REKOMENDACIJA DĖL SAUGAUS MOBILIŲJŲ APLIKACIJŲ NAUDOJIMO MOBILIUOSIUOSE ĮRENGINIUOSE

2023-06-15

Valstybinės duomenų apsaugos inspekcijos (toliau – VDAI) rekomendacija skirta mobiliųjų įrenginių naudotojams. Šios rekomendacijos tikslas – atkreipti mobiliąsias aplikacijas naudojančių fizinių asmenų (toliau – naudotojai) dėmesį į aplikacijų renkamus duomenis ir paskatinti jomis naudotis atsakingai, t. y. saugant savo asmens duomenis. Taip pat svarbu atkreipti dėmesį ir į priemones, kurių asmenys galėtų imtis, kad nebūtų renkami pertekliniai duomenys.

Mobiliųjų aplikacijų renkama informacija

Mobiliosios aplikacijos gali rinkti skirtingą kiekį duomenų, tačiau daugeliu atvejų renkamų asmens duomenų kiekis priklauso nuo tokios aplikacijos naudotojo suteiktų leidimų, t. y. naudotojas, kontroliuodamas savo asmens duomenų tvarkymą naudojantis mobiliąja aplikacija, paprastai gali pasirinkti, prie kokių mobiliojo įrenginio duomenų jis leidžia tokiai aplikacijai prieiti ar kitaip naudoti. Naudotojui davus leidimą, mobilioji aplikacija gali gauti prieigas prie: kontaktų, skambučių ar žinučių, mikrofono, vaizdo kameros, įrenginyje esančių nuotraukų, užrašų, grojaraščių, įrenginio buvimo vietos, o tam tikrais atvejais ir prie visų mobiliajame įrenginyje esančių duomenų. Taip pat svarbu būti atidiems ne tik suteikiant leidimus dėl prieigų prie mobiliajame įrenginyje esančių asmens duomenų, bet taip pat nurodant asmens duomenis, suteikiant teisę juos rinkti ir tvarkyti, naudojantis tokia aplikacija (t. y. papildomai renkami ar tretiesiems asmenims teikiami asmens duomenys), pavyzdžiui, aplikacijų naudotojų buvimo vietos, judėjimo krypties, greičio, kitų įpročių ar kt.

Kylančios grėsmės dėl mobiliųjų aplikacijų renkamos informacijos

BDAR[1] kelia griežtus reikalavimus mobiliąsias aplikacijas norintiems naudoti duomenų valdytojams (toliau – Duomenų valdytojai), jie turi ne tik įvertinti tokiomis aplikacijomis tvarkomų asmens duomenų apimtį ir judėjimą (iš kur renkami, kaip tvarkomi aplikacijoje, su kuo jungiami, kam teikiami ir pan.), bet taip pat, kaip tvarkomus asmens duomenis apsaugoti (kokias taikyti technines ir organizacines saugumo priemones (žr. VDAI rizikos vertinimo gaires arba ENISA rizikos vertinimo įrankį). Tai ypač svarbu, kai asmens duomenys, naudojantis konkrečia aplikacija, tvarkomi (saugomi) serveriuose, debesų infrastruktūroje ar duomenų bazėse trečiosiose valstybėse, įskaitant atsargines kopijas. Tokiais atvejais mobiliąsias aplikacijas siūlantys Duomenų valdytojai turi imtis papildomų priemonių, siekiant užtikrinti būtiną apsaugos lygį.

Tuo atveju, jei naudojamasi nesaugiomis (nepatikimomis) mobiliosiomis aplikacijomis, jų naudotojai gali susidurti su tokiomis rizikomis:

