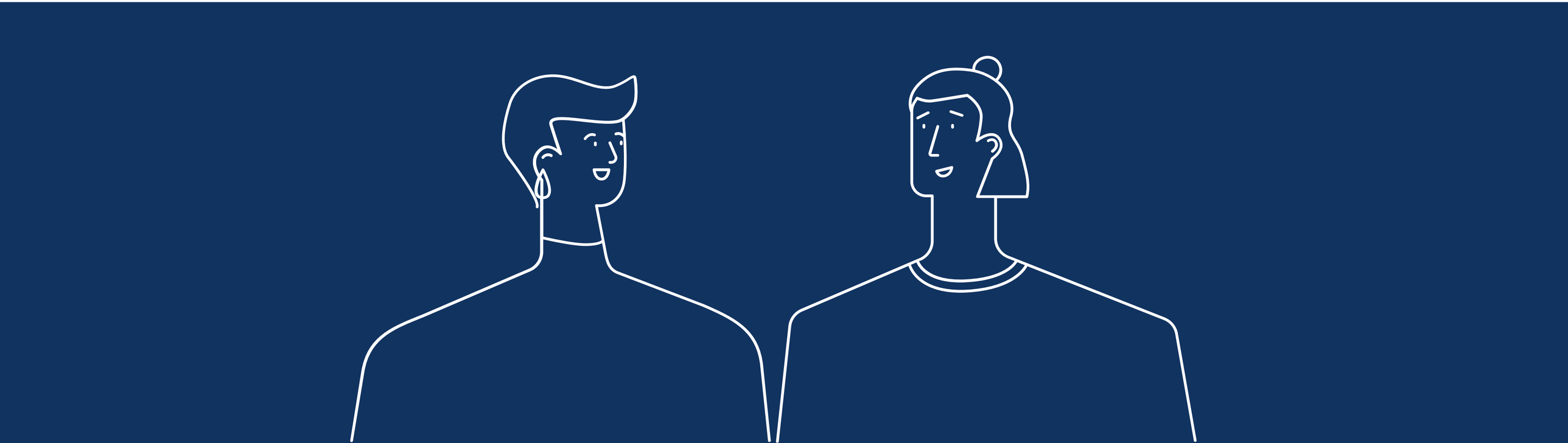
- **მოწყობილობის და აპლიკაციის ისტორია (Device & app history)** - აღნიშნული წვდომა აპლიკაციას საშუალებას აძლევს მიიღოს ინფორმაცია მოწყობილობაში ჩაწერილი და მიმდინარედ გააქტიურებული აპლიკაციების/პროგრამების შესახებ. მაგალითად, თუ თქვენს მოწყობილობაში ჩაწერილი გაქვთ Facebook-ის, Viber-ისა და WhatsApp-ის აპლიკაციები და მიმდინარედ გააქტიურებულია ისინი, TikTok-ის აპლიკაციას შეუძლია აღნიშნული ინფორმაციის მიღება. აპლიკაციისთვის მოწყობილობის და აპლიკაციის ისტორიაზე წვდომის გათიშვა შეუძლებელია;

- **მიკროფონი - აუდიო ჩაწერა (Microphone-record audio)** - აღნიშნული წვდომის საშუალებით აპლიკაციას შეუძლია მოწყობილობის მიკროფონის გამოყენებით ნებისმიერ დროს განახორციელოს ხმის ჩაწერა, დამატებითი დადასტურების გარეშე. აპლიკაციის საშუალებით მიკროფონის პირველი გამოყენების დროს, იგი გეკითხებათ მოწყობილობის მიკროფონის გამოყენების ფუნქციაზე წვდომის მიღების შესახებ. მაგალითად, როდესაც პირველად გადაწყვეტთ ამ აპლიკაციის საშუალებით ვიდეოს ჩაწერას, აპლიკაცია მოგთხოვთ თქვენი მოწყობილობის მიკროფონისა და კამერის გამოყენების უფლებას. თქვენ შეგიძლიათ აპლიკაციას მისცეთ უფლება, დამატებითი დადასტურების გარეშე, შემდგომში გამოიყენოს თქვენი მოწყობილობის მიკროფონი. აპლიკაციას მიკროფონის გამოყენების ფუნქციაზე წვდომა შეგიძლიათ გაუთიშოთ ტელეფონის პარამეტრებიდან;