- į aplikaciją pateikiami ir su aplikacija susieti asmens duomenys gali būti naudojami nusikalstamų veikų tikslais (pavyzdžiui, siekiant gauti prieigas prie naudotojo ar su juo susijusių asmenų piniginių lėšų, atlikti pinigų perlaidas į trečiųjų asmenų sąskaitas; naudotojo buvimo vietų ar kalendoriuje esantys duomenys gali padėti prognozuoti, kada naudotojas paliks tam tikras patalpas ir kiek laiko tokiose patalpose nebus pašalinių asmenų; ar kt.);
- aplikacijoje vykdomas susirašinėjimas arba šiame susirašinėjime esanti foto ar vaizdo medžiaga gali būti naudojama paveikti asmenį (pavyzdžiui, grasinant susirašinėjimą paviešinti internete);
- aplikacijoje tvarkomi asmens duomenys gali būti panaudoti jos naudotojo profiliui sudaryti ir tokiu pagrindu siųsti tikslinę reklamą (pavyzdžiui, perduodant tokius profilius tretiesiems asmenims);
- asmens duomenys gali būti perduoti į trečiąsias valstybes ir dėl to naudotojas prarastų tokių asmens duomenų kontrolę bei galimybes įgyvendinti savo, kaip duomenų subjekto, teises ar jas ginti priežiūros institucijose ar teisme;
- tinkamai neužtikrinama aplikacijų apsauga gali sudaryti sąlygas aplikacijoje saugomos intelektinės nuosavybės praradimui, reputacinei žalai ir kt.;
- asmens duomenys gali būti naudojami kibernetinėms atakoms (pavyzdžiui, iš naudotojo įrenginio ar paskyros) vykdyti;
- aplikacijoje tvarkomi ar su aplikacija susieti asmens duomenys gali būti naudojami socialinės inžinerijos atakoms[2] ar kt.

Mobiliųjų aplikacijų Duomenų valdytojų pateikiama informacija apie renkamus naudotojų duomenis

Mobiliųjų aplikacijų naudotojai, prieš įdiegdami ar pradėdami naudoti mobiliąsias aplikacijas, turėtų susipažinti su tokių aplikacijų privatumo pranešimais ir naudojimosi taisyklėmis, taip pat atidžiai įvertinti prašomus suvesti asmens duomenis ar suteikiamus leidimus (šiuo atveju rekomenduotina

[1] 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).

[2] Socialinė inžinerija (angl. *social engineering*) – tai psichologinio manipuliavimo forma, kuri apima socialines priemones nukreiptas ir vykdomas atliekant sistemos puolimą ne techninėmis priemonėmis.

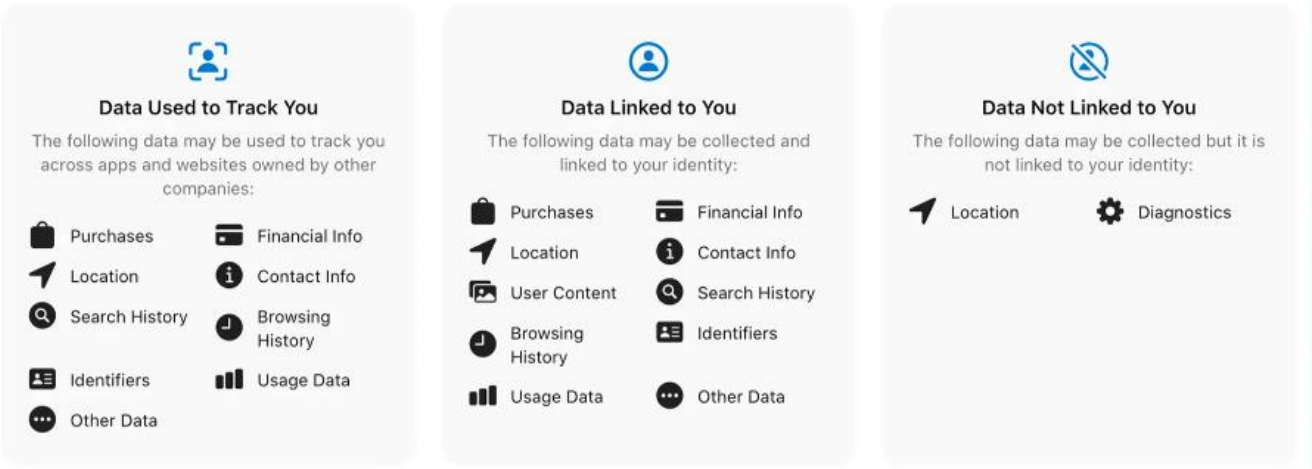
atidžiai įvertinti, kurie asmens duomenys bus tvarkomi nepriklausomai nuo naudotojo valios, t. y. kokie asmens duomenys bet kuriuo atveju bus tvarkomi naudojantis konkrečia aplikacija). Tokia informacija turi būti pateikiama ne tik įmonės, įstaigos, kuri naudoja mobiliąją aplikaciją savo veikloje, interneto svetainėje, bet ir pačioje mobiliojoje aplikacijoje. Pabrėžtina, kad minėta informacija turi būti pasiekiama naudotojui dar prieš suvedant savo asmens duomenis, suteikiant leidimus ar sukuriant paskyras. Tuo atveju, jei naudotojui prieinama informacija kelia abejonių arba mobiliojoje aplikacijoje privatumo politika, naudojimosi taisyklės ar pan. nėra pateikiamos arba pateikiamos paviršutiniškai, rekomenduotina gerai apsvarstyti, ar tokia mobiliąja aplikacija vertėtų pasitikėti.

Tuo atveju, jei siekiama įsidiegti mobiliąsias aplikacijas iš mobiliųjų aplikacijų platformų, jose pasirinkus konkrečią aplikaciją, galima rasti nuorodą į privatumo pranešimą (kuriame pateikiama informacija apie aplikacijų renkamus asmens duomenimis, jų naudojimo tikslus ir t. t.), taip pat atskirai pateikiama informacija, kokie asmens duomenys konkrečiai bus tvarkomi, pavyzdžiui:

Duomenys naudojami sekti jus (angl. *Data Used to Track You*) skirti sekti naudotojo veiksmus ir rinkti duomenis, ne tik jam naudojantis aplikacija, bet ir naudotojui naudojantis kitomis aplikacijomis ar lankantis interneto svetainėse, naudojant naudotojo kontaktinę informaciją (pavyzdžiui, elektroninio pašto adresus, telefono numerius) ir įrenginio identifikatorių (kuris leidžia trečiosioms šalims sekti naudotojus per kitas aplikacijas, svetaines ar teikiamas paslaugas). Toks asmens duomenų rinkimas užtikrina galimybę trečiosioms šalims pateikti naudotojams tikslinę reklamą.

Su Jumis susietų duomenų (angl. *Data Linked to You*) rinkimas ir tolesnis tvarkymas skirtas Duomenų valdytojams gebėti identifikuoti naudotojus pagal surinktus asmens duomenis, t. y. nustatyti jų tapatybę.

Su jumis nesusieti duomenys (angl. *Data Not Linked to You*) skirti rinkti statistinius duomenis. Tai reiškia, kad šiuo atveju surinkti duomenys negali būti susieti su naudotoju taip, kad jį būtų galima identifikuoti (pavyzdžiui, tokiu atveju nėra tvarkomas elektroninio pašto adresas, naudotojo buvimo vieta ar kt.).



Informacija, kaip naudotojams susipažinti su aplikacijų privatumo pranešimais, pateikta tolesniame skyriuje.

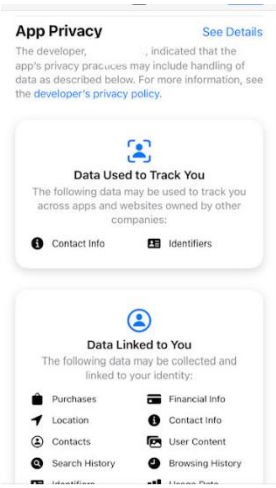
Patarimai dėl asmens duomenų saugumo užtikrinimo naudojant mobiliąsias aplikacijas

Mobiliąsias aplikacijas naudotojai gali atsisiųsti ne tik iš mobiliųjų aplikacijų platformų, bet ir tiesiogiai iš interneto svetainių, todėl siekiant geriau užtikrinti duomenų saugumą, naudotojams būtų aktualu susipažinti su VDAI parengta susijusia metodine informacija: dėl sukčiavimo internete, saugaus naršymo internete ir patarimais, ką daryti, jeigu paskyra buvo „nulaužta“. Naudotojams naudojantiems „Android“ įrenginius taip pat būtų aktualu nepamiršti rekomendacijos dėl asmens duomenų apsaugos „Android“ įrenginiuose.