- **ტელეფონის მეხსიერება (Storage)** - მოცემული წვდომის საშუალებით აპლიკაციას შეუძლია განახორციელოს მოწყობილობის მეხსიერებაში ჩაწერილი მონაცემების წაკითხვა/დათვალიერება, ჩაწერა, წაშლა ან რედაქტირება. მაგალითად, თუ თქვენს მოწყობილობაში ჩაწერილი გაქვთ სურათები ან ვიდეოგამოსახულებები, აპლიკაციას შეუძლია მათი დათვალიერება. აღსანიშნავია, რომ აპლიკაცია თქვენი მოწყობილობის მეხსიერებაზე წვდომისათვის დამატებით გეკითხებათ ტელეფონში აპლიკაციის საშუალებით პირველი ვიდეო/აუდიო გამოსახულების შენახვის დროს. შესაბამისად, აპლიკაციას შეგიძლიათ მისცეთ უფლება დამატებითი დადასტურების გარეშე შემდგომში წვდომა ჰქონდეს თქვენს ტელეფონში ჩაწერილ სურათებზე ან ვიდეო გამოსახულებებზე. აპლიკაციას თქვენი მოწყობილობის მეხსიერებაზე წვდომა შეგიძლიათ გაუთიშოთ ტელეფონის პარამეტრებიდან;

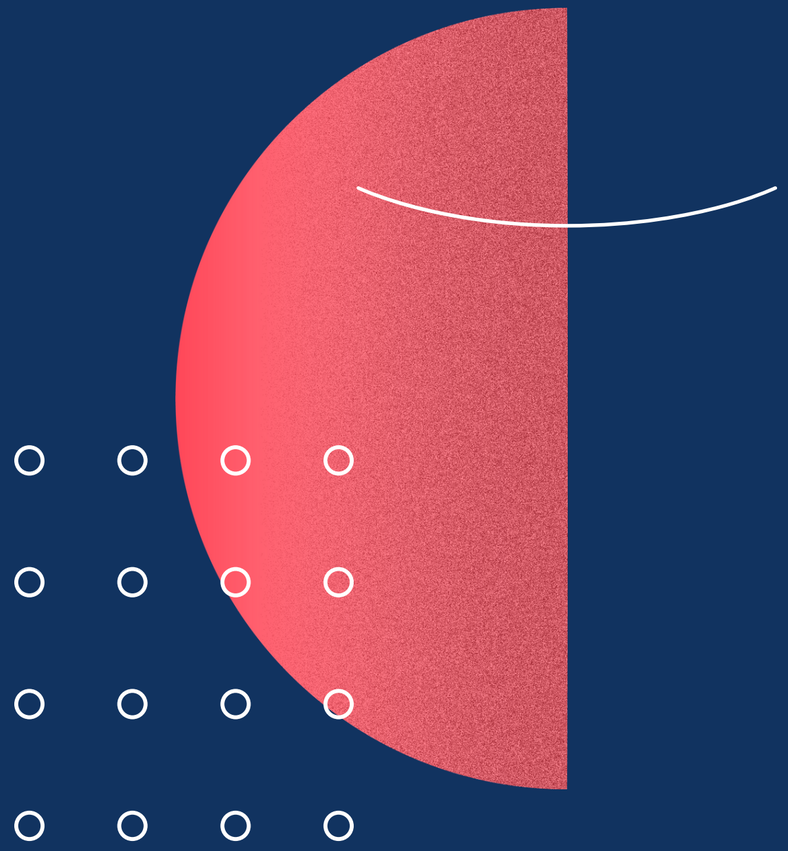
- **მაიდენტიფიცირებელი მონაცემები** - ანგარიშის დამატება ან წაშლა (Identity - add or remove accounts) - აღნიშნული წვდომის საშუალებით აპლიკაციას შეუძლია მოწყობილობაში ანგარიშების (Account) დამატება, ამოშლა და მათი პაროლების წაშლა. მაგალითად, თუ თქვენს მოწყობილობაში ჩაწერილია Facebook-ის მობილური აპლიკაცია, ამ წვდომის საშუალებით TikTok-ის აპლიკაციას შეუძლია მიიღოს ინფორმაცია იმის შესახებ, თუ Facebook-ის რომელი ანგარიში არის დარეგისტრირებული ტელეფონში. ასევე, შეუძლია ამ ანგარიშის პაროლის წაშლა. აპლიკაციისთვის მოწყობილობაში ანგარიშის დამატების ან წაშლის ფუნქციაზე წვდომის გათიშვა შეუძლებელია;