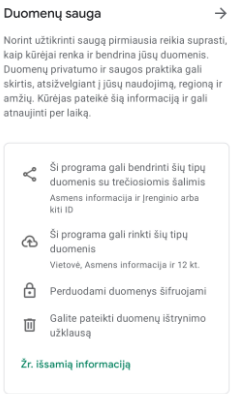
Daugeliu atvejų naudotojai į savo mobiliuosius įrenginius mobiliąsias aplikacijas diegiasi iš mobiliųjų aplikacijų platformų, todėl toliau pateikiami patarimai, kaip naudotojams, naudojantiems mobiliuosius įrenginius su „iOS“ ar „Android“ operacinėmis sistemomis, apsaugoti savo asmens duomenis.

1. **Siųstis mobiliąsias aplikacijas tik iš oficialių mobiliųjų aplikacijų platformų („App Store“, „Google Play“ ar kt.).**

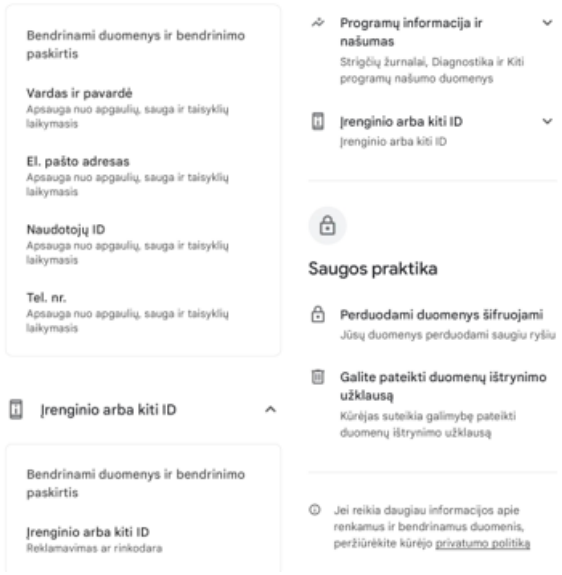
2. **Prieš siunčiantis mobiliąsias aplikacijas iš oficialių aplikacijų platformų, susipažinkite su platformose paskelbtais privatumo pranešimais:**



a) „App Store“ pateikiamos mobiliųjų aplikacijų privatumo politikos: platformoje pasirinkus norimą atsisiųsti mobiliąją aplikaciją, žemiau skiltyje „Duomenų sauga“ arba „Privatumas aplikacijoje“ (angl. *App Privacy*) pateikiama informacija, kokios asmens duomenų kategorijos renkamos, ir nuoroda į mobiliosios aplikacijos privatumo politiką ar kitą su asmens duomenų tvarkymu susijusią informaciją, pavyzdžiui, papildomai prie „Privatumas aplikacijoje“ (angl. *App Privacy*) paspaudžiant „Peržiūrėti detaliau“ (angl. *See Details*).

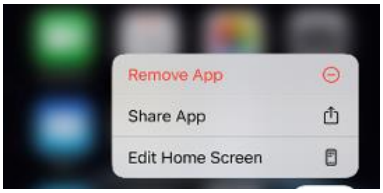


b) „Google Play“ pateikiamos mobiliųjų aplikacijų privatumo politikos: platformoje pasirinkus norimą atsisiųsti mobiliąją aplikaciją, žemiau esančiose skiltyse „Apie šią programą“ (angl. *About This App*) ir „Duomenų sauga“ (angl. *Data Safety*) pateikiama informacija, kokios duomenų kategorijos renkamos, jų rinkimo tikslai, kam asmens duomenys teikiami ir pan. (paspaudus šių skilčių pavadinimus arba „Žr. išsamią informaciją“ (angl. *See Details*).



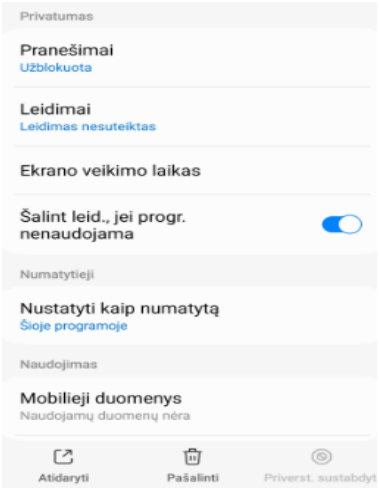
Taip pat skiltyje „Duomenų sauga“ (angl. *Data Safety*) pateikiama nuoroda į privatumo pranešimą.

3. Periodiškai peržiūrėti mobiliajame įrenginyje turimas mobiliąsias aplikacijas, o nenaudojamas ištrinti. Tokiu būdu kontroliuojama, kiek mobiliųjų aplikacijų turi prieigą prie naudotojo asmens duomenų.



a) Naudojamų mobiliųjų aplikacijų ištrynimas „iOS“ operacinėje sistemoje – ilgai laikant nuspaudus pasirinktos mobiliosios aplikacijos piktogramą ir iššokusiame langelyje pasirinkus „Ištrinti programėlę“ (angl. *Remove App*).

b) Naudojamų mobiliųjų aplikacijų ištrynimas „Android“ operacinėje sistemoje – ilgai laikant nuspaudus mobiliosios aplikacijos piktogramą ir iššokusiame langelyje pasirenkama „Šalinti“ (angl. *Uninstall*).



Arba pasirinkus „Nustatymai“ (angl. *Settings*), „Programos“ (angl. *Apps*), tuomet reikiamą mobiliąją programėlę ir, atsidarius jos informacijai, pasirenkama „Pašalinti“ (angl. *Uninstall*).

4. Prieš naudojantis mobiliosiomis aplikacijomis, svarbu įsivertinti, kokių tikslų siekiama, ir atsižvelgiant į juos apriboti prieigas.

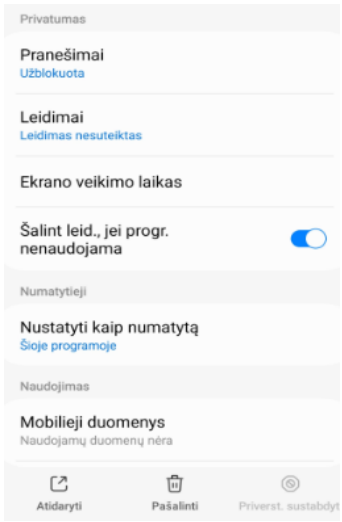
1 Pavyzdys. Naudojantis tiesioginiam bendravimui skirtomis aplikacijomis (pavyzdžiui, susirašinėjimo aplikacijomis ir pan.) galima apriboti prieigas prie mikrofono, jei naudotojas niekada nenaudoja skambinimo funkcijos ar balso pranešimo (angl. *Voice Message*).

2 Pavyzdys. Naudojantis tiesioginiam bendravimui skirtomis aplikacijomis (pavyzdžiui, susirašinėjimo aplikacijomis ir pan.) galima apriboti prieigas prie fotonuotraukų, įrenginio fotoaparato, jei naudotojas nesiekia šia aplikacija daryti fotonuotraukų ar jomis dalintis.

Svarbu atkreipti dėmesį, kad prieigos mobiliosioms aplikacijoms gali būti apribotos diegiantis aplikacijas ar bet kuriuo kitu naudotojo pasirinktu laiku. Taip pat naudotojas bet kuriuo metu gali suteikti prieigas, pavyzdžiui pasikeitus mobiliosios aplikacijos naudojimosi tikslams.