- **კამერა - ფოტო და ვიდეო გადაღება (Camera - take pictures and videos)** - მოცემული წვდომის საშუალებით აპლიკაციას შეუძლია ნებისმიერ დროს განახორციელოს კამერაზე წვდომა (სურათების და ვიდეოს გადაღება) დამატებითი დადასტურების გარეშე. მაგალითად, TikToK-ის აპლიკაციას შეუძლია მოწყობილობის კამერის საშუალებით ვიდეო ან ფოტო გამოსახულება ჩაიწეროს, მაშინაც კი, როდესაც აპლიკაციას არ იყენებთ. აღსანიშნავია, რომ აპლიკაცია თქვენი მოწყობილობის კამერით გადაღების ფუნქციაზე წვდომის მისაღებად დამატებით შეგეკითხებათ აპლიკაციის საშუალებით ვიდეო ან ფოტო გამოსახულების პირველი გადაღების დროს. მაგალითად, როდესაც პირველად გადაწყვეტთ ამ აპლიკაციის საშუალებით ვიდეოს ჩაწერას, აპლიკაცია მოგთხოვთ მოწყობილობის კამერისა და მიკროფონის გამოყენების უფლებას. შესაბამისად, აპლიკაციას შეგიძლიათ მისცეთ, შემდგომში დამატებითი დადასტურების გარეშე, თქვენი მოწყობილობის კამერით ვიდეო და ფოტო გამოსახულების გადაღების შესაძლებლობა. აპლიკაციისთვის კამერით გადაღების ფუნქციაზე წვდომა შეიძლება გაუთიშოთ ტელეფონის პარამეტრებიდან;



- **Wi-Fi კავშირის შესახებ ინფორმაცია (Wi-Fi connection information)** - აღნიშნული წვდომა აპლიკაციას საშუალებას აძლევს ნებისმიერ დროს მიიღოს ინფორმაცია მოწყობილობაში უკაბელო ქსელთან წვდომისა და უკაბელო მოწყობილობის დასახელების შესახებ. მაგალითად, თუ თქვენს სახლში გაქვთ უკაბელო მოწყობილობა (Wi-Fi) ინტერნეტთან კავშირისათვის, რომელსაც თქვენი მოწყობილობა უკავშირდება, TikToK-ის აპლიკაცია კითხულობს თქვენი უკაბელო მოწყობილობის დასახელებას. გარდა ამისა, მას აქვს წვდომა ყველა უკაბელო მოწყობილობის (Wi-Fi) დასახელებებთან, რომელებიც ოდესმე გამოგიყენებიათ და მათ შესახებ მონაცემები თქვენს მოწყობილობაშია შენახული. აპლიკაციისთვის თქვენი მოწყობილობის Wi-Fi კავშირის შესახებ ინფორმაციაზე წვდომის გათიშვა შეუძლებელია;

- **კონტაქტები - კონტაქტების წაკითხვა (Contacts - read your contacts)** - მოცემული წვდომის საშუალებით აპლიკაციას შეუძლია წაიკითხოს მოწყობილობაში ყველა საკონტაქტო მონაცემი. მაგალითად, თუ მოწყობილობაში ჩაწერილი გაქვთ თქვენი ნაცნობების სახელები და გვარები, ტელეფონის ნომრები, ელ-ფოსტის მისამართები და სხვა საკონტაქტო მონაცემები, TikTok-ის აპლიკაცია კითხულობს ყველა ამ მონაცემს. აღსანიშნავია, რომ აპლიკაცია თქვენს ტელეფონში შენახულ საკონტაქტო მონაცემებზე წვდომის მისაღებად დამატებით შეგეკითხებათ თქვენს ტელეფონში შენახული კონტაქტების TikTok-ში მოძებნის დროს. შესაბამისად, შეგიძლიათ აპლიკაციას მისცეთ აღნიშნული უფლება. აპლიკაციას თქვენს ტელეფონში შენახულ საკონტაქტო მონაცემებზე წვდომა შეიძლება გაუთიშოთ ტელეფონის პარამეტრებიდან.



აპლიკაცია აგროვებს ყველა იმ ვიდეო მასალას, რომელიც პირმა ატვირთა აპლიკაციაში, ასევე ატვირთულ ვიდეოზე სხვა მომხმარებლის მიერ განხორციელებულ ყველა კომენტარსა და მოწონებას. ამასთან, ინახავს ყველა იმ ვიდეო მასალას, რომელსაც მომხმარებელი წინასწარ ტვირთვას აპლიკაციაში და საჯაროდ ჯერ არ გამოუქვეყნებია (კონფიდენციალურობის პოლიტიკის თანახმად, აღნიშნული მიზნად ისახავს მომხმარებლის მიერ ვიდეო მასალის ატვირთვის სიჩქარის გაუმჯობესებას. იმ შემთხვევაში თუ, მომხმარებელი ვერ ან არ მოახდენს ვიდეო ფაილის საბოლოოდ ატვირთვას და სხვა მომხმარებლებისთვის გაზიარებას, ვიდეო მასალის აპლიკაციის შემქმნელი კომპანიის სერვერიდან იგი წაიშლება). აპლიკაცია, ორივე შემთხვევაში, როდესაც მომხმარებელს შექმნილი აქვს საკუთარი ანგარიში ან უბრალოდ იყენებს აპლიკაციას მასში არსებული ინფორმაციის დათვალიერების მიზნით, ავტომატურად აგროვებს მომხმარებელთან დაკავშირებულ ისეთ ტექნიკურ მონაცემებს, როგორიცაა მაგალითად, IP მისამართი; ძებნის ისტორია; ინფორმაცია მობილური ოპერატორის, აპლიკაციის იმ ვერსიის შესახებ, რომელსაც მომხმარებელი იყენებს და სხვა. ადგილმდებარეობის დადგენის მიზნით აპლიკაცია იყენებს მომხმარებლის მიერ საკუთარ გვერდზე მითითებულ ინფორმაციას საცხოვრებელ რეგიონთან დაკავშირებით ან/და GPS-ს სერვისს.

რა მიზნით ხდება მონაცემთა გამოყენება და რა ვადით ინახება ისინი ?

კონფიდენციალურობის პოლიტიკის თანახმად, აპლიკაციის მიერ მომხმარებელთან დაკავშირებით შეგროვებული მონაცემების შენახვა შესაძლოა განხორციელდეს სინგაპურში ან ამერიკის შეერთებულ შტატებში განთავსებულ სერვერებზე, ხოლო აღნიშნული მონაცემები ინახება იქამდე, სანამ მომხმარებელი იყენებს აპლიკაციას ან იქამდე სანამ კომპანიას აქვს ლეგიტიმური ბიზნეს ინტერესი.

მომხმარებლის შესახებ შეგროვებული მონაცემების გამოყენება შესაძლოა მოხდეს სხვადასხვა მიზნით. მაგალითად, აპლიკაციის ეფექტიანი ფუნქციონირების, მათ შორის, მისი გაუმჯობესების, განვითარების და პოპულარობის ხელშეწყობის, მომხმარებლის ინტერესებზე მორგებული სერვისის/რეკლამის შეთავაზების მიზნით.

მონაცემთა გამოყენების მიზნების მრავალფეროვნებიდან გამომდინარე, აპლიკაციის საშუალებით შეგროვებულ მონაცემებზე წვდომა აქვთ მესამე პირებსაც:

- სერვისის მიმწოდებელ კომპანიებს, რომლებიც უზრუნველყოფენ აპლიკაციის გამართულ ფუნქციონირებას;
- ანალიტიკური სერვისის მიმწოდებელ კომპანიებს, რომლებიც მათ შორის, აწარმოებენ მიზნობრივ რეკლამებს;
- სარეკლამო კომპანიებს და სარეკლამო კომპანიათა ქსელებს, რომლებიც მათ შორის, აფასებენ აპლიკაციის რამდენმა მომხმარებელმა ნახა კონკრეტული რეკლამა, რა სახის აქტივობებს ახორციელებს მომხმარებელი აპლიკაციის ფარგლებში და სხვა ვებ-გვერდებზე (აღნიშნული შესაძლებელს ხდის მომხმარებლის ინტერესების იდენტიფიცირებას და შესაბამისი რეკლამის შეთავაზებას).

კონფიდენციალურობის პოლიტიკის თანახმად, აპლიკაციის შემქმნელი კომპანიის მიერ მიღებულია შესაბამისი ორგანიზაციულ-ტექნიკური ზომები მონაცემთა უსაფრთხოების უზრუნველყოფის მიზნით, თუმცა, მითითებულია, რომ ინტერნეტის საშუალებით მონაცემთა გადაცემა არასდროს არ არის აბსოლუტურად უსაფრთხო. შესაბამისად, მიუხედავად იმისა, რომ კომპანია სხვადასხვა გზით, მაგალითად დაშიფვრის გამოყენებით, ახდენს მონაცემთა დაცვას, ის არ იძლევა გარანტიას აპლიკაციის საშუალებით გადაცემული მონაცემების სრულ უსაფრთხოებაზე.

დაცულია თუ არა არასრულწლოვანთა უფლებები?

კონფიდენციალურობის პოლიტიკაში მითითებულია, რომ აპლიკაცია არ არის განკუთვნილი 13 წლამდე ასაკის პირთათვის. რიგ შემთხვევაში, ეს ასაკი შესაძლოა იყოს ნაკლები ქვეყანაში მოქმედი კანონმდებლობის გათვალისწინებით. შესაბამისად, კომპანია მოუწოდებს ყველა იმ პირს, ვინც ფლობს ინფორმაციას, რომ აპლიკაციის საშუალებით ხდება მითითებულ ასაკზე ქვემოთ არასრულწლოვანთა მონაცემების დამუშავება, კომპანიას მიაწოდოს შესაბამისი ინფორმაცია მითითებულ ელექტრონული ფოსტის მისამართზე - privacy@tiktok.com.

გამომდინარე იქიდან, რომ ბავშვის პერსონალურ მონაცემების დამუშავება სპეციალურ, უფრო მკაცრ სტანდარტებსა და წესებს ექვემდებარება, მსოფლიოში განსაკუთრებული აქცენტი სწორედ ამ კუთხით კეთდება. კერძოდ, რამდენად მარტივი ენით აფრთხილებს აპლიკაცია ბავშვებს მონაცემთა დამუშავების შესახებ და რამდენად სწორად ხდება მშობლის თანხმობის მოპოვება.

TikTok-ის შემთხვევა საინტერესოა, რადგან მას შესაძლოა სარეკომენდაციო ხასიათი გააჩნდეს ყველა სხვა აპლიკაციისთვის, რომლებიც ბავშვების პერსონალურ მონაცემებს ამუშავებენ.

როგორ აფასებენ აპლიკაციის უსაფრთხოებას მსოფლიოს სხვადასხვა ქვეყანაში?

ამერიკის შეერთებული შტატები

TikTok აპლიკაციამ ყურადღება მიიქცია აშშ-ში. აპლიკაციის კომპანია 5.7 მილიონი დოლარით დაჯარიმდა ფედერალური სავაჭრო კომისიის მიერ 13 წლის და უფრო პატარა ასაკის მქონე პირთა პერსონალური ინფორმაციის დამუშავების გამო[2]. კომპანიას დაევალა, 13 წლის ასაკამდე ბავშვთა ვერიფიკაციის ადეკვატური ღონისძიებების დანერგვა, რომელიც გამორიცხავდა მათ მიერ აპლიკაციით სარგებლობას (რადგან აპლიკაციით სარგებლობისთვის შესაძლოა, ბავშვები ცრუ ინფორმაციას უთითებდნენ საკუთარ ასაკთან დაკავშირებით).

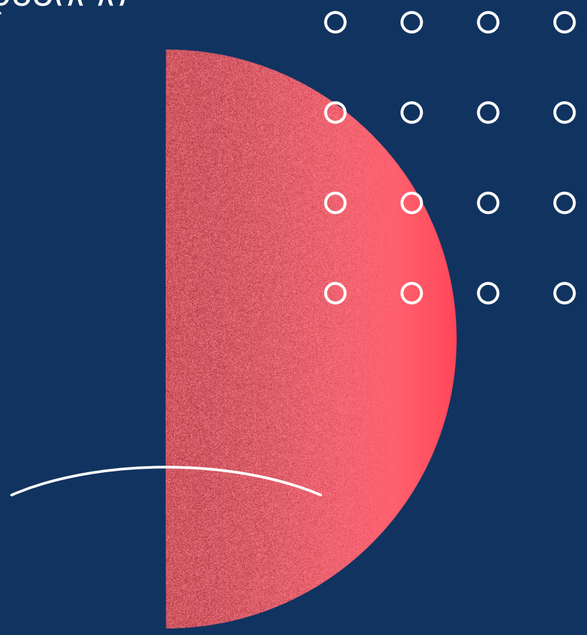
პრობლემა შეიქმნა იმ კუთხითაც, რომ TikTok- მა საბჭოს მოთხოვნების მხედველობაში მიღებისა და ახალი პროფილის შექმნისას ასაკის ვერიფიკაციას ფუნქციის დამატების მიუხედავად, არ გაითვალისწინა ასეთი ვერიფიკაცია უკვე არსებული პროფილების მქონე პირების შემთხვევაში. კერძოდ, 2017 წლის ივლისიდან TikTok ითხოვდა ასაკის ვერიფიკაციას ახალი მომხმარებლებისგან, თუმცა არ განახორციელა ასეთი ვერიფიკაცია იქამდე არსებულ 56 მილიონამდე მომხმარებლებთან მიმართებით. შესაბამისად, უკვე დარეგისტრირებულ მომხმარებლებს ცვლილებები არ შეეხოთ. ასევე, მიუხედავად იმისა, რომ კომპანიამ წაშალა ძველი მომხმარებლის პროფილი, მას არ წაუშლია ის მასალა, რაც ამ მომხმარებლების მიერ უკვე იყო ატვირთული აპლიკაციაში (ამასთან დაკავშირებით სამასამდე მშობელმა გამოთქვა პროტესტი ჯერ კიდევ 2016 წლის სექტემბრისთვის).

[2]
https://iapp.org/news/a/ico-investigating-tiktok-for-handling-of-uk-childrens-data/

ამასთან, *TikTok* ინახავდა პერსონალურ მონაცემებს იმაზე მეტი ხნით, ვიდრე სჭირდებოდა.*[3]* სწორედ ამ დარღვევების გამო იქნა დაჯარიმებული კომპანია.

ვინაიდან მსგავს აპლიკაციებს ხშირად წვდომა აქვთ იმაზე მეტ ინფორმაციაზე, ვიდრე ამის შესახებ თანხმობას აძლევს მომხმარებელი, აშშ-ში დაიწყო საუბარი იმაზეც, ხომ არ იყენებს აპლიკაციით შეგროვებულ ინფორმაციას ჩინეთი.*[4]* მითუმეტეს, რომ *TikTok*-ის ამერიკაში მცხოვრებ პირთათვის განკუთვნილი უსაფრთხოების პოლიტიკის თანახმად, აპლიკაცია ავტომატურად აგროვებს სხვდასხვა ინფორმაციას - *IP* მისამართები, გეოლოკაცია, უნიკალური მადენტიფიცირებლები *(unique device identifiers),* ინტერნეტ ბრაუზერისა და ძებნის ისტორია *(*ასევე ის ინფორმაცია, რაც მომხმარებელმა ნახა პლატფორმის მეშვეობით*)* და *Cookies* ფაილები.

ვინაიდან გაჩნდა ეჭვი ჩინეთის მიერ ზემოაღნიშნული მონაცემების სადაზვერვო მიზნებისთვის გამოყენების შესახებ, აშშ-ში ოფიციალურ დონეზე დაიწყო საუბარი იმაზე, რომ სახელმწიფო მოხელეებს მიეცეთ პირდაპირი მითითება, არ გამოიყენონ აპლიკაცია.



[3]
https://books.google.ge/books?id=Db64DwAAQBAJ&pg=PA135&lpg=PA135&dq=tiktok+personal+data&source=bl&ots=bRJr8axrxv&sig=ACfU3U24cgUO8bAySmJorG_Yi_Wjwbj8YQ&hl=en&sa=X&ved=2ahUKEwjgxLKI_LLpAhVz8uAKHR1ED3g4FBDoATAAegQIChAB#v=onepage&q=tiktok%20personal%20data&f=false

[4]
https://www.lawfareblog.com/unpacking-tiktok-mobile-apps-and-national-security-risks

ნიდერლანდები

აპლიკაციის შემოწმება, დაწყებულია ნიდერლანდების პერსონალურ მონაცემთა საზედამხედველო ორგანოს მიერ,[5] რომელმაც შემოწმების დაწყების შესახებ ოფიციალური განცხადება 2020 წლის 8 მაისს გააკეთა.

ნიდერლანდების საზედამხედველო ორგანო შეისწავლის, რამდენადაა დაცული ნიდერლანდელი ბავშვების პირადი ცხოვრება, რამდენად ხორციელდება მშობლებისგან თანხმობის აღება ბავშვების პერსონალურ მონაცემთა დასამუშავებლად და რამდენად უსაფრთხოდ მუშავდება მონაცემები. საზედამხედველო ორგანო ასევე შეაფასებს, რამდენად მეგობრულია (privacy-friendly) აღნიშნული აპლიკაცია პირადი ცხოვრებისადმი.

[5]
იხ. საზედამხედველო ორგანოს ოფიციალური განცხადება შემდეგ ბმულზე: https://autoriteitpersoonsgegevens.nl/en/news/dutch-data-protection-authority-investigate-tiktok

იტალია

აპლიკაციით დაინტერესდა იტალიის მონაცემთა დაცვის საზედამხედველო ორგანოც, რომელმაც ოფიციალური წერილით მიმართა ევროპის მონაცემთა დაცვის საბჭოს (EDPB) და მოსთხოვა მომდევნო შეხვედრაზე, რომელიც 2020 წლის 28-29 იანვარს უნდა ჩატარებულიყო, აღნიშნული აპლიკაციის საკითხის დღის წესრიგში შეეტანა[6].

აღსანიშნავია, რომ იტალიური კანონის თანახმად, 16 წლის ასაკამდე პირთა პერსონალური მონაცემების დამუშავებისთვის აუცილებელია მშობლის ან მეურვის თანხმობა, ხოლო 13 წლის ასაკამდე პირთა პერსონალურ მონაცემთა დამუშავება საერთოდ აკრძალულია.

[6]
იხ. იტალიის საზედამხედველო ორგანოს ოფიციალური ვებგვერდი შემდეგ ბმულზე: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9249681

დიდი ბრიტანეთი

აპლიკაციას ასევე სწავლობს დიდი ბრიტანეთის პერსონალურ მონაცემთა საზედამხედველო ორგანო, რომლის განცხადებითაც TikTok დიდი ალბათობით შესაძლოა არღვევდეს GDPR-ს, რომელიც კომპანიებისაგან მოითხოვს სხვადასხვა სერვისს და დაცვის ღონისძიებას ბავშვებისთვის. ბრიტანეთის საზედამხედველო ორგანო დაინტერსდა იმითაც, არის თუ არა შესაძლებელი, უცხო პირი მიერ არასრულწლო-ვნებთან პირდაპირ კონტაქტზე გასვლა და მიმოწერა, რაც შესაძლოა გარკვეული საფრთხეების შემცველი იყოს.

სახელმწიფო
ინსპექტორის
სამსახური