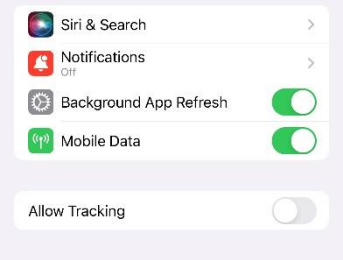
5. Periodiškai peržiūrėkite mobiliosioms aplikacijoms suteiktus leidimus savo mobiliuosiuose įrenginiuose:

a) Naudojamoms mobiliosioms aplikacijoms suteiktų leidimų peržiūra ir leidimų atšaukimas „iOS“ operacinėje sistemoje: mobiliojo įrenginio nustatymuose (angl. *Settings*), žemiau šioje skiltyje, pasirenkama konkreti mobilioji aplikacija. Atsidariusiame atskirame lange galima valdyti šiai aplikacijai suteiktus leidimus (juos atšaukti arba suteikti).



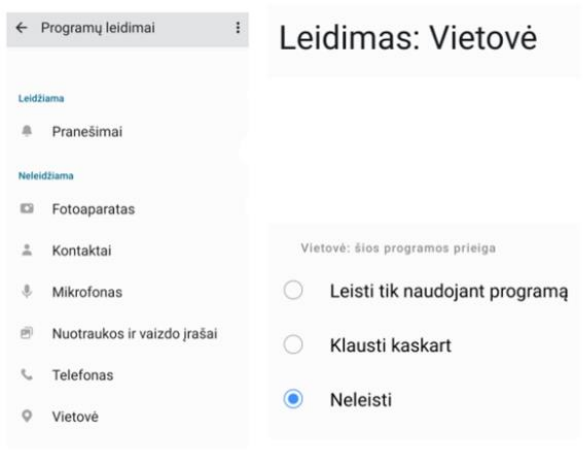
b) Naudojamoms mobiliosioms aplikacijoms suteiktų leidimų peržiūra ir leidimų atšaukimas „Android“ operacinėje sistemoje: mobiliojo įrenginio nustatymuose (angl. *Settings*) pasirenkama skiltyje „Programos“ (angl. *Apps*) konkreti mobilioji aplikacija. Atsidariusiame atskirame lange paspaudus „Leidimai“ (angl. *Permissions*) galima valdyti šiai aplikacijai suteiktus leidimus (juos atšaukti arba suteikti).

6. Įsitikinkite, kad nesant būtinumui mobiliajai aplikacijai nėra suteiktas leidimas sekti naudotoją ar prieiga prie buvimo vietos duomenų.



a) „iOS“ operacinę sistemą turinčių mobiliųjų įrenginių nustatymuose (angl. *Settings*) pasirinkus konkrečią mobiliąją aplikaciją galima išjungti stebėjimo funkciją (angl. *Allow Tracking*).

arba pasirinkus buvimo vietos duomenų tvarkymo nustatymus (angl. *Location*), galima pasirinkti atvejus, kai tokią prieigą sutinkate suteikti, pavyzdžiui, „niekada“ (angl. *Never*).



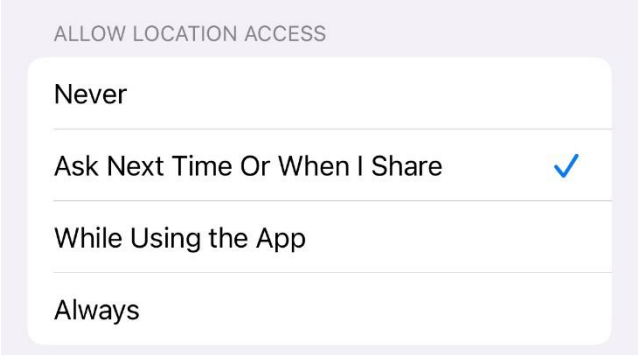
b) „Android“ operacinę sistemą turinčių mobiliųjų įrenginių nustatymuose (angl. *Settings*) pasirinkti „Programos“ (angl. *Apps*) ir jose pasirinkus konkrečią mobiliąją aplikaciją, galima pasirinkti atvejus, kai prieigą prie buvimo vietos duomenų (angl. *Location*) sutinkate suteikti.

Apriboti prieigą prie buvimo vietos duomenų aktualu tuomet, jei buvimo vietos nustatymo funkcionalumas tuo metu naudotojui nėra reikalingas. Norėdamas apriboti ar atšaukti prieigą prie buvimo vietos duomenų, naudotojas gali pasirinkti vieną iš šių siūlomų galimybių:

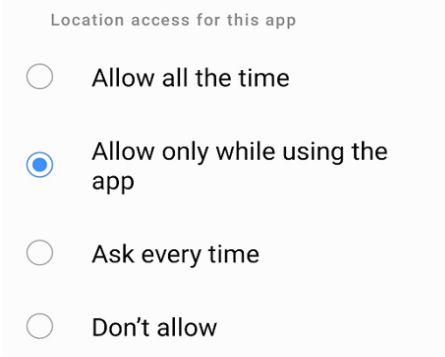
- pasirinkus „Niekada“ (angl. *Never*), prieiga prie naudotojo buvimo vietos duomenų nebus suteikiama;
- pasirinkus „Kaskart klausti arba kai dalinuosi“ (angl. *Ask Next Time or When I Share*), prieiga prie naudotojo buvimo vietos duomenų bus suteikta tik naudotojui įsijungus mobiliąją aplikaciją ir patvirtinus tokį leidimą papildomai;
- pasirinkus „Leisti tik naudojant programą“ (angl. *While Using the App*), prieiga prie naudotojo buvimo vietos duomenų suteikiama tik naudojant mobiliąją aplikaciją (t. y. iš jos išėjus buvimo vietos duomenys nebebus jai perduodami);
- pasirinkus „Visada“ (angl. *Always*), naudotojo buvimo vietos duomenys perduodami mobiliajai aplikacijai nuolat. Tai reiškia, kad kai prieigos naudotojui yra aktualios (reikalingos) (pavyzdžiui,

naudojantis navigacija ar kt.), tuomet naudotojas gali pasirinkti vienkartinį leidimą suteikti prieigą mobiliajai aplikacijai prie buvimo vietos duomenų („Kaskart klausti arba kai dalinuosi“ (angl. *Ask Next Time or When I Share“*) arba tik tuomet, kai konkrečia mobiliąja aplikacija naudotojas naudojasi „Leisti tik naudojant programą“ (angl. *While Using the App*).

1 Pavyzdys (jei naudojama „iOS“)



2 Pavyzdys (jei naudojama „Android“)



7. **Socialinių tinklų, pažinčių, susirašinėjimo mobiliosioms aplikacijoms patartina nesuteikti leidimo prie naudotojo mobiliajame įrenginyje išsaugotų kontaktų, o konkrečius naudotojo pasirinktus asmenis pridėti į tokią aplikaciją atskirai.**

8. **Ilgą laiką naudojantis mobiliąja aplikacija, rekomenduotina reguliariai peržiūrėti jos skelbiamą privatumo politiką ir susijusią informaciją (įvertinti, ar nebuvo atlikta jų pakeitimų, kurie gali būti svarbūs naudotojui), taip pat susipažinti su mobiliosiose aplikacijose sukauptais Jūsų asmens duomenimis.**

Kai kuriose mobiliosiose aplikacijose tvarkomus naudotojo asmens duomenis galima atsisiųsti šiais žingsniais:

- „Nustatymai“ (angl. *Settings*) > „Paskyra“ (angl. *Account*) arba „Paskyros nustatymai“ (angl. *Account Settings*) > „Atsisiųsti duomenis“ (angl. *Download Your Data*).
  arba
- „Daugiau“ (angl. *More*) > „Nustatymai“ (angl. *Settings*) > „Privatumas“ (angl. *Privacy*) > „Asmeniniai duomenys“ (angl. *Personal Data*) > „Prašyti savo duomenų“ (angl. *Request Your Data*).

Svarbu pabrėžti, kad teisė susipažinti su savo duomenimis ir kitos duomenų subjekto teisės (teisė ištaisyti netikslius duomenis, teisė būti pamirštam ir kt.) gali būti įgyvendinamos įvairiais būdais, todėl visais atvejais siūloma susipažinti su informacija mobiliosios aplikacijos privatumo politikoje ir aplikacijos nustatymuose